ISSN 1851-1295

Fascículo 9 | Cursos de grado

Teresa Krick

Álgebra I

Departamento de Matemática

Facultad de Ciencias Exactas y Naturales

Universidad de Buenos Aires

2017

Cursos de grado

Fascículo 9

Comité Editorial:

Carlos Cabrelli (Director)
Departamento de Matemática, FCEyN, Universidad de Buenos Aires
E-mail: cabrelli@dm.uba.ar

Gabriela Jerónimo
Departamento de Matemática, FCEyN, Universidad de Buenos Aires
E-mail: jeronimo@dm.uba.ar

Claudia Lederman
Departamento de Matemática, FCEyN, Universidad de Buenos Aires
E-mail: clederma@dm.uba.ar

Leandro Vendramin
Departamento de Matemática, FCEyN, Universidad de Buenos Aires.
E-mail: lvendramin@dm.uba.ar

ISSN 1851-1317 (Versión Electrónica)
ISSN 1851-1295 (Versión Impresa)

Derechos reservados
© 2017 Departamento de Matemática, Facultad de Ciencias Exactas y Naturales,

Universidad de Buenos Aires.
Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria – Pabellón I
(1428) Ciudad de Buenos Aires
Argentina.
http://www.dm.uba.ar
e-mail. secre@dm.uba.ar
tel/fax: (+54-11)-4576-3335

UNIVERSIDAD DE BUENOS AIRES

Facultad de Ciencias Exactas y Naturales

Departamento de Matemática

ÁLGEBRA I

Teresa Krick

–2017–

Prefacio

Estas notas reflejan el contenido teórico de la materia Algebra I que se dicta en la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires para les estudiantes de las carreras de computación y de matemática, y ahora también de ciencias de datos, e incluyen el enfoque algorítmico que se decidió acentuar a partir del segundo cuatrimestre 2013 en un proyecto conjunto con el Departamento de Computación.

Las empecé a redactar en 2013 con el apoyo del Departamento de Matemática al que agradezco mucho, y la revisión de 2017 comprende los ajustes que se han discutido a lo largo de estos años. Va mi reconocimiento a Carlos Cabrelli que me animó a juntar los capítulos que están online desde el 2013 en una publicación del departamento. Muches me ayudaron en esta tarea durante las largas discusiones que mantuvimos, con respecto a la forma de presentar las cosas y a formular los conceptos: Matías Graña, Ariel Pacetti, Pablo de Nápoli, y también con sus comentarios y correcciones a lo largo del tiempo: Nicolás Allo Gomez, Eda Cesaratto, Marco Farinati, Daniel Perrucci, Mauro Rodriguez Cartabia, Román Sasyk, Mariano Suárez-Alvarez, Leandro Vendramin; y seguramente me estoy olvidando de unes cuántes que ruego me disculpen. Persisten aún así muchos errores que son todos míos: agradeceré mucho a todes les que me ayuden a corregirlos.

Charlando con la dirección del departamento en ese momento, Noemí Wolanski y Gabriela Jeronimo, hemos acordado en agregar a este texto las prácticas de la materia, que por supuesto no me pertenecen sino que son el resultado del trabajo de muches docentes de la materia a lo largo de los años. Los contenidos teóricos presentados aquí apuntan a permitir entender los conceptos necesarios para poder resolver los ejercicios, brindando además varios ejemplos que ilustran su utilización para esa resolución. Además, intentan incluir aunque sea de modo muy superficial un poco de la historia y/o protagonistas que hicieron esta historia, incluyendo acontecimientos actuales, con el afán de ilustrar que el álgebra no es para nada una ciencia muerta sino que está en constante movimiento. Cabe mencionar que mucho de este movimiento es hoy debido al desarrollo de la computación y su influencia en la matemática.

Quiero prevenir a la lectora y al lector que a lo mejor se puede desmoralizar por la cantidad de demostraciones que va a encontrar en estas notas: al ser un texto escrito intenté ser bastante detallada por afán de completitud, pero está claro que a la hora de dictar esta materia, le docente va a tener que elegir –por una cuestión de tiempo– qué demostraciones presenta para ejemplificar el desarrollo de estos temas, y cuáles va a esbozar solamente, o incluso pasar por alto. De todos modos puede resultar provechoso para le estudiante interesade encontrar aquí demostraciones que no se han terminado de dar o formalizar en el aula.

Finalmente, no incluí bibliografía ya que es enorme la cantidad de referencias que hay sobre estos temas, en general mucho más profundas que lo que presento aquí. Quiero mencionar sin embargo el completísimo texto de Carlos Sánchez del 2014, *Lecciones de Álgebra*, en esta misma serie, donde les lectores podrán encontrar mucho más contenido y también información sobre dónde buscar más si así lo desean. La diferencia es que las notas que están mirando ahora, bastante menos profundas y más informales, intentan acompañar exactamente el dictado de la materia en el primer cuatrimestre de la Facultad de Ciencias Exactas y Naturales de nuestras y nuestros estudiantes.

Se hizo una revisión de estas notas en diciembre 2020. Agradezco muy especialmente a Leandro Otouzbirian por su minuciosa lectura y múltiples correcciones de la revisión correspondiente a marzo 2019. ¡Gracias por ayudar a que el texto tenga cada vez menos errores groseros, matemáticos y de los otros!

Enseñé la materia durante el año 2021 tomando como base este texto. Allí aparecieron una multitud de errores más que fueron –espero– corregidos. Agradezco enfáticamente a todo mi equipo docente y a mis estudiantes, no sólo por señalarmelos sino también por el gran año compartido. Mi gratitud total a Ian Apster quién debe ser, junto con Leandro Otouzbirian, la persona que más me ayudó a limpiar estas líneas. También, junto con mis entrañables docentes Nico Alló Gómez, Georgi Giacobbe e Isa Herrero aprovechamos para revisar y ajustar las guías de prácticas de la materia: va sin decir que fueron elles quiénes hicieron todo el trabajo, sumándolo a todas sus obligaciones y responsabilidades y sacando horas de no sé donde. Sin palabras...

Teresa Krick, Mayo 2022

Índice general

Prefacio **1**

1 Conjuntos, Relaciones y Funciones. **9**

1.1 Conjuntos. 9

1.1.1 Conjuntos y subconjuntos, pertenencia e inclusión. . . 9

1.1.2 Operaciones entre conjuntos. 12

1.1.3 Tablas de verdad de la lógica proposicional. 17

1.1.4 Producto cartesiano. 20

1.2 Relaciones. 21

1.2.1 Relaciones en un conjunto. 22

1.3 Funciones. 29

1.3.1 Funciones biyectivas y función inversa. 35

1.4 Ejercicios. 38

2 Números Naturales e Inducción. **47**

2.1 La suma de Gauss y la serie geométrica. 49

2.1.1 La suma de Gauss. 49

2.1.2 La serie geométrica. 49

2.2 Sumatoria y Productoria. 50

2.2.1 Sumatoria. 50

2.2.2 Productoria. 52

2.3 El conjunto inductivo $\mathbb{N}$ y el principio de inducción. 53

2.3.1 Inducción “corrida”. 58

2.4 Sucesiones definidas por recurrencia. 61

2.5 Inducción completa. 65
2.5.1 Inducción completa – Un caso particular. 65
2.5.2 La sucesión de Fibonacci. 67
2.5.3 Sucesiones de Lucas. 71
2.5.4 Inducción completa – Formulación general. 73
2.6 Apéndice 78
2.6.1 Los axiomas de Peano. 78
2.6.2 El Principio de Buena Ordenación y los Principios de Inducción. 79
2.7 Ejercicios. 80

3 Combinatoria **87**
3.1 Cardinal de conjuntos y cantidad de relaciones. 87
3.1.1 Cardinal de un producto cartesiano y del conjunto de partes. 88
3.1.2 Cantidad de relaciones y de funciones. 90
3.2 El factorial. 91
3.2.1 Cantidad de funciones inyectivas. 92
3.3 El número combinatorio. 93
3.3.1 El triángulo de Pascal: una fórmula recursiva para $\binom{n}{k}$. 95
3.3.2 La expresión del número combinatorio. 97
3.3.3 El Binomio de Newton. 99
3.4 Ejercicios. 102

4 Enteros – Primera parte. **107**
4.1 Hechos generales. 107
4.2 Divisibilidad. 109
4.2.1 Congruencia. 113
4.3 Algoritmo de división. 117
4.4 Sistemas de numeración. 124
4.4.1 Criterios de divisibilidad. 130

4.5 Máximo común divisor. 131
4.5.1 Algoritmo de Euclides. 132
4.5.2 Números coprimos. 140
4.6 Primos y factorización. 144
4.6.1 La propiedad fundamental de los números primos. . . 148
4.6.2 El Teorema fundamental de la aritmética. 150
4.6.3 Mínimo común múltiplo. 159
4.7 Apéndice 161
4.8 Ejercicios. 162

5 Enteros – Segunda parte. 169
5.1 Ecuaciones lineales diofánticas. 169
5.2 Ecuaciones lineales de congruencia. 175
5.3 Teorema chino del resto (TCR). 181
5.4 El Pequeño Teorema de Fermat (PTF) 192
5.4.1 Tests probabilísticos de primalidad. 199
5.5 El sistema criptográfico RSA. 202
5.6 El anillo $\mathbb{Z}/m\mathbb{Z}$ y el cuerpo $\mathbb{Z}/p\mathbb{Z}$. 206
5.6.1 El anillo $\mathbb{Z}/m\mathbb{Z}$. 206
5.6.2 El cuerpo $\mathbb{Z}/p\mathbb{Z}$. 208
5.7 Ejercicios. 210

6 Números Complejos. 215
6.1 Cuerpos. 215
6.2 Números complejos: forma binomial. 216
6.3 Números complejos: forma trigonométrica. 222
6.4 Raíces n-ésimas de números complejos. 227
6.4.1 El grupo G_n de raíces n-ésimas de la unidad. 228
6.5 Ejercicios. 236

7 Polinomios. 239
7.1 El anillo de polinomios $K[X]$: generalidades. 239

7.1.1 Operaciones en $K[X]$ 240
7.1.2 Divisibilidad, Algoritmo de División y MCD en $K[X]$. 242
7.1.3 El Teorema Fundamental de la Aritmética para Polinomios. 248
7.2 Evaluación y Raíces. 249
7.2.1 Multiplicidad de las raíces. 251
7.2.2 Cantidad de raíces en K 257
7.2.3 Cálculo de raíces en $\mathbb{Q}$ de polinomios en $\mathbb{Q}[X]$ 258
7.3 Factorización en $K[X]$ 260
7.3.1 Polinomios cuadráticos en $K[X]$ 260
7.3.2 Polinomios en $\mathbb{C}[X]$ y el Teorema Fundamental del Álgebra. 263
7.3.3 Polinomios en $\mathbb{R}[X]$ 266
7.3.4 Polinomios en $\mathbb{Q}[X]$ 270
7.4 Ejercicios. 274

Capítulo 1

Conjuntos, Relaciones y Funciones.

1.1 Conjuntos.

1.1.1 Conjuntos y subconjuntos, pertenencia e inclusión.

Definición 1.1.1. (informal de conjunto y elementos.)

Un conjunto es una colección de objetos, llamados *elementos*, que tiene la propiedad que dado un objeto cualquiera, se puede decidir si ese objeto es un elemento del conjunto o no.

Ejemplos:

- $A = \{1, 2, 3\}$, $B = \{\triangle, \square\}$, $C = \{1, \{1\}, \{2, 3\}\}$.
- $\mathbb{N} = \{1, 2, 3, 4, \dots\}$ el conjunto de los números naturales.
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ el conjunto de los números enteros.
- $\mathbb{Q} = \{\frac{a}{b};\ a \in \mathbb{Z}, b \in \mathbb{N}\}$ el conjunto de los números racionales.
- $\mathbb{R}$ el conjunto de los números reales, $\mathbb{C}$ el conjunto de los números complejos.
- $\emptyset$ o $\{\ \}$ el *conjunto vacío*, o sea el conjunto que no posee ningún elemento.

Observación 1.1.2. El orden de los elementos no importa en un conjunto, y en un conjunto no se tiene en cuenta repeticiones de elementos.

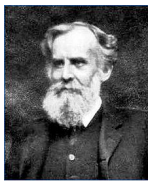
Se dice que cada elemento a de un conjunto A *pertenece* al conjunto A, y se nota $a \in A$. Si un objeto b no pertenece al conjunto A, se nota $b \notin A$.

Ejemplos:

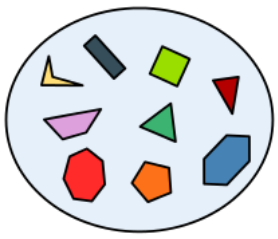
- Sea $A = \{1, 2, 3\}$: $1 \in A$, $2 \in A$, $4 \notin A$, $\{1, 2\} \notin A$, $\emptyset \notin A$.
- Sea $B = \{2, \{1\}, \{2, 3\}\}$: $\{1\} \in B$, $\{2, 3\} \in B$, $1 \notin B$, $3 \notin B$.

Para notar los conjuntos se suele reservar letras mayúsculas: A, B, ..., X, Y, ..., U, V, ...

Las definiciones comunes de un conjunto son por *extensión* (listando todos los elementos del conjunto entre las llaves { y }, cuando es posible hacerlo, o sea cuando el conjunto es finito) y por *comprensión* (a través de una propiedad que describe los elementos del conjunto, pero usualmente para eso se necesita la noción de subconjunto porque hay que dar un conjunto *referencial*, de donde se eligen los elementos). También presentamos en forma informal los conjuntos infinitos $\mathbb{N}$ y $\mathbb{Z}$ usando los puntos suspensivos ..., aunque esto no es muy riguroso: se puede dar una definición formal del conjunto $\mathbb{N}$ sin usar ..., y a partir de ello definir $\mathbb{Z}$ y $\mathbb{Q}$. El conjunto $\mathbb{R}$ se supone "conocido", aunque para él también se puede dar una construcción rigurosa (que no se verá en esta materia), y a través de $\mathbb{R}$ se puede definir $\mathbb{C}$ fácilmente.



Los conjuntos se suelen representar gráficamente por los llamados diagramas de Venn (por el lógico y filósofo británico *John Archibald Venn*, 1834–1923): simplemente se utiliza una circunferencia para representar el conjunto, y eventualmente en el interior sus elementos.



Aquí, está por ejemplo representado por medio de un diagrama de Venn un conjunto cuyos elementos son polígonos.

Definición 1.1.3. (Subconjuntos e Inclusión.)

Sea A un conjunto. Se dice que un conjunto B *está contenido en* A, y se nota $B \subseteq A$ (o también $B \subset A$), si todo elemento de B es un elemento

de A. En ese caso decimos también que B *está incluído en* A, o que B es un *subconjunto* de A. Si B no es un subconjunto de A se nota $B \not\subseteq A$ (o $B \not\subset A$).

Ejemplos:

- Sea $A = \{1, 2, 3\}$: $\{1\} \subseteq A$, $\{2, 3\} \subseteq A$, $\emptyset \subseteq A$, $A \subseteq A$, $\{3, 4\} \not\subseteq A$.
- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.
- $A \subseteq A$ y $\emptyset \subseteq A$ cualquiera sea el conjunto A.

O sea, B está incluído en A si para todo x, se tiene que si x pertenece a B entonces x pertenece a A, y B no está incluído en A si existe x perteneciendo a B tal que x no pertenece a A. Matemáticamente se escribe:

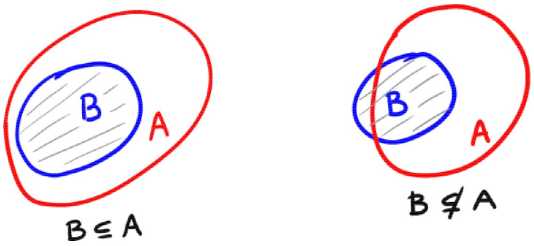
$$B \subseteq A \text{ si } \forall x,\ x \in B \Rightarrow x \in A \quad , \quad B \not\subseteq A \text{ si } \exists x \in B : x \notin A.$$

Aquí el símbolo "$\forall$" significa "*para todo*": la construcción "$\forall x, \ldots$" se lee "para todo x, se tiene $\ldots$", y el símbolo "$\exists$" significa "*existe*": la construcción "$\exists x \in B : \ldots$" se lee "existe x en B tal que $\ldots$". El símbolo "$\Rightarrow$" significa "*implica*": la construcción "$x \in B \Rightarrow x \in A$" se lee "$x$ en B implica x en A", o también "si x en B, entonces x en A" (significa que si ocurre lo primero, entonces obligatoriamente tiene que ocurrir lo segundo, veremos esto con más precisión por medio de las tablas de la lógica un poco más adelante).

Ejemplos de conjuntos dados por comprensión:

- $A = \{x \in \mathbb{R} : x \geq -2\}$, $B = \{k \in \mathbb{Z} : k \geq -2\}$.
- $P = \{n \in \mathbb{N} : n \text{ es par}\}$, $I = \{k \in \mathbb{Z} : k \text{ es impar}\}$.

Representación de Venn de $B \subset A$:



Observación 1.1.4. (Igualdad de conjuntos.)

$$A = B \iff A \subseteq B \text{ y } B \subseteq A.$$

Es decir $A = B$ si tienen exactamente los mismos elementos (sin importar el orden y sin tener en cuenta repeticiones de elementos). (Aquí, el símbolo "$\Leftrightarrow$" es el símbolo de la bi-implicación, que se lee "*si y sólo si*".)

Definición 1.1.5. (Conjunto de partes.)

Sea A un conjunto. El *conjunto de partes* de A, que se nota $\mathcal{P}(A)$, es el conjunto formado por todos los subconjuntos de A, o sea el conjunto cuyos *elementos* son los subconjuntos de A. Es decir

$$\mathcal{P}(A) = \{B : B \subseteq A\} \quad \text{o también} \quad B \in \mathcal{P}(A) \iff B \subseteq A.$$

Ejemplos:

- Sea $A = \{1, 2, 3\}$: $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$.
- Cualquiera sea el conjunto A, $\emptyset \in \mathcal{P}(A)$, $A \in \mathcal{P}(A)$.
- $\mathcal{P}(\emptyset) = \{\emptyset\}$, o sea el conjunto que tiene como único elemento al conjunto vacío.

1.1.2 Operaciones entre conjuntos.

Supondremos en todo lo que sigue que los conjuntos $A, B, C, \ldots$ que se consideran son subconjuntos de un mismo *conjunto referencial* (o de referencia) U (para poder "operar"). Esto también es generalmente indispensable al definir un conjunto *por comprensión*, como por ejemplo $P = \{n \in \mathbb{N} : n \text{ es un número par }\}$, o $I = \{x \in \mathbb{R} : x \leq 2\} = [-\infty, 2)$, que no es lo mismo que $J = \{x \in \mathbb{N} : x \leq 2\} = \{1, 2\}$.

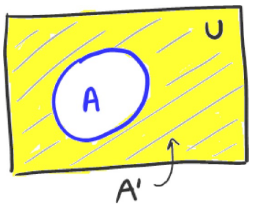
Complemento ^{c}: Sea A subconjunto de un conjunto referencial U. El *complemento* de A (en U) es el conjunto de los elementos de U que no pertenecen a A, que se suele notar con A' o A^c (aquí usaremos la notación A^c que es la que aparece en la práctica). Es decir

$$A^c = \{x \in U : x \notin A\}.$$

Ejemplos:

- Si $U = \{1, 2, 3\}$ y $A = \{2\}$, entonces $A^c = \{1, 3\}$.
- Si $U = \mathbb{N}$ y $A = \{2\}$, entonces $A^c = \{n \in \mathbb{N}, n \neq 2\}$.
- Si $U = \mathbb{N}$ y $P = \{n \in \mathbb{N} : n \text{ es un número par }\}$, entonces $P^c = \{n \in \mathbb{N} : n \text{ es un número impar }\}$.
- Para el conjunto referencial U, se tiene $\emptyset^c = U$ y $U^c = \emptyset$.
- $(A^c)^c = A$.

Representación de Venn del complemento:



Unión $\cup$: Sean A, B subconjuntos de un conjunto referencial U. La *unión* de A y B es el conjunto $A \cup B$ de los elementos de U que pertenecen a A o a B. Es decir

$$A \cup B = \{x \in U : x \in A \text{ o } x \in B\}.$$

Notemos que este "o" involucrado en la definición de la unión es no excluyente, es decir si un elemento está en A y en B, está en la unión por estar en al menos alguno de los dos.

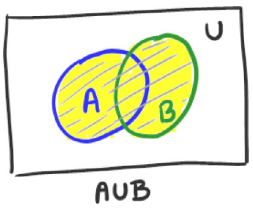
Ejemplos:

- Si $A = \{1, 2, 3, 5, 8\}$ y $B = \{3, 4, 5, 10\} \subseteq U = \{1, \ldots, 10\}$, entonces $A \cup B = \{1, 2, 3, 4, 5, 8, 10\}$.
- Si $I = \{x \in \mathbb{R} : x \leq 2\} = (-\infty, 2]$ y $J = \{x \in \mathbb{R} : -10 \leq x < 10\} = [-10, 10) \subseteq U = \mathbb{R}$, entonces $I \cup J = \{x \in \mathbb{R} : x < 10\} = (-\infty, 10)$.
- Cualesquiera sean A y B, se tiene $A \cup B = B \cup A$ (conmutatividad), $A \cup \emptyset = A$, $A \cup U = U$, $A \cup A^c = U$.

  Probemos por ejemplo la afirmación $A \cup A^c = U$: Hay que probar las dos inclusiones $A \cup A^c \subseteq U$ y $U \subseteq A \cup A^c$.

  - $A \cup A^c \subseteq U$: Sea $x \in A \cup A^c$; si $x \in A$ entonces $x \in U$ pues $A \subseteq U$, y si $x \in A^c$, entonces $x \in U$ pues $A^c \subseteq U$; por lo tanto $A \cup A^c \subseteq U$.
  - $U \subseteq A \cup A^c$: Sea $x \in U$; entonces $x \in A$ o $x \notin A$. Si $x \in A$, entonces $x \in A \cup A^c$, y si $x \notin A$, por definición $x \in A^c$ y luego $x \in A \cup A^c$; por lo tanto $U \subset A \cup A^c$.

Representación de Venn de la unión:



Intersección $\cap$. Sean A, B subconjuntos de un conjunto referencial U. La *intersección* de A y B es el conjunto $A \cap B$ de los elementos de U que pertenecen tanto a A como a B. Es decir

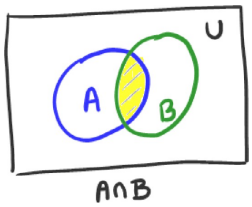
$$A \cap B = \{x \in U : x \in A \text{ y } x \in B\}.$$

Ejemplos:

- Sean $A = \{1, 2, 3, 5, 8\}$, $B = \{3, 4, 5, 10\} \subseteq U = \{1, \ldots, 10\}$. Entonces $A \cap B = \{3, 5\}$.
- Sean $I = \{x \in \mathbb{R} : x \leq 2\} = (-\infty, 2]$, $J = \{x \in \mathbb{R} : -10 \leq x < 10\} = [-10, 10) \subseteq U = \mathbb{R}$. Entonces $I \cap J = \{x \in \mathbb{R} : -10 \leq x \leq 2\} = [-10, 2]$.
- Cualesquiera sean A y B, se tiene $A \cap B = B \cap A$ (conmutatividad), $A \cap \emptyset = \emptyset$, $A \cap U = A$, $A \cap A^c = \emptyset$.

Cuando $A \cap B = \emptyset$, se dice que A y B son conjuntos *disjuntos*.

Representación de Venn de la intersección:



Podemos notar que a diferencia del complemento, la unión y la intersección no dependen del conjunto referencial U, siempre que A y B estén incluídos en U.

Proposición 1.1.6. (Leyes de De Morgan y distributivas.)

Sean A, B, C conjuntos dentro de un conjunto referencial U. Entonces

- **Leyes de De Morgan**, *por el matemático británico* Augustus De Morgan, *1806-1871:*

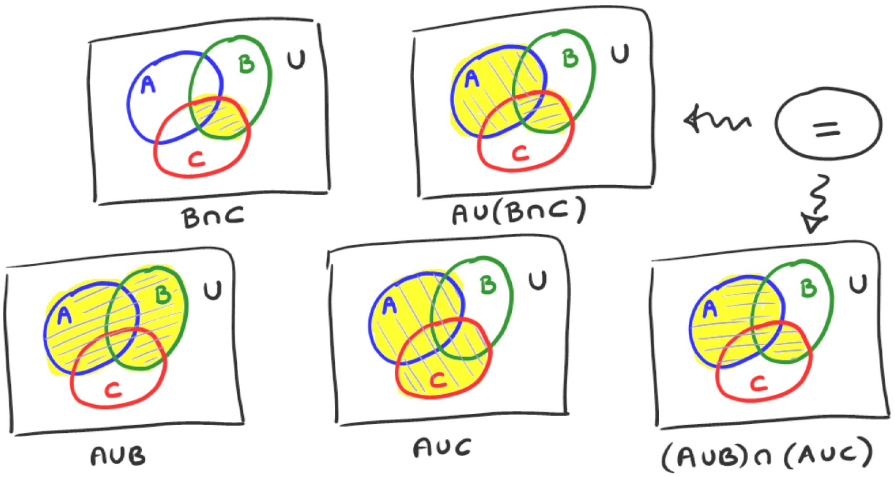
$$(A \cup B)^c = A^c \cap B^c \quad y \quad (A \cap B)^c = A^c \cup B^c.$$

- **Leyes distributivas**:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad y \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Demostración. Haremos la demostración de $(A \cup B)^c = A^c \cap B^c$ en forma directa, y la demostración de $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ con los diagramas de Venn (donde es necesario explicitar todos los pasos). Las otras demostraciones quedan para el lector.

- $(A \cup B)^c = A^c \cap B^c$: Tenemos que probar la doble inclusión.
  - $(A \cup B)^c \subseteq A^c \cap B^c$: Sea $x \in (A \cup B)^c$. Entonces $x \notin A \cup B$. Como $A \cup B = \{x \in U : x \in A \text{ o } x \in B\}$, $x \notin A$ y $x \notin B$, es decir $x \in A^c$ y $x \in B^c$, y por lo tanto $x \in A^c \cap B^c$.
  - $A^c \cap B^c \subseteq (A \cup B)^c$: Sea $x \in A^c \cap B^c$. Entonces $x \in A^c$ y $x \in B^c$. Es decir $x \notin A$ y $x \notin B$, lo que significa que x no está ni en A ni en B, por lo tanto no está en la unión: $x \notin A \cup B$. O sea $x \in (A \cup B)^c$.
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$:



(Esta demostración con diagrama de Venn es válida porque solo involucra tres conjuntos y el diagrama expresa todas las posibilidades de pertenencia de elementos en esos tres conjuntos (8 posibilidades: x en A pero no en B ni en C, x en A y en B pero no en C, x en ninguno de los tres conjuntos, etc.). Si fueran 4 conjuntos, no hay forma en un dibujo de expresar todas las posibilidades para un elemento x, que son en ese caso 16, pero esto se arregla con las tablas de verdad como veremos enseguida.)

De las operaciones básicas se derivan las operaciones siguientes:

Diferencia $-$: $A - B := A \cap B^c$, es decir

$$x \in A - B \iff x \in A \text{ y } x \in B^c \iff x \in A \text{ y } x \notin B.$$

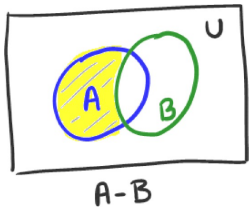
Es decir, $A - B$ es el conjunto de los elementos de A que no son elementos de B:

$$A - B = \{a \in A : a \notin B\}.$$

Ejemplos:

- Sean $A = \{1, 2, 3, 5, 8\}$, $B = \{3, 4, 5, 10\} \subseteq U = \{1, \ldots, 10\}$. Entonces $A - B = \{1, 2, 8\}$ y $B - A = \{4, 10\}$.
- Sean $I = (-\infty, 2]$, $J = [-10, 10) \subseteq U = \mathbb{R}$. Entonces $I - J = [-\infty, -10)$ y $J - I = (2, 10]$.
- Siempre $A - \emptyset = A$, $A - U = \emptyset$, $A - A = \emptyset$, $A - A^c = A$. Pero $A - B \neq B - A$ en general.

Representación de Venn de la diferencia:



Diferencia simétrica $\triangle$: $A \triangle B$ es el conjunto de los elementos de U que pertenecen a A o a B pero no a los dos a la vez. Es decir

$$A \triangle B = \{c \in U : (c \in A \text{ y } c \notin B) \text{ o } (c \in B \text{ y } c \notin A)\}.$$

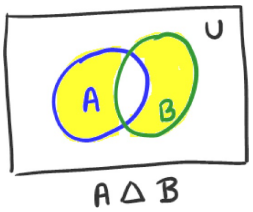
Vale

$$A \triangle B = (A - B) \cup (B - A) = (A \cap B^c) \cup (B \cap A^c) = (A \cup B) - (A \cap B).$$

Ejemplos:

- Sean $A = \{1, 2, 3, 5, 8\}$, $B = \{3, 4, 5, 10\} \subseteq U = \{1, \ldots, 10\}$. Entonces $A \triangle B = \{1, 2, 4, 8, 10\}$.
- Sean $I = (-\infty, 2]$, $J = [-10, 10) \subseteq U = \mathbb{R}$. Entonces $I \triangle J = [-\infty, -10) \cup (2, 10]$.
- Siempre $A \triangle B = B \triangle A$ (simetría), $A \triangle \emptyset = A$, $A \triangle U = A^c$, $A \triangle A = \emptyset$, $A \triangle A^c = U$.

Representación de Venn de la diferencia simétrica:



1.1.3 Tablas de verdad de la lógica proposicional.

Otra forma de visualizar esas operaciones es por medio de las tablas de verdad de la lógica proposicional, aplicadas a las operaciones de conjuntos.

Se vio que las operaciones básicas de conjuntos están definidas por medio del *no* (para el complemento), del *o no excluyente* para la unión, del *y* para la intersección, y del *o excluyente* para la diferencia simétrica. Estos se llaman conectores lógicos: $\neg$ ("no", o "NOT"), $\vee$ ("o" no excluyente, u "OR"), $\wedge$ ("y", o "AND"), $\veebar$ ("o excluyente", u "XOR"), y se les puede agregar $\Rightarrow$ (implica, o si ... entonces) y $\Leftrightarrow$ (si y solo si).

Tablas de verdad de los conectores lógicos:

Sean p, q proposiciones, es decir afirmaciones que son o bien verdaderas o bien falsas, como por ejemplo "hoy es domingo", o "$\forall\, n \in \mathbb{N}, n \geq 3$", o "los perros son mamíferos". Las tablas de verdad de los conectores lógicos son las siguientes:

p	$\neg p$
V	F
F	V

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

p	q	$p \veebar q$
V	V	F
V	F	V
F	V	V
F	F	F

p	q	$p \Rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

p	q	$p \Leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

.

(La definición formal de $p \Rightarrow q$ es $\neg p \vee q$.)

Las tablas de los conectores lógicos se relacionan con las tablas de las operaciones de conjuntos: Dados A, B conjuntos incluídos en un un conjunto referencial U, y dado un elemento $x \in U$, se puede pensar en las proposiciones p y q asociadas a A, B (y x) definidas por

$$p: \text{ "}x \in A\text{"} \qquad \text{y} \qquad q: \text{ "}x \in B\text{".}$$

Notemos que la proposición p es verdadera si y sólo el elemento x de U pertenece al subconjunto A, y del mismo modo, la proposición q es verdadera si y sólo el elemento x de U pertenece al subconjunto B. Dado un elemento $x \in U$ cualquiera, puede pertenecer a A o no. Esto describe dos posibilidades para cualquier elemento de U. Ahora bien, si tenemos dos conjuntos $A, B \subseteq U$, hay 4 posibilidades para un $x \in U$: estar en A y en B, no en A pero sí en B, en A pero no en B, y finalmente ni en A ni en B. Así describimos todas las posibilidades para un elemento "genérico" de U. Las tablas de verdad de las operaciones de conjuntos se corresponden con las tablas de verdad de los conectores lógicos de la manera siguiente:

<u>*Tablas de verdad de las operaciones de conjuntos:*</u>

- *Complemento:* El complemento A^c de A en U se corresponde con $\neg p$.
- *Unión:* La unión $A \cup B$ se corresponde con $p \vee q$.
- *Intersección:* La intersección $A \cap B$ se corresponde con $p \wedge q$.
- *Diferencia simétrica:* La diferencia simétrica $P \triangle Q$ se corresponde con $p \veebar q$.
- *Inclusión:* La inclusión $A \subseteq B$ se corresponde con $p \Rightarrow q$.
- *Igualdad:* La igualdad $A = B$ se corresponde con $p \Leftrightarrow q$.

A	A^c
V	F
F	V

A	B	$A \cup B$
V	V	V
V	F	V
F	V	V
F	F	F

A	B	$A \cap B$
V	V	V
V	F	F
F	V	F
F	F	F

A	B	$A \triangle B$
V	V	F
V	F	V
F	V	V
F	F	F

A	B	$A \subseteq B$
V	V	V
V	F	F
F	V	V
F	F	V

A	B	$A = B$
V	V	V
V	F	F
F	V	F
F	F	V

.

<u>*Ejemplos:*</u> (*de afirmaciones sobre conjuntos por medio de tablas)*

- La tabla de la diferencia $A - B$ se obtiene de la definición $A - B = A \cap B^c$:

A	B	B^c	$A \cap B^c = A - B$
V	V	F	F
V	F	V	V
F	V	F	F
F	F	V	F

.

- Retomemos la primer ley de de Morgan, que demostramos más arriba, $(A \cup B)^c = A^c \cap B^c$:

A	B	$A \cup B$	$(A \cup B)^c$	A^c	B^c	$A^c \cap B^c$
V	V	V	F	F	F	F
V	F	V	F	F	V	F
F	V	V	F	V	F	F
F	F	F	V	V	V	V

.

Se observa que las columas correspondientes a $(A \cup B)^c$ y a $A^c \cap B^c$ son exactamente las mismas, o sea los elementos pertenecen a $(A \cup B)^c$ si y solo si pertenecen a $A^c \cap B^c$. Luego los dos conjuntos son iguales.

- $A \cap B \subseteq (B - C) \cup (A \cap C)$:

A	B	C	$A \cap B$	$B - C$	$A \cap C$	$(B - C) \cup (A \cap C)$	$A \cap B \subseteq (B - C) \cup (A \cap C)$
V	V	V	V	F	V	V	V
V	V	F	V	V	F	V	V
V	F	V	F	F	V	V	V
V	F	F	F	F	F	F	V
F	V	V	F	F	F	F	V
F	V	F	F	V	F	V	V
F	F	V	F	F	F	F	V
F	F	F	F	F	F	F	V

.

Vemos que la columna correspondiente a la inclusión es Verdadera siempre, lo que implica que es verdad que $A \cap B \subseteq (B - C) \cup (A \cap C)$.

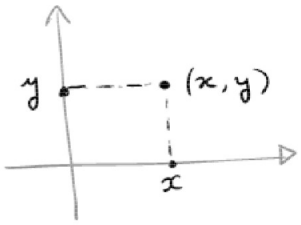
- $A^c \cap B = B \Rightarrow A \cap B = \emptyset$:

A	B	A^c	$A^c \cap B$	$A \cap B$
V	V	F	F	V
V	F	F	F	F
F	V	V	V	F
F	F	V	F	F

.

Comparando la 2da y la 4ta columna, se ve que $A^c \cap B = B$ cuando no se está en la primera fila, o sea cuando no se está en el caso de algún $x \in A$, $x \in B$. Por lo tanto esta fila no cumple con la hipótesis y se la olvida. Para las demás filas, $A \cap B$ da siempre Falso, es decir, no existe ningún elemento $x \in A \cap B$. Por lo tanto $A \cap B = \emptyset$.

1.1.4 Producto cartesiano.



El nombre *producto cartesiano* fue puesto en honor al matemático, físico y filósofo francés *René Descartes*, 1596-1650. El plano euclideo $\mathbb{R}^2 = \{(x, y);\, x, y \in \mathbb{R}\}$ representado mediante los ejes cartesianos es el plano donde constantemente dibujamos los gráficos de las funciones.

Definición 1.1.7. (Producto cartesiano.)

Sean A, B conjuntos. El producto cartesiano de A con B, que se nota $A \times B$, es el conjunto de *pares ordenados*

$$A \times B := \{(x, y) : x \in A, y \in B\}.$$

Ejemplos:

- Sean $A = \{1, 2, 3\}$, $B = \{a, b\}$. Entonces

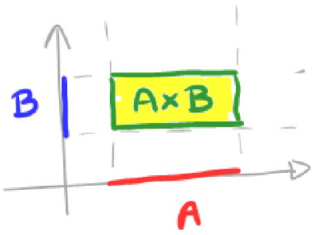
$$\begin{aligned} A \times B &= \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}, \\ B \times A &= \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}, \\ B \times B &= \{(a, a), (a, b), (b, a), (b, b)\}. \end{aligned}$$

- Si $A = B = \mathbb{R}$, entonces $\mathbb{R} \times \mathbb{R}$ es el plano real $\mathbb{R}^2$.
- $A \times \emptyset = \emptyset$, $\emptyset \times B = \emptyset$.
- Si $A \neq B$ son ambos no vacíos, entonces $A \times B \neq B \times A$.
- Sean $A \subseteq U$, $B \subseteq V$ entonces $A \times B \subseteq U \times V$. Analizar si vale $(A \times B)^c = A^c \times B^c$.

De la misma forma se puede definir el producto cartesiano de n conjuntos $A_1, \ldots, A_n$ como el conjunto de n-uplas ordenadas:

$$A_1 \times \cdots \times A_n := \{(x_1, \ldots, x_n) : x_1 \in A_1, \ldots, x_n \in A_n\}.$$

Representación del producto cartesiano:



1.2 Relaciones.

En lo que sigue daremos la formalización matemática de la noción de *relación* que usamos constantemente en el lenguaje.

Definición 1.2.1. (Relación.)

Sean A y B conjuntos. Una *relación* $\mathcal{R}$ *de* A *en* B es un subconjunto cualquiera $\mathcal{R}$ del producto cartesiano $A \times B$. Es decir $\mathcal{R}$ es una relación de A en B si $\mathcal{R} \in \mathcal{P}(A \times B)$.

Ejemplos:

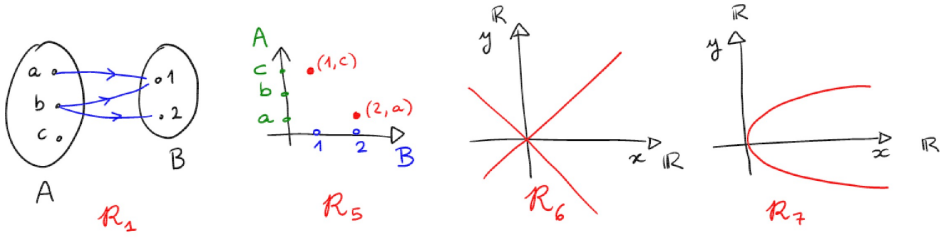
- Sean $A = \{a, b, c\}$, $B = \{1, 2\}$. Entonces $\mathcal{R}_1 = \{(a, 1), (b, 1), (b, 2)\}$, $\mathcal{R}_2 = \{(a, 2), (b, 2), (c, 1), (c, 2)\}$, $\mathcal{R}_3 = \emptyset$ y $\mathcal{R}_4 = A \times B$ son ejemplos de relaciones de A en B, y $\mathcal{R}_5 = \{(1, c), (2, a)\}$ es un ejemplo de relación de B en A (notar que importa el orden).

- Sean $A = B = \mathbb{R}$: $\mathcal{R}_6 = \{(x, y) \in \mathbb{R}^2 : x^2 = y^2\}$ y $\mathcal{R}_7 = \{(x, y) \in \mathbb{R}^2 : x = y^2\}$ son relaciones de $\mathbb{R}$ en $\mathbb{R}$, o, como veremos luego, relaciones en $\mathbb{R}$.

Dados $x \in A$, $y \in B$ y una relación $\mathcal{R}$ de A en B, se dice que x *está relacionado con* y (por la relación $\mathcal{R}$) si $(x, y) \in \mathcal{R}$. En ese caso se escribe $x \mathcal{R} y$. Si x no está relacionado con y, es decir $(x, y) \notin \mathcal{R}$, se escribe $x \not\mathcal{R} y$.

En los ejemplos arriba, se tiene $b \mathcal{R}_1 1$ pero $a \not\mathcal{R}_1 2$, $x \mathcal{R}_4 y$, $\forall x \in A, y \in B$, y $\nexists x \in A, \nexists y \in B$ tal que $x \mathcal{R}_3 y$. También, $-2 \mathcal{R}_6 2$ y $4 \mathcal{R}_7 -2$.

Posibles representaciones gráficas de las relaciones:



1.2.1 Relaciones en un conjunto.

En esta sección consideramos *relaciones de un conjunto en sí mismo.*

Definición 1.2.2. (Relación en un conjunto.)

Sea A un conjunto. Se dice que $\mathcal{R}$ es una relación en A cuando $\mathcal{R} \subseteq A \times A$.

Ejemplos:

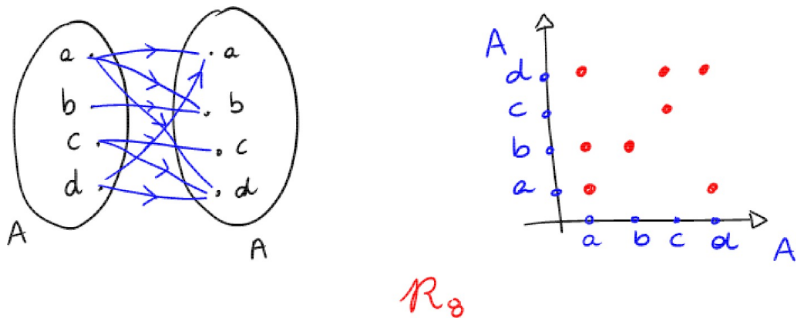
- Las relaciones $\mathcal{R}_6$ y $\mathcal{R}_7$ arriba son relaciones en el conjunto $\mathbb{R}$.
- La igualdad de elementos siempre es una relación en cualquier conjunto A:

$$\mathcal{R} = \{(x, x),\ x \in A\}, \quad \text{es decir } \forall\, x, y \in A:\ x\,\mathcal{R}\,y \Leftrightarrow x = y.$$

- $\leq$ es una relación en $\mathbb{R}$, y $\subseteq$ es una relación en $\mathcal{P}(A)$, cualquiera sea el conjunto A.
- Sea $A = \{a, b, c, d\}$, entonces

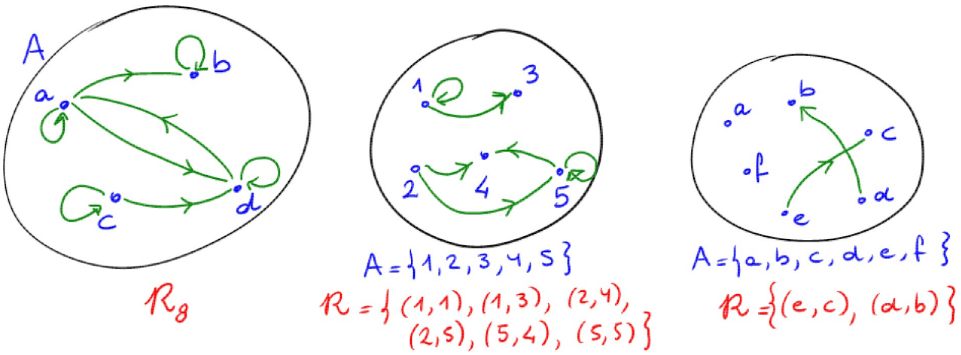
$$\mathcal{R}_8 = \{(a,a), (a,b), (a,d), (b,b), (c,c), (c,d), (d,a), (d,d)\}$$

es una relación en A, que según lo que vimos arriba se puede representar de las siguientes maneras:



Sin embargo, cuando el conjunto A es finito (como en este caso), una relación $\mathcal{R}$ en A se puede representar también por medio de un *grafo dirigido*, o sea un conjunto de puntos (llamados *vértices*, que son los elementos del conjunto A) y un conjunto de *flechas* entre los vértices, que se corresponden con los elementos relacionados: se pone una flecha (que parte de x y llega a y) para cada elemento $(x, y) \in \mathcal{R}$, es decir cada vez que $x \mathcal{R} y$.

Ejemplos:



La teoría de grafos juega un rol esencial en matemática y computación

Las relaciones en un conjunto dado son particularmente importantes, y algunas de las propiedades que pueden cumplir merecen un nombre.

Definición 1.2.3. (Relación reflexiva, simétrica, antisimétrica y transitiva.)

Sean A un conjunto y $\mathcal{R}$ una relación en A.

- Se dice que $\mathcal{R}$ es *reflexiva* si $(x, x) \in \mathcal{R}, \forall\, x \in A$ (dicho de otra manera, $x \mathcal{R} x, \forall\, x \in A$). En términos del grafo de la relación, $\mathcal{R}$ es reflexiva si en cada vértice hay una flecha que es un "bucle", es decir que parte de él y llega a él.

- Se dice que $\mathcal{R}$ es *simétrica* si cada vez que un par $(x, y) \in \mathcal{R}$, entonces el par "simétrico" $(y, x) \in \mathcal{R}$ también (dicho de otra manera, $\forall\, x, y \in A,\ x \mathcal{R} y \Rightarrow y \mathcal{R} x$). En términos del grafo de la relación, $\mathcal{R}$ es simétrica si por cada flecha que une dos vértices en un sentido, hay una flecha (entre los mismos vértices) en el sentido opuesto.

- Se dice que $\mathcal{R}$ es *antisimétrica* si cada vez que un par $(x, y) \in \mathcal{R}$ con $x \neq y$, entonces el par $(y, x) \notin \mathcal{R}$ (dicho de otra manera, $\forall\, x, y \in A,\ x \mathcal{R} y$ e $y \mathcal{R} x \Rightarrow x = y$). En términos del grafo de la relación, $\mathcal{R}$ es antisimétrica si no hay ningún par de flechas en sentidos opuestos que unen dos vértices distintos.

- Se dice que $\mathcal{R}$ es *transitiva* si para toda terna de elementos $x, y, z \in A$ tales que $(x, y) \in \mathcal{R}$ e $(y, z) \in \mathcal{R}$, se tiene que $(x, z) \in \mathcal{R}$ también (dicho de otra manera, $\forall\, x, y, z \in A,\ x \mathcal{R} y$ e $y \mathcal{R} z \ \Rightarrow\ x \mathcal{R} z$). En términos del grafo de la relación, $\mathcal{R}$ es transitiva si hay un "camino directo" por cada "camino con paradas".

<u>*Ejemplos:*</u>

- La relación $\mathcal{R}_8$ de arriba es reflexiva, pero no es simétrica ni antisimétrica, y tampoco transitiva como se ve en el grafo arriba: están todos los "bucles" (es reflexiva), está por ejemplo la flecha $a \to b$ pero no la vuelta $b \to a$ (no es simétrica), están las flechas $a \to d$ y $d \to a$ (no es antisimétrica) y están las flechas $c \to d$ y $d \to a$ pero no el camino corto $c \to a$ (no es transitiva).

- $\mathcal{R}_6$ es reflexiva, pues $\forall\, x \in \mathbb{R}$, se tiene $x \mathcal{R}_6 x$ pues $x^2 = x^2$. Es simétrica pues $\forall\, x, y \in \mathbb{R}$, se tiene que si $x \mathcal{R}_6 y$, es decir $x^2 = y^2$, entonces $y^2 = x^2$, es decir $y \mathcal{R}_6 x$. No es antisimétrica pues no es cierto que $x \mathcal{R}_6 y$ e $y \mathcal{R}_6 x$ implica $x = y$: por ejemplo para $x = 1$ e $y = -1$ se tiene $x^2 = y^2$ e $y^2 = x^2$. Y es transitiva pues $\forall\, x, y, z \in \mathbb{R}$, $x^2 = y^2$ e $y^2 = z^2$ implica $x^2 = z^2$.

  ¿Cómo se ve que una relación es reflexiva en la representación gráfica del producto cartesiano? ¿Y simétrica?

  ¿Puede ser una relación simétrica y antisimétrica a la vez? Si sí, ¿en qué caso?

- $=$ en A, con A un conjunto, es una relación reflexiva, simétrica y transitiva.

- $\leq$ en $\mathbb{R}$ es una relación reflexiva pues para todo $x \in \mathbb{R}$, se tiene $x \leq x$, no es simétrica pues en general $x \leq y$ no implica $y \leq x$: por ejemplo para $x = 1$ e $y = 2$. Pero es antisimétrica pues si $x \leq y$ e $y \leq x$, entonces $x = y$. Y es transitiva pues $x \leq y$ e $y \leq z$ implica $x \leq z$.

- Mostrar que $\subseteq$ en $\mathcal{P}(A)$ es una relación reflexiva, antisimétrica y transitiva.

- $\mathcal{R}_7$ no es reflexiva, pues $\exists\, x \in \mathbb{R}$ tal que $x \not\mathcal{R}_7 x$, es decir $x \neq x^2$ (por ejemplo $x = 2$). Tampoco es simétrica porque $x = y^2$ no implica en general $y = x^2$ (por ejemplo para $x = 4, y = 2$). ¿Es antisimétrica? Supongamos $x, y \in \mathbb{R}$ tales que $x = y^2$ e $y = x^2$, por lo tanto $x = x^4$, lo que implica $x(x^3 - 1) = 0$, es decir $x = 0$ o $x = 1$ (por estar en $\mathbb{R}$, ¡ojo!), y luego en el caso $x = 0$ se tiene $y = x^2 = 0^2 = 0 = x$, y en el caso $x = 1$ se tiene $y = x^2 = 1^2 = 1 = x$ también, o sea es

antisimétrica nomás. Finalmente $\mathcal{R}_7$ no es transitiva pues $x = y^2$ e $y = z^2$ implica $x = z^4$ que no es igual a z^2 en general, por ejemplo tomando $x = 16$, $y = 4$, $z = 2$.

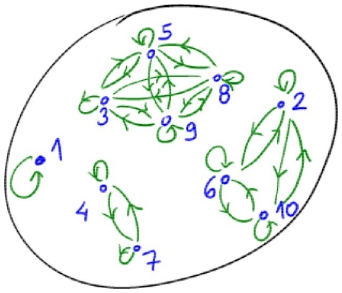
Definición 1.2.4. (Relación de equivalencia y relación de orden.)

Sean A un conjunto y $\mathcal{R}$ una relación en A.

- Se dice que una relación $\mathcal{R}$ en un conjunto A es una *relación de equivalencia* cuando es una relación reflexiva, simétrica y transitiva.
- Se dice que una relación $\mathcal{R}$ en un conjunto A es una *relación de orden* cuando es una relación reflexiva, antisimétrica y transitiva.

Ejemplos:

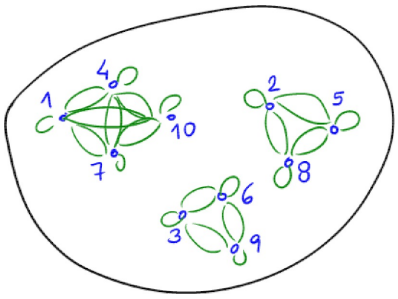
- Las relaciones $=$ en un conjunto A y $\mathcal{R}_6$ en $\mathbb{R}$ son relaciones de equivalencia, las relaciones $\leq$ en $\mathbb{R}$ y $\subseteq$ en $\mathcal{P}(A)$ son relaciones de orden.
- La relación $\sim$ descrita con el grafo siguiente es una relación de equivalencia, pues en cada uno de los subgrafos formados, están todas las flechas posibles (cada subgrafo es "completo").



Las relaciones de equivalencia juegan un rol muy importante en matemática, porque de algún modo funcionan como una generalización de la igualdad (que es el ejemplo más simple de relación de equivalencia): clasifican, a través de las *clases de equivalencia*, a los elementos del conjunto en subconjuntos donde se los considera "iguales" en algún sentido. Veamoslo primero en un ejemplo.

Ejemplo:

Sea la relación $\sim$ siguiente en el conjunto $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$: $x \sim y$ si al dividir x e y por 3 tienen el mismo resto. Por ejemplo $1 \sim 4$ pues al dividirlos por 3 tienen resto 1, y $6 \sim 9$ porque al dividirlos por 3 ambos tienen resto 0. El grafo de la relación es:



Esta relación es claramente una relación de equivalencia. La clase de equivalencia de $x \in A$ es el subconjunto de A formado por todos los elementos y de A relacionados con x, y se nota $\overline{x}$. Aquí,

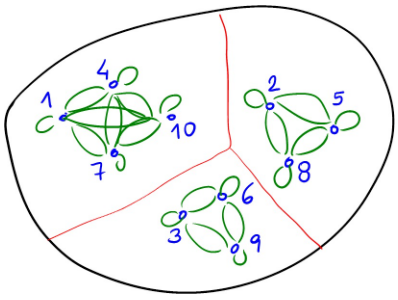
$$\overline{1} = \{1, 4, 7, 10\} = \overline{4} = \overline{7} = \overline{10},\ \overline{2} = \{2, 5, 8\} = \overline{5} = \overline{8},\ \overline{3} = \{3, 6, 9\} = \overline{6} = \overline{9}.$$

Estas clases de equivalencia clasifican entonces los elementos de A según su resto al dividir por 3: dos elementos que están en la misma clase de equivalencia tienen mismo resto, y dos elementos en distintas clases tienen restos distintos.

Ahora bien, observemos que los tres subconjuntos obtenidos son disjuntos dos a dos (y su unión da todo el conjunto A). Podemos considerar el conjunto de clases de equivalencia:

$$\left\{\overline{1}, \overline{2}, \overline{3}\right\} = \left\{\{1, 4, 7, 10\}, \{2, 5, 8\}, \{3, 6, 9\}\right\}$$

que tiene 3 elementos (que caracterizan los posibles restos al dividir por 3). Lo que hicimos fue "partir" al conjunto A en tres subconjuntos, que son las tres clases de equivalencia.



Definición 1.2.5. (Clases de equivalencia.)

Sean A un conjunto y $\sim$ una relación de equivalencia en A. Para cada $x \in A$, la *clase de equivalencia de* x es el conjunto

$$\overline{x} = \{y \in A : y \sim x\} \subseteq A.$$

Observemos que debido a la simetría, podríamos haber definido $\overline{x} = \{y \in A : x \sim y\}$ y daría el mismo subconjunto de A. También, debido a la reflexividad, siempre tenemos $x \in \overline{x}$ (pues $x \sim x$). Finalmente la simetría y transitividad muestran que si $y \in \overline{x}$ y $z \in \overline{x}$, entonces $y \sim z$ (pues $y \sim x$ y $x \sim z$ implica $y \sim z$), es decir todos los elementos de una clase de equivalencia están relacionados entre sí.

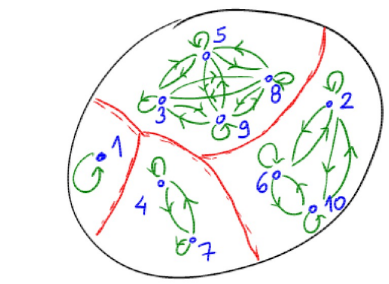
Proposición 1.2.6. (Propiedad fundamental de las clases de equivalencia.)

Sean A un conjunto y $\sim$ una relación de equivalencia en A. Sean $x, y \in A$. Entonces, o bien $\overline{x} \cap \overline{y} = \emptyset$, o bien $\overline{x} = \overline{y}$.

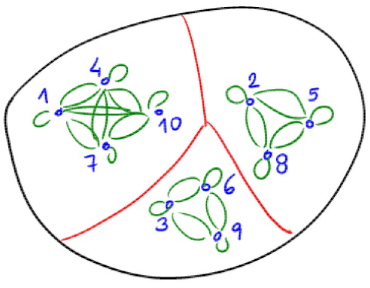
Observación 1.2.7. En la proposición anterior, nuestro enunciado es que alguna de las proposiciones "$\overline{x} \cap \overline{y} = \emptyset$", o "$\overline{x} = \overline{y}$" es verdadera. Si llamamos p a la primera y q a la segunda, queremos probar que siempre es verdadera $p \vee q$. Si p es verdadera, también lo es $p \vee q$, luego basta probar que si no es verdadera p (es decir es falsa p) entonces debe ser verdadera q (que es lo que haremos a continuación). El rol de p y de q son intercambiables, con lo cual si resultase mas fácil también podemos suponer que si es falsa q entonces debe ser verdadera p.

Demostración. Supongamos que $\overline{x} \cap \overline{y} \neq \emptyset$. Existe entonces $z \in A$ tal que $z \in \overline{x} \cap \overline{y}$, es decir $z \sim x$ y $z \sim y$. Pero por simetría, $x \sim z$ también, y por transitividad, $x \sim z$ y $z \sim y$ implica $x \sim y$, esto quiere decir que $x \in \overline{y}$ (y por simetría, $y \in \overline{x}$). Pero luego, todo elemento $z' \in \overline{x}$ satisface $z' \sim x$, y como $x \sim y$, se tiene $z' \sim y$, o sea $z' \in \overline{y}$. Es decir, hemos probado que $\overline{x} \subseteq \overline{y}$, y del mismo modo se prueba $\overline{y} \subseteq \overline{x}$. Por lo tanto $\overline{x} = \overline{y}$. □

Así, logramos partir el conjunto A en una unión disjunta de subconjuntos no vacíos, sus clases de equivalencia. Eso se se llama hacer una *partición* de A:



Partición: $\{\{1\}, \{2,6,10\}, \{3,5,8,9\}, \{4,7\}\}$



Partición: $\{\{1,4,7,10\}, \{2,5,8\}, \{3,6,9\}\}$

Ejemplos:

- Para la relación $=$ en A, las clases de equivalencia son simplemente $\overline{x} = \{x\}$, y para la relación $\mathcal{R}_6$ en $\mathbb{R}$, las clases de equivalencia son $\overline{x} = \{x, -x\}$, $\forall\, x \in \mathbb{R}$, o sea todas las clases tienen dos elementos de la forma $\pm x$, salvo la clase del 0 que tiene solo el elemento 0. Esta relación clasifica a los números reales según su módulo. En cada clase podemos elegir un *representante*, es decir un elemento en la clase que "representa" la clase: por ejemplo aquí podemos elegir en casa clase al $x \geq 0$ como representante.

- Miremos el conjunto L de las rectas del plano, con relación de equivalencia $/\!/$ (ser paralelo). Cada clase consiste de rectas todas paralelas entre sí. Esta relación clasifica a las rectas según su dirección. En cada clase de rectas paralelas podemos elegir como representante la recta que pasa por el 0.

- Si uno quiere describir el conjunto $\mathbb{Q}$ de números racionales sin repetir elementos, la forma correcta de hacerlo es por medio de las clases de equivalencia de la siguiente relación $\sim$ en $\mathbb{Z} \times \mathbb{N}$: Dados $(k_1, n_1), (k_2, n_2) \in \mathbb{Z} \times \mathbb{N}$,

$$(k_1, n_1) \sim (k_2, n_2) \iff k_1 n_2 = k_2 n_1.$$

  Verificar que es una relación de equivalencia. Se tiene $(k_1, n_1) \sim (k_2, n_2) \Leftrightarrow \frac{k_1}{n_1} = \frac{k_2}{n_2}$, o sea $\frac{k_1}{n_1}$ y $\frac{k_2}{n_2}$ determinan el mismo número racional: todos los elementos de una clase de equivalencia $\overline{(k, n)}$ dada determinan el mismo número racional $\frac{k}{n}$. En cada clase podemos elegir como representante el par (k, n) con k y n coprimos.

Proposición 1.2.8. (Relaciones de equivalencia y particiones.)

Sea A un conjunto. Hay una manera natural de asociarle a una relación de equivalencia en A una partición de A. Recíprocamente, a toda partición se le puede asociar una relación de equivalencia, y estas asociaciones son inversas una de la otra.

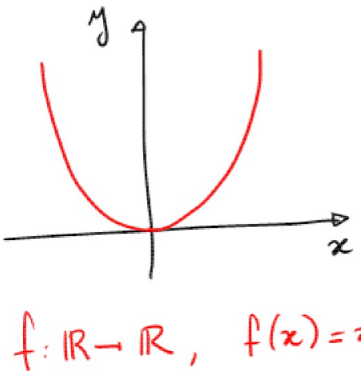
Demostración. Si $\sim$ es una relación de equivalencia, como vimos anteriormente podemos considerar las clases de equivalencia de los elementos de A. Cada clase de equivalencia es un subconjunto, y dos de estos subconjuntos distintos son disjuntos. Como el conjunto es la unión de las clases, obtenemos una partición.

Recíprocamente, dada una partición, definimos la relación $\sim$ de la siguiente manera: $x \sim y$ si y sólo si x e y están en el mismo subconjunto. Es fácil ver que esto da una relación de equivalencia. También es fácil ver que estas

asignaciones son una la inversa de la otra, en el sentido de que si empezamos con una relación de equivalencia, miramos la partición asociada, y la relación asociada a esta partición, recuperamos la relación original. Asimismo, si empezamos con una partición, miramos la relación de equivalencia asociada, y la partición que tiene esta relación, recuperamos la partición original. □

1.3 Funciones.

En esta sección volvemos a considerar relaciones de un conjunto A en un conjunto B y formalizamos la noción de función, que todos sabemos que es una asignación que a cada elemento de un conjunto de partida A le hace corresponder algún elemento de un conjunto de llegada B. Como por ejemplo la famosa función cuadrática:



Definición 1.3.1. (Función.)

Sean A y B conjuntos, y sea $\mathcal{R}$ una relación de A en B. Se dice que $\mathcal{R}$ es una *función* cuando todo elemento $x \in A$ está relacionado con algún $y \in B$, y este elemento y es único. Es decir:

$$\forall\, x \in A,\ \exists !\, y \in B : x\, \mathcal{R}\, y.$$

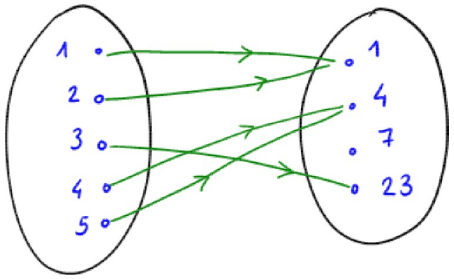
Aquí el símbolo "$\exists !$" significa "existe un único", es decir:

$$\begin{aligned} &\forall\, x \in A,\ \exists\, y \in B \text{ tal que } x\, \mathcal{R}\, y, \\ &\text{y si } y, z \in B \text{ son tales que } x\, \mathcal{R}\, y \text{ y } x\, \mathcal{R}\, z, \text{ entonces } y = z. \end{aligned}$$

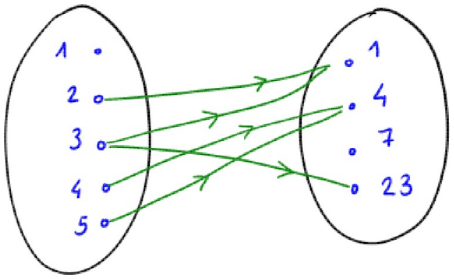
Como a cada $x \in A$ le corresponde un $y \in B$ y este y es único, se le puede dar un nombre que hace notar que y depende de x: se dice que y es la *imagen* de x por f, y se suele notar "$y = f(x)$", que es la forma usual en la que conocemos a las funciones; se nota "$f : A \to B$" a una función del conjunto A en el conjunto B.

Ejemplos:

- La relación de $A = \{1, 2, 3, 4, 5\}$ en $B = \{1, 4, 7, 23\}$ descrita por el diagrama siguiente es una función, la función $f_1 : A \to B$ que satisface $f_1(1) = 1$, $f_1(2) = 1$, $f_1(3) = 23$, $f_1(4) = 4$ y $f_1(5) = 4$.



- La relación de $A = \{1, 2, 3, 4, 5\}$ en $B = \{1, 4, 7, 23\}$ descrita por el diagrama siguiente no es una función.



  Falla tanto que el elemento $1 \in A$ no está relacionado con nadie en B como que el elemento $3 \in A$ está relacionado con dos elementos distintos de B. (Lo primero se puede solucionar "restrigiendo el dominio", pero lo segundo no tiene solución clara para hacer de esta relación una función.)

- La relación $\mathcal{R} \subseteq \mathbb{R} \times \mathbb{R}$ dada por $\mathcal{R} = \{(x, x^2) : x \in \mathbb{R}\}$ es la función $f : \mathbb{R} \to \mathbb{R}, f(x) = x^2$ graficada arriba.

- La relación $\mathcal{R} \subseteq \mathbb{Z} \times \mathbb{N}_0$ dada por $\mathcal{R} = \{(k, |k|) : k \in \mathbb{Z}\}$ es una función, que se escribe $f : \mathbb{Z} \to \mathbb{N}_0, f(k) = |k|$.

- La relación $\mathcal{R} \subseteq \mathbb{N}_0 \times \mathbb{Z}$ dada por $\mathcal{R} = \{(k^2, k) : k \in \mathbb{Z}\}$ *no* es una función, ya que por ejemplo tanto $(1, 1)$ como $(1, -1)$ pertenecen a $\mathcal{R}$ (el elemento $1 \in \mathbb{N}_0$ está relacionado con dos elementos de $\mathbb{Z}$).

- Dado un conjunto $A \neq \emptyset$ cualquiera, la relación $\mathcal{R} \subseteq A \times A$ dada por $\mathcal{R} = \{(x, x) : x \in A\}$ siempre es una función, que se llama la *función identidad* de A y se nota id_A (o id cuando está claro el conjunto A): satisface $\mathrm{id}_A(x) = x$, $\forall\, x \in A$.

- Una n-upla $x = (x_1, \dots, x_n) \in \mathbb{R}^n$ se puede pensar como una función $f : \{1, \dots, n\} \to \mathbb{R}$: la función

  $f : \{1, \dots, n\} \to \mathbb{R}$ definida por $f(1) = x_1, f(2) = x_2, \dots, f(n) = x_n$.

  Recíprocamente, una función $f : \{1, \dots, n\} \to \mathbb{R}$ se puede pensar como una n-upla de $\mathbb{R}^n$: la n-upla

  $$(x_1, \dots, x_n) = \big(f(1), f(2), \dots, f(n)\big) \in \mathbb{R}^n.$$

- Extendiendo el ejemplo anterior, si A es un conjunto, una sucesión

  $$(x_i)_{i\in\mathbb{N}} = (x_1, x_2, x_3, \dots)$$

  de elementos de A se puede pensar como una función $f : \mathbb{N} \to A$: la función definida por

  $$f(1) = x_1, f(2) = x_2, f(3) = x_3, \dots, \text{ es decir } f(i) = x_i, \forall\, i \in \mathbb{N}.$$

  Recíprocamente, una función $f : \mathbb{N} \to A$ se puede pensar como una sucesión en A: la sucesión

  $(x_1, x_2, x_3 \dots) = \big(f(1), f(2), f(3), \dots\big)$, es decir $(x_i)_{i\in\mathbb{N}} = \big(f(i)\big)_{i\in\mathbb{N}}$.

Definición 1.3.2. (Igualdad de funciones.)

Sean $f, g : A \to B$ funciones. Se tiene

$$f = g \iff f(x) = g(x),\ \forall\, x \in A.$$

Dada una función $f : A \to B$, el conjunto A se llama el *dominio* de la función f, y el conjunto B se llama el *codominio* de la función f. Como se ve de los ejemplos anteriores, todos los elementos del dominio tienen que estar involucrados en una función, o sea tienen que tener al menos una imagen y con $y = f(x)$, pero puede ocurrir que haya elementos y del codominio que no estén involucrados, que no tengan preimagen x tal que $f(x) = y$. Esto motiva la siguiente definición:

Definición 1.3.3. (Imagen de una función.)

Sea $f : A \to B$ es una función. La *imagen* de f, que se nota $\mathrm{Im}(f)$, es el subconjunto de elementos de B que están relacionados con algún elemento de A. Es decir

$$\mathrm{Im}(f) = \{y \in B : \exists\, x \in A \text{ tal que } f(x) = y\}.$$

En términos del diagrama, la imagen es el conjunto de elementos de B a los que les llega al menos una flecha. En términos del gráfico, es el conjunto de puntos del eje vertical que cuando tiro una recta horizontal por ese punto, corta el gráfico en al menos un punto.

Ejemplos:

- La imagen de la función $f_1 : \{1,2,3,4,5\} \to \{1,4,7,23\}$ descrita arriba es el conjunto $\{1,4,23\}$.
- Sea $f_2 : \mathbb{N} \to \mathbb{N}, f_2(n) = n+1$. Entonces $\mathrm{Im}(f_2) = \mathbb{N}_{\geq 2}$ pues para todo $m \geq 2$, existe $n \in \mathbb{N}$ tal que $n+1 = m$ (tomando $n = m-1$ que pertenece a $\mathbb{N}$ pues $m \geq 2$) pero $1 \notin \mathrm{Im}(f_2)$ pues no existe $n \in \mathbb{N}$ tal que $n+1 = 1$.
- ¿Y si se considera $f_3 : \mathbb{Z} \to \mathbb{Z}, f(n) = n+1$?
- Sea $f_4 : \mathbb{R} \to \mathbb{R}, f(x) = x^2$. Entonces $\mathrm{Im}(f) = \mathbb{R}_{\geq 0}$.
- Sea $f_5 : \mathbb{Z} \to \mathbb{Z}, f(k) = |k|$. Entonces $\mathrm{Im}(f) = \mathbb{N}_0$.
- Sea $A \neq \emptyset$ un conjunto, entonces $\mathrm{Im}(\mathrm{id}_A) = A$.
- Sea

$$f_6 : \mathbb{N} \to \mathbb{Z},\ f_6(n) = \begin{cases} \dfrac{n-1}{2} & \text{si} \quad n \text{ es impar} \\ -\dfrac{n}{2} & \text{si} \quad n \text{ es par.} \end{cases}$$

  Esto es efectivamente una función bien definida sobre los números naturales, y para cada número natural n, se tiene $f_6(n) \in \mathbb{Z}$. Más aún probemos que $\mathrm{Im}(f_6) = \mathbb{Z}$:

  Se tiene $1 \mapsto \dfrac{1-1}{2} = 0$ pues 1 es impar, $2 \mapsto -\dfrac{2}{2} = -1$ pues 2 es par, $3 \mapsto 1$, $4 \mapsto -2$, $5 \mapsto 2$ y esto da una indicación de cómo funciona esta función: los impares va a parar a los enteros ≥ 0 y los pares van a parar a los enteros ≤ -1.

  Sea entonces $k \in \mathbb{Z}$. Queremos probar que $k = f_6(n)$ para algún $n \in \mathbb{N}$.

  Si $k \geq 0$, probemos que $k = f_6(n) = \dfrac{n-1}{2}$ para algún *número natural impar* n:

$$k = \frac{n-1}{2} \iff 2k = n-1 \iff n = 2k+1$$

  que pertenece a $\mathbb{N}$ por ser $k \geq 0$ (se tiene $k \geq 0 \Rightarrow n = 2k+1 \geq 1$), y es además impar, como se quería probar.

  Si $k \leq -1$, probemos que $k = f_6(n) = -\dfrac{n}{2}$ para *algún número natural par* n:

$$k = -\frac{n}{2} \iff 2k = -n \iff n = -2k$$

que pertenece a $\mathbb{N}$ por ser $k \leq -1$ (se tiene $k \leq -1 \Rightarrow -2k \geq 2$), y es además par, como se quería probar.

Luego $\mathrm{Im}(f_6) = \mathbb{Z}$.

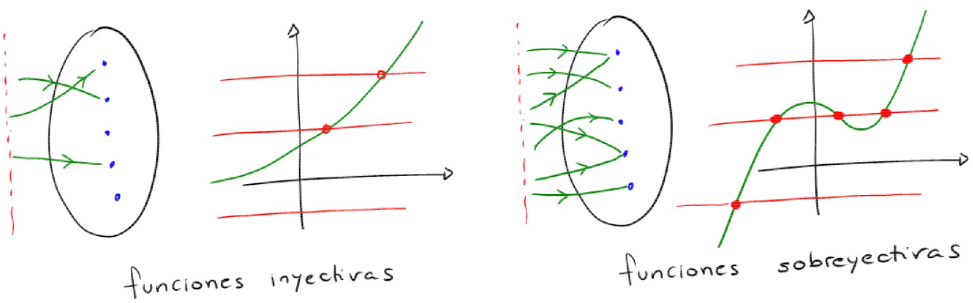
Propiedades importantes que pueden satisfacer las funciones son las siguientes:

Definición 1.3.4. (Funciones inyectivas, sobreyectivas y biyectivas.)

Sea $f : A \to B$ una función. Se dice que

- f es *inyectiva* si *para todo* elemento $y \in B$ existe *a lo sumo un* elemento $x \in A$ para el cual $f(x) = y$. Dicho de otra manera, f es inyectiva si para todo $x, x' \in A$ tales que $f(x) = f(x')$ se tiene que $x = x'$.
- f es *sobreyectiva* si *para todo* elemento $y \in B$ existe *al menos un* elemento $x \in A$ para el cual $f(x) = y$. Dicho de otra manera, f es sobreyectiva si $\mathrm{Im}(f) = B$.
- f es *biyectiva* si es a la vez inyectiva y sobreyectiva, es decir *para todo* elemento $y \in B$ existe *exactamente un* elemento $x \in A$ para el cual $f(x) = y$.

Ser inyectiva, sobreyectiva y biyectiva son propiedades que se chequean a nivel del codominio: en las representaciones gráficas, ser inyectiva significa que a cada elemento del codominio le llega a lo sumo una flecha, o en el producto cartesiano, que si se trazan rectas horizontales, se corta el grafo de la función a lo sumo corta en un punto. Ser sobreyectiva significa que a cada elemento del codominio le llega por lo menos una flecha, o en el producto cartesiano, que si se trazan rectas horizontales, siempre se corta el grafo de la función en al menos un punto. Biyectiva significa que a cada elemento del codominio le llega exactamente una flecha, o en el producto cartesiano, que si se trazan rectas horizontales, siempre se corta el grafo de la función en exactamente un punto.



Ejemplos:

- La función f_1 arriba no es ni inyectiva pues por ejemplo $f_1(1) = f_1(2) = 1$ ni sobreyectiva pues $7 \notin \mathrm{Im}(f_1)$.
- La función $f_2 : \mathbb{N} \to \mathbb{N}$ es inyectiva pues $f_2(n) = f_2(m)$ significa $n+1 = m+1$ de lo cual se deduce $n = m$, pero no es sobreyectiva pues $1 \notin \mathrm{Im}(f_2)$. Pasa a ser sobreyectiva si se restringe el codomino a la imagen $\mathbb{N}_{\geq 2}$ y se la considera como $f_2 : \mathbb{N} \to \mathbb{N}_{\geq 2}$.
- La función $f_3 : \mathbb{Z} \to \mathbb{Z}$ es inyectiva, igual que f_2, y también es sobreyectiva pues $\forall\, k \in \mathbb{Z}$, $\exists\, n \in \mathbb{Z}$ t.q. $f_3(n) = k$: simplemente tomando $n = k-1$ se satisface que $f_3(n) = k$. Luego es biyectiva.
- La función $f_4 : \mathbb{R} \to \mathbb{R}$ no es ni inyectiva ni sobreyectiva. Pero se puede forzar a que sea sobreyectiva restringiendo el codominio $\mathbb{R}$ a la imagen $\mathbb{R}_{\geq 0}$, o sea definiendo en realidad $f_4 : \mathbb{R} \to \mathbb{R}_{\geq 0}$.
- La función f_5 tampoco es inyectiva ni sobreyectiva.
- id_A es claramente biyectiva, cualquiera sea el conjunto $A \neq \emptyset$.
- La función f_6 es sobreyectiva ya que probamos que $\mathrm{Im}(f_6) = \mathbb{Z}$. Probemos que es también inyectiva:

  Sean $n, m \in \mathbb{N}$ tales que $f_6(n) = f_6(m) = k$. Está claro que para tener la misma imagen k, o bien n y m son ambos impares, o bien son ambos pares (pues si son uno impar y el otro par, por la definición de la función, uno tiene imagen ≥ 0 y el otro < 0). Si son ambos impares, entonces $k = \dfrac{n-1}{2} = \dfrac{m-1}{2}$ implica $n = m$. Si por otro lado son ambos impares, entonces $k = -\dfrac{n}{2} = -\dfrac{m}{2}$ también implica $n = m$. Luego la función f_6 es inyectiva.

  Por lo tanto f_6 es biyectiva (esta función biyectiva entre $\mathbb{N}$ y $\mathbb{Z}$ muestra que $\mathbb{N}$ y $\mathbb{Z}$ tienen el mismo cardinal, el "mismo infinito"...).

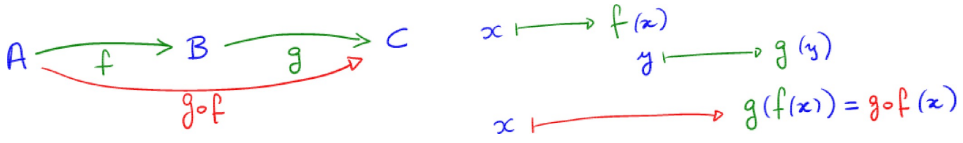
Las funciones se pueden componer, cuando el codominio de una coincide con el dominio de la siguiente:

Definición 1.3.5. (Composición de funciones.)

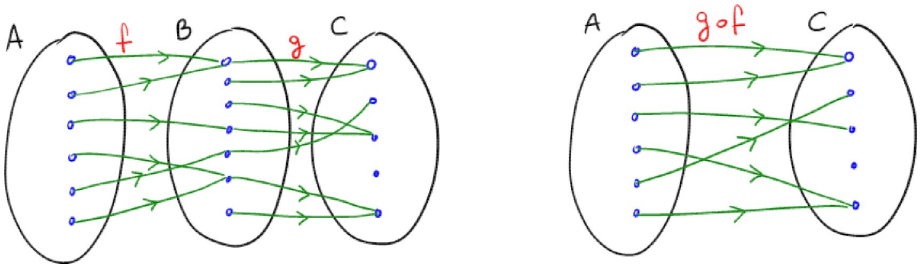
Sean A, B, C conjuntos, y $f : A \to B$, $g : B \to C$ funciones. Entonces la *composición* de f con g, que se nota $g \circ f$, definida por

$$g \circ f(x) = g\big(f(x)\big),\ \forall\, x \in A$$

resulta ser una función de A en C. Esto se visualiza mejor en el diagrama:



Ejemplos:

- 

- Sean $f : \mathbb{N} \to \mathbb{R}$, $f(n) = \sqrt{n}$ y $g : \mathbb{R} \to \mathbb{R}_{\geq 0}$, $g(x) = x^2 + 1$, entonces $g \circ f : \mathbb{N} \to \mathbb{R}_{\geq 0}$ es la función dada por:

$$g \circ f(n) = g\big(f(n)\big) = g(\sqrt{n}) = (\sqrt{n})^2 + 1 = n + 1, \ \forall\, n \in \mathbb{N}.$$

- Sean $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 + 3x + 2$ y $g : \mathbb{R} \to \mathbb{R}$, $g(x) = x^2 - 1$. En este caso se pueden calcular $g \circ f$ y $f \circ g$ que son ambas funciones de $\mathbb{R}$ en $\mathbb{R}$:

$$\begin{aligned} g \circ f(x) &= g\big(f(x)\big) = g(x^2 + 3x + 2) \\ &= (x^2 + 3x + 2)^2 - 1 = x^4 + 6x^3 + 11x^2 + 12x + 3, \\ f \circ g(x) &= f\big(g(x)\big) = f(x^2 - 1) \\ &= (x^2 - 1)^2 + 3(x^2 - 1) + 2 = x^4 + x^2, \quad \forall\, x \in \mathbb{R} \end{aligned}$$

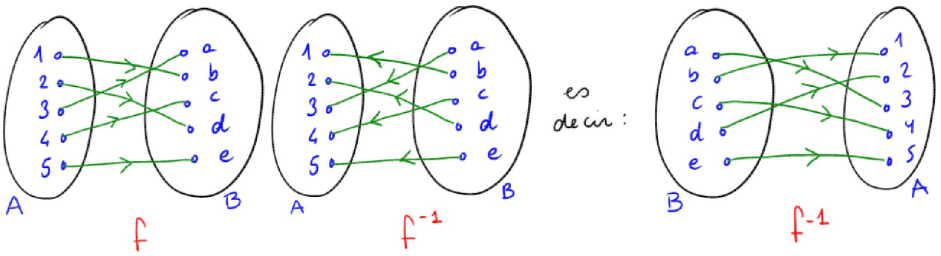
- Sea $f : A \to B$ una función, entonces $\mathrm{id}_B \circ f = f$ y $f \circ \mathrm{id}_A = f$.

1.3.1 Funciones biyectivas y función inversa.

Cuando $f : A \to B$ es una función biyectiva, recordemos que se tiene que *para todo* elemento $y \in B$ existe *exactamente un* elemento $x \in A$ tal que $f(x) = y$. Por lo tanto el conjunto $\mathcal{R}' = \{(y, x) : f(x) = y\} \subseteq B \times A$ es una relación de B en A que también satisface las propiedades de función! Pues todos los $y \in B$ están relacionados con algún $x \in A$, y ese x es único. Esta función $\mathcal{R}'$ se nota f^{-1} y se llama la *función inversa* de f. Está definida

únicamente cuando la función f es biyectiva. Se tiene que $f^{-1}: B \to A$ es la función que satisface para todo $y \in B$:

$$f^{-1}(y) = x \iff f(x) = y.$$



Ejemplos:

- La función inversa de la función $\mathrm{id}_A : A \to A$ es la misma función $\mathrm{id}_A : A \to A$.
- La función inversa de la función $f_3 : \mathbb{Z} \to \mathbb{Z}$, $f_3(n) = n + 1$ es la función $f_3^{-1} : \mathbb{Z} \to \mathbb{Z}$, $f_3^{-1}(k) = k - 1$ (simplemente se despeja en la expresión $k = f_3(n)$ quién es n en función de k, lo que se suele hacer para calcular la imagen).
- La función inversa de la función

$$f_6 : \mathbb{N} \to \mathbb{Z},\ f_6(n) = \begin{cases} \dfrac{n-1}{2} & \text{si} \quad n \text{ es impar} \\ -\dfrac{n}{2} & \text{si} \quad n \text{ es par} \end{cases}$$

  es la función $f_6^{-1} : \mathbb{Z} \to \mathbb{N}$ dada por

$$f_6^{-1}(k) = \begin{cases} 2k+1 & \text{si} \quad k \geq 0 \\ -2k & \text{si} \quad k \leq -1. \end{cases}$$

Las funciones biyectivas y su inversa están relacionadas por medio de la composición. Por ejemplo para $f_3 : \mathbb{Z} \to \mathbb{Z}:\ f_3(n) = n + 1$ se tiene que

$$f_3^{-1} \circ f_3(n) = f_3^{-1}\big(f_3(n)\big) = f_3^{-1}(n+1) = (n+1) - 1 = n,\ \forall\, n \in \mathbb{Z},$$

y por lo tanto $f_3^{-1} \circ f_3 = \mathrm{id}_{\mathbb{Z}}$, y del mismo modo,

$$f_3 \circ f_3^{-1}(k) = f_3\big(f_3^{-1}(k)\big) = f_3(k-1) = (k-1) + 1 = k,\ \forall\, k \in \mathbb{Z},$$

y por lo tanto $f_3 \circ f_3^{-1} = \mathrm{id}_{\mathbb{Z}}$. Esto ocurre siempre, y más aún, vale una recíproca:

Proposición 1.3.6. (Biyectividad y función inversa.)

Sea $f : A \to B$ *una función.*

- *Si* f *es biyectiva, entonces* $f^{-1} \circ f = \mathrm{id}_A$ *y* $f \circ f^{-1} = \mathrm{id}_B$.

- *Si existe una función* $g : B \to A$ *tal que* $g \circ f = \mathrm{id}_A$ *y* $f \circ g = \mathrm{id}_B$, *entonces* f *es biyectiva y* $f^{-1} = g$.

Demostración.

- $f^{-1} \circ f(x) = f^{-1}\big(f(x)\big) = f^{-1}(y)$ donde $y = f(x)$ y por lo tanto $f^{-1}(y) = x$ por la definición de la función inversa. Es decir $f^{-1} \circ f(x) = x$, $\forall\, x \in A$. Así $f^{-1} \circ f = \mathrm{id}_A$. Del mismo modo, se prueba que $f \circ f^{-1} = \mathrm{id}_B$.

- Sea $g : B \to A$ la función tal que $g \circ f = \mathrm{id}_A$ y $f \circ g = \mathrm{id}_B$. Probemos primero que f es biyectiva:

  – f es inyectiva pues $f(x) = f(x')$ implica $g\big(f(x)\big) = g\big(f(x')\big)$, es decir $g \circ f(x) = g \circ f(x')$. Pero $g \circ f = \mathrm{id}_A$, por lo tanto $x = \mathrm{id}_A(x) = \mathrm{id}_A(x') = x'$. Es decir $x = x'$ como se quería probar.

  – f es sobreyectiva pues si $y \in B$, podemos tomar $x = g(y)$. Luego $f(x) = f\big(g(y)\big) = f \circ g(y) = \mathrm{id}_B(y) = y$. Por lo tanto y tiene un antecedente, que es $x = g(y)$.

  Así acabamos de probar que f es biyectiva.

  Para probar que $g = f^{-1}$, hay que probar que $g(y) = f^{-1}(y)$, $\forall\, y \in B$. Pero $g(y) = g\big(f(x)\big)$ donde $y = f(x)$, y por lo tanto $g(y) = g \circ f(x) = \mathrm{id}_A(x) = x = f^{-1}(y)$ por la definición de f^{-1}, $\forall\, y \in B$. Así $g = f^{-1}$.

□

1.4 Ejercicios.

Conjuntos

1. Dado el conjunto $A = \{1, 2, 3\}$, determinar cuáles de las siguientes afirmaciones son verdaderas

   i) $1 \in A$ iii) $\{2, 1\} \subseteq A$ v) $\{2\} \in A$
   ii) $\{1\} \subseteq A$ iv) $\{1, 3\} \in A$

2. Dado el conjunto $A = \{1, 2, \{3\}, \{1, 2\}\}$, determinar cuáles de las siguientes afirmaciones son verdaderas:

   i) $3 \in A$ v) $\{1, 2\} \in A$ ix) $\emptyset \in A$
   ii) $\{3\} \subseteq A$ vi) $\{1, 2\} \subseteq A$ x) $\emptyset \subseteq A$
   iii) $\{3\} \in A$ vii) $\{\{1, 2\}\} \subseteq A$ xi) $A \in A$
   iv) $\{\{3\}\} \subseteq A$ viii) $\{\{1, 2\}, 3\} \subseteq A$ xii) $A \subseteq A$

3. Determinar si $A \subseteq B$ en cada uno de los siguientes casos

   i) $A = \{1, 2, 3\},\ B = \{5, 4, 3, 2, 1\}$
   ii) $A = \{1, 2, 3\},\ B = \{1, 2, \{3\}, -3\}$
   iii) $A = \{x \in \mathbb{R} \,/\, 2 < |x| < 3\},\ B = \{x \in \mathbb{R} \,/\, x^2 < 3\}$
   iv) $A = \{\emptyset\},\ B = \emptyset$

4. Dados los subconjuntos

   $$A = \{1, -2, 7, 3\},\ B = \{1, \{3\}, 10\} \text{ y } C = \{-2, \{1, 2, 3\}, 3\}$$

   del conjunto referencial $V = \{1, \{3\}, -2, 7, 10, \{1, 2, 3\}, 3\}$, hallar

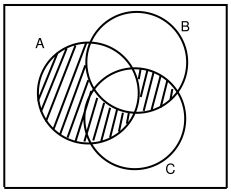
   i) $A \cap (B \triangle C)$
   ii) $(A \cap B) \triangle (A \cap C)$
   iii) $A^c \cap B^c \cap C^c$

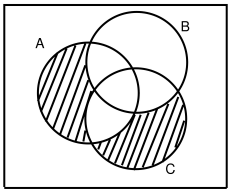
5. Dados subconjuntos A, B, C de un conjunto referencial V, describir $(A \cup B \cup C)^c$ en términos de intersecciones y complementos, y $(A \cap B \cap C)^c$ en términos de uniones y complementos.

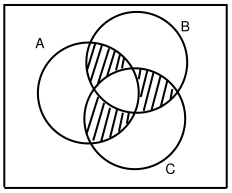
6. Sean A, B y C conjuntos. Representar en un diagrama de Venn

i) $(A \cup B^c) \cap C$ ii) $A \triangle (B \cup C)$ iii) $A \cup (B \triangle C)$

7. Encontrar fórmulas que describan las partes rayadas de los siguientes diagramas de Venn, utilizando únicamente intersecciones, uniones y complementos.

i) 

ii) 

iii) 

8. Hallar el conjunto $\mathcal{P}(A)$ de partes de A en los casos

i) $A = \{1\}$

ii) $A = \{a, b\}$

iii) $A = \{1, \{1, 2\}, 3\}$

9. Sean A y B conjuntos. Probar que $\mathcal{P}(A) \subseteq \mathcal{P}(B) \Leftrightarrow A \subseteq B$.

10. Sean p, q proposiciones. Verificar que las siguientes expresiones tienen la misma tabla de verdad para concluir que son equivalentes:

i) $p \Rightarrow q$, $\sim q \Rightarrow \sim p$, $\sim p \vee q$ y $\sim (p \wedge \sim q)$.

Cuando para probar $p \Rightarrow q$ se prueba en su lugar $\sim q \Rightarrow \sim p$ se dice que es una *demostración por* **contrarrecíproco**, mientras que cuando se prueba en su lugar que suponer que vale $p \wedge \sim q$ lleva a una contradicción, se dice que es una *demostración por* **reducción al absurdo**.

ii) $\sim (p \Rightarrow q)$ y $p \wedge \sim q$.

11. Hallar contraejemplos para mostrar que las siguientes proposiciones son falsas:

i) $\forall a \in \mathbb{N}$, $\frac{a-1}{a}$ no es un número entero.

ii) $\forall x, y \in \mathbb{R}$ con x, y positivos, $\sqrt{x+y} = \sqrt{x} + \sqrt{y}$.

iii) $\forall x \in \mathbb{R}$, $x^2 > 4 \Rightarrow x > 2$.

12. i) Decidir si las siguientes proposiciones son verdaderas o falsas, justificando debidamente:

(a) $\forall n \in \mathbb{N},\ n \geq 5 \ \vee\ n \leq 8$.
(b) $\exists n \in \mathbb{N} /\ n \geq 5 \ \wedge\ n \leq 8$.
(c) $\forall n \in \mathbb{N},\ \exists m \in \mathbb{N} \,/\, m > n$.
(d) $\exists n \in \mathbb{N} /\ \forall m \in \mathbb{N},\ m > n$.
(e) $\forall x \in \mathbb{R},\ x > 3 \Rightarrow x^2 > 4$.
(f) Si z es un número real, entonces z es un número complejo.

ii) Negar las proposiciones anteriores, y en cada caso verificar que la proposición negada tiene el valor de verdad opuesto al de la original.

iii) Reescribir las proposiciones (e) y (f) del inciso (i) utilizando las equivalencias del ejercicio 10 (i).

13. Determinar cuáles de las siguientes afirmaciones son verdaderas cualesquiera sean los subconjuntos A, B y C de un conjunto referencial V y cuáles no. Para las que sean verdaderas, dar una demostración, para las otras dar un contraejemplo.

i) $(A \triangle B) - C = (A - C) \triangle (B - C)$
ii) $(A \cap B) \triangle C = (A \triangle C) \cap (B \triangle C)$
iii) $C \subseteq A \ \Rightarrow\ B \cap C \subseteq (A \triangle B)^c$
iv) $A \triangle B = \emptyset \ \Leftrightarrow\ A = B$

14. Sean A, B y C subconjuntos de un conjunto referencial V. Probar que

i) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$
ii) $A - (B - C) = (A - B) \cup (A \cap C)$
iii) $A \triangle B \subseteq (A \triangle C) \cup (B \triangle C)$
iv) $(A \cap C) - B = (A - B) \cap C$
v) $A \subseteq B \ \Rightarrow\ A \triangle B = B \cap A^c$
vi) $A \subseteq B \ \Leftrightarrow\ B^c \subseteq A^c$
vii) $A \cap C = \emptyset \ \Rightarrow\ A \cap (B \triangle C) = A \cap B$

15. Sean $A = \{1, 2, 3\}$, $B = \{1, 3, 5, 7\}$. Hallar

$$A \times A,\ A \times B \ \text{ y } \ (A \cap B) \times (A \cup B).$$

16. Sean A, B y C conjuntos. Probar que

i) $(A \cup B) \times C = (A \times C) \cup (B \times C)$

ii) $(A \cap B) \times C = (A \times C) \cap (B \times C)$
iii) $(A - B) \times C = (A \times C) - (B \times C)$
iv) $(A \triangle B) \times C = (A \times C) \triangle (B \times C)$

Relaciones

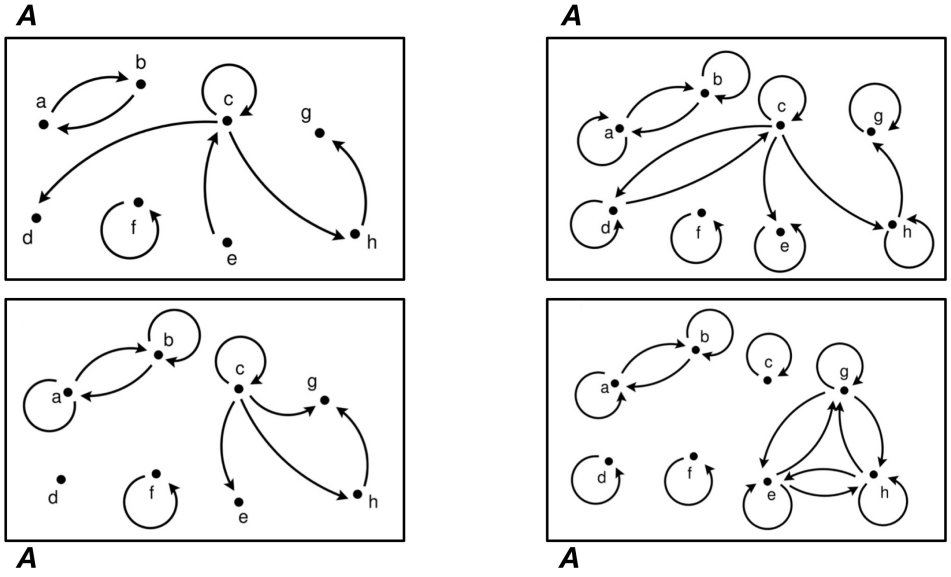
17. Sean $A = \{1, 2, 3\}$ y $B = \{1, 3, 5, 7\}$. Verificar si las siguientes son relaciones de A en B y en caso afirmativo graficarlas por medio de un diagrama con flechas de A en B, y por medio de puntos en el producto cartesiano $A \times B$.

    i) $\mathcal{R} = \{(1,1), (1,3), (1,7), (3,1), (3,5)\}$
    ii) $\mathcal{R} = \{(1,1), (1,3), (2,7), (3,2), (3,5)\}$
    iii) $\mathcal{R} = \{(1,1), (2,7), (3,7)\}$
    iv) $\mathcal{R} = \{(1,3), (2,1), (3,7)\}$

18. Sean $A = \{1, 2, 3\}$ y $B = \{1, 3, 5, 7\}$. Describir por extensión cada una de las relaciones siguientes de A en B:

    i) $(a,b) \in \mathcal{R} \iff a \leq b$
    ii) $(a,b) \in \mathcal{R} \iff a > b$
    iii) $(a,b) \in \mathcal{R} \iff a \cdot b$ es par
    iv) $(a,b) \in \mathcal{R} \iff a + b > 6$

19. Sea $A = \{a, b, c, d, e, f, g, h\}$. Para cada uno de los siguientes gráficos describir por extensión la relación en A que representa y determinar si es reflexiva, simétrica, antisimétrica o transitiva.

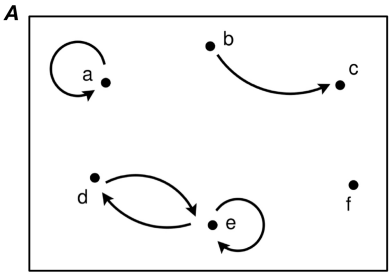


20. Sea $A = \{1, 2, 3, 4, 5, 6\}$. Graficar la relación

$$\mathcal{R} = \{(1,1), (1,3), (3,1), (3,3), (6,4), (4,6), (4,4), (6,6)\}$$

como está hecho en el ejercicio anterior y determinar si es reflexiva, simétrica, antisimétrica o transitiva.

21. Sea $A = \{a, b, c, d, e, f\}$ y sea $\mathcal{R}$ la relación en A representada por el gráfico



Hallar la mínima cantidad de pares que se deben agregar a $\mathcal{R}$ de manera que la nueva relación obtenida sea

i) reflexiva,
ii) simétrica,
iii) transitiva,
iv) reflexiva y simétrica,
v) simétrica y transitiva,
vi) de equivalencia.

22. En cada uno de los siguientes casos determinar si la relación $\mathcal{R}$ en A es reflexiva, simétrica, antisimétrica, transitiva, de equivalencia o de orden.

i) $A = \{1, 2, 3, 4, 5\}$,
$\mathcal{R} = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,2), (1,3), (2,5), (1,5)\}$

ii) $A = \mathbb{N}$, $\mathcal{R} = \{(a,b) \in \mathbb{N} \times \mathbb{N} \,/\, a + b \text{ es par}\}$

iii) $A = \mathbb{Z}$, $\mathcal{R} = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \,/\, |a| \leq |b|\}$

iv) $A = \mathbb{Z}$, $\mathcal{R}$ dada por "$a \,\mathcal{R}\, b \;\Leftrightarrow\; b$ es múltiplo de a"

v) $A = \mathcal{P}(\mathbb{R})$, $\mathcal{R}$ dada por "$X \,\mathcal{R}\, Y \Leftrightarrow X \cap \{1,2,3\} \subseteq Y \cap \{1,2,3\}$"

vi) $A = \mathcal{P}(\{n \in \mathbb{N} / n \leq 30\})$, $\mathcal{R}$ dada por "$X \,\mathcal{R}\, Y \Leftrightarrow 2 \notin X \cap Y^c$"

vii) $A = \mathbb{N} \times \mathbb{N}$, $\mathcal{R}$ dada por "$(a,b) \,\mathcal{R}\, (c,d) \Leftrightarrow bc$ es múltiplo de ad"

23. Sea A un conjunto. Describir todas las relaciones en A que son a la vez

    i) simétricas y antisimétricas ii) de equivalencia y de orden

    ¿Puede una relación en A no ser ni simétrica ni antisimétrica?

24. Sea $A = \{a, b, c, d, e, f\}$. Dada la relación de equivalencia en A:

$$\mathcal{R} = \big\{(a,a),(b,b),(c,c),(d,d),(e,e),(f,f),\\ (a,b),(b,a),(a,f),(f,a),(b,f),(f,b),(c,e),(e,c)\big\}$$

    hallar la clase $\overline{a}$ de a, la clase $\overline{b}$ de b, la clase $\overline{c}$ de c, la clase $\overline{d}$ de d, y la partición asociada a $\mathcal{R}$.

25. Sea $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.
    Hallar y graficar la relación de equivalencia en A asociada a la partición $\big\{\{1,3\},\{2,6,7\},\{4,8,9,10\},\{5\}\big\}$. ¿Cuántas clases de equivalencia distintas tiene? Hallar un representante para cada clase.

26. Sean $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ y $P = \mathcal{P}(X)$ su conjunto de partes. Sea $\mathcal{R}$ la relación en P definida por

$$A \mathcal{R} B \iff (A \triangle B) \cap \{1, 2, 3\} = \emptyset$$

    i) Probar que $\mathcal{R}$ es una relación de equivalencia y decidir si es antisimétrica (*Sugerencia:* usar adecuadamente el ejercicio 14(iii)).

    ii) Hallar la clase de equivalencia de $A = \{1, 2, 3\}$.

27. Sean $A = \{n \in \mathbb{N} / n \leq 92\}$ y $\mathcal{R}$ la relación en A definida por

$$x \mathcal{R} y \iff x^2 - y^2 = 93x - 93y$$

    i) Probar que $\mathcal{R}$ es una relación de equivalencia ¿Es antisimétrica?

    ii) Hallar la clase de equivalencia de cada $x \in A$. Deducir cuántas clases de equivalencia **distintas** determina la relación $\mathcal{R}$.

28. i) Sea $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Consideremos en $\mathcal{P}(A)$ la relación de equivalencia dada por el cardinal (es decir, la cantidad de elementos): dos subconjuntos de A están relacionados si y solo si tienen la misma cantidad de elementos ¿Cuántas clases de equivalencia **distintas** determina la relación? Hallar un representante para cada clase.

ii) En el conjunto de todos los subconjuntos finitos de $\mathbb{N}$, consideremos nuevamente la relación de equivalencia dada por el cardinal: dos subconjuntos finitos de $\mathbb{N}$ están relacionados si y solo si tienen la misma cantidad de elementos ¿Cuántas clases de equivalencia **distintas** determina la relación? Hallar un representante para cada clase.

Funciones

29. Determinar si $\mathcal{R}$ es una función de A en B en los casos

    i) $A = \{1,2,3,4,5\}$, $B = \{a,b,c,d\}$,
    $\mathcal{R} = \{(1,a),(2,a),(3,a),(4,b),(5,c),(3,d)\}$

    ii) $A = \{1,2,3,4,5\}$, $B = \{a,b,c,d\}$, $\mathcal{R} = \{(1,a),(2,a),(3,d),(4,b)\}$

    iii) $A = \{1,2,3,4,5\}$, $B = \{a,b,c,d\}$,
    $\mathcal{R} = \{(1,a),(2,a),(3,d),(4,b),(5,c)\}$

    iv) $A = \mathbb{N}$, $B = \mathbb{R}$, $\mathcal{R} = \{(a,b) \in \mathbb{N} \times \mathbb{R} \,/\, a = 2b - 3\}$

    v) $A = \mathbb{R}$, $B = \mathbb{N}$, $\mathcal{R} = \{(a,b) \in \mathbb{R} \times \mathbb{N} \,/\, a = 2b - 3\}$

    vi) $A = \mathbb{Z}$, $B = \mathbb{Z}$, $\mathcal{R} = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \,/\, a + b$ es divisible por $5\}$

30. Determinar si las siguientes funciones son inyectivas, sobreyectivas o biyectivas. Para las que sean biyectivas hallar la inversa y para las que no sean sobreyectivas hallar la imagen.

    i) $f : \mathbb{R} \longrightarrow \mathbb{R}, \quad f(x) = 12x^2 - 5$

    ii) $f : \mathbb{R}^2 \longrightarrow \mathbb{R}, \quad f(x,y) = x + y$

    iii) $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^2, \quad f(x,y,z) = (x + y, 2z)$

    iv) $f : \mathbb{N} \longrightarrow \mathbb{N}, \quad f(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ es par} \\ n+1 & \text{si } n \text{ es impar} \end{cases}$

    v) $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \quad f(a,b) = 3a - 2b$

    vi) $f : \mathbb{Z} \longrightarrow \mathbb{N}, \quad f(a) = \begin{cases} 2a & \text{si } a > 0 \\ 1 - 2a & \text{si } a \leq 0 \end{cases}$

31. i) Dadas las funciones

    $$f : \mathbb{N} \to \mathbb{N},\ f(n) = \begin{cases} \frac{n^2}{2} & \text{si } n \text{ es divisible por 6} \\ 3n+1 & \text{en los otros casos} \end{cases} \quad \text{y}$$

    $$g : \mathbb{N} \times \mathbb{N} \to \mathbb{N},\ g(n,m) = n(m+1),$$

    calcular, de ser posible, $(f \circ g)(3,4)$, $(f \circ g)(2,5)$ y $(f \circ g)(3,2)$.

ii) Dadas las funciones

$$f : \mathbb{R} \to \mathbb{R},\ f(x) = \begin{cases} x^2 & \text{si } x \leq 7 \\ 2x - 1 & \text{si } x > 7 \end{cases} \quad \text{y} \quad g : \mathbb{N} \to \mathbb{R},\ g(n) = \sqrt{n},$$

hallar, si existen, todos los $n \in \mathbb{N}$ tales que $(f \circ g)(n) = 13$ y todos los $m \in \mathbb{N}$ tales que $(f \circ g)(m) = 15$.

32. Hallar $f \circ g$ y $g \circ f$ (cuando sea posible) en los casos

i) $f : \mathbb{R} \to \mathbb{R},\ f(x) = 2x^2 - 18$ y $g : \mathbb{R} \to \mathbb{R},\ g(x) = x + 3$

ii) $f : \mathbb{N} \to \mathbb{N},\ f(n) = \begin{cases} n - 2 & \text{si } n \text{ es divisible por 4} \\ n + 1 & \text{si } n \text{ no es divisible por 4} \end{cases}$ y $g : \mathbb{N} \to \mathbb{N},\ g(n) = 4n$

iii) $f : \mathbb{R} \to \mathbb{R} \times \mathbb{R},\ f(x) = (x + 5, 3x)$ y $g : \mathbb{N} \to \mathbb{R},\ g(n) = \sqrt{n}$

33. Hallar dos funciones $f : \mathbb{N} \longrightarrow \mathbb{N}$ y $g : \mathbb{N} \longrightarrow \mathbb{N}$ tales que $f \circ g = \mathrm{Id}_{\mathbb{N}}$ y $g \circ f \neq \mathrm{id}_{\mathbb{N}}$, donde $\mathrm{Id}_{\mathbb{N}} : \mathbb{N} \longrightarrow \mathbb{N}$ denota la función identidad del conjunto $\mathbb{N}$.

34. Sean A, B y C conjuntos. Probar que si $f : B \longrightarrow C$ y $g : A \longrightarrow B$ son funciones entonces valen

i) si $f \circ g$ es inyectiva entonces g es inyectiva.

ii) si $f \circ g$ es sobreyectiva entonces f es sobreyectiva

iii) si f y g son inyectivas entonces $f \circ g$ es inyectiva

iv) si f y g son sobreyectivas entonces $f \circ g$ es sobreyectiva

v) si f y g son biyectivas entonces $f \circ g$ es biyectiva

35. Sean $A = \{1, \ldots, 10\}$ y $\mathcal{F} = \{f : A \to A : f \text{ es } \textbf{biyectiva}\}$. Sea $\mathcal{R}$ la relación en $\mathcal{F}$ dada por "$f \,\mathcal{R}\, g \Leftrightarrow \exists\, n \in A : f(n) = 1 \,\textbf{y}\, g(n) = 1$."

i) Probar que $\mathcal{R}$ es una relación de equivalencia ¿Es antisimétrica?

ii) Sea $\mathrm{Id} : A \longrightarrow A$ la función identidad, o sea, $\mathrm{Id}(n) = n,\ \forall\, n \in A$. Dar tres elementos **distintos** de la clase de equivalencia de Id
Importante: al exhibir una función es indispensable definirla en **todos** los elementos de su dominio.

36. Sean $A = \{1, 2, 3, 4\}$, $B = \{1, 2, 3, 4, 5, 6, 7, 8\}$ y $\mathcal{F} = \{g : A \longrightarrow B\}$ el conjunto de **todas** las funciones de A en B.
Sea ahora $f : A \longrightarrow A$ una función dada. Definimos en $\mathcal{F}$ la relación dada por "$g \,\mathcal{R}\, h \iff g \circ f = h \circ f$."

i) Probar que $\mathcal{R}$ es una relación de equivalencia ¿Es siempre antisimétrica (sin importar cómo sea f)?

ii) Asumiendo que f es sobreyectiva, calcular la clase de equivalencia de cada $g \in \mathcal{F}$.

Capítulo 2

Números Naturales e Inducción.

Como ya sabemos, los *números naturales* son informalmente el conjunto infinito

$$\mathbb{N} = \{1, 2, 3, 4, \ldots, 1001, 1002, \ldots, 2356789, \ldots\}$$

de números que empiezan en 1 y se obtienen los demás sumando siempre 1. Al final de este capítulo, se describe una construcción formal de los números naturales a través de los axiomas de Peano.

En el conjunto $\mathbb{N}$ se puede sumar y multiplicar: si $m, n \in \mathbb{N}$, entonces $m + n \in \mathbb{N}$ y $m \cdot n \in \mathbb{N}$. Además la suma y el producto se "portan bien":

- *Conmutatividad:* $m + n = n + m$ y $m \cdot n = n \cdot m$, $\forall\, m, n \in \mathbb{N}$.
- *Asociatividad:* $(m + n) + k = m + (n + k)$ y $(m \cdot n) \cdot k = m \cdot (n \cdot k)$, $\forall\, m, n, k \in \mathbb{N}$.
- *Distributividad del producto sobre la suma:* $m \cdot (n + k) = m \cdot n + m \cdot k$, $\forall\, m, n, k \in \mathbb{N}$.

El objetivo de este capítulo es adquirir herramientas que permiten demostrar (en algunos casos) que una proposición p enunciada sobre el conjunto de los números naturales es Verdadera, o sea si la proposición p está dada para cada $n \in \mathbb{N}$ por una afirmación $p(n)$, probar que $p(n)$ es Verdadera para todo $n \in \mathbb{N}$.

Ejemplos de tales proposiciones p, q pueden ser

$$p:\ \forall\, n \in \mathbb{N}:\ n^2 \geq 1 \quad \text{o} \quad q:\ \forall\, n \in \mathbb{N}:\ n \geq 3.$$

Una tal proposición p es Verdadera si la afirmación asociada $p(n) : n^2 \geq 1$ es Verdadera para todo $n \in \mathbb{N}$, o Falsa si la afirmación $p(n) : n^2 \geq 1$ es Falsa para al menos algún $n \in \mathbb{N}$, o sea en este caso si existe $n \in \mathbb{N} : \ n^2 < 1$. En estos ejemplos es claro que p es Verdadera, y que q es Falsa, pues $\exists\, n \in \mathbb{N} : n < 3$, por ejemplo $n = 1$.

Demostrar que una proposición p enunciada sobre todos los números naturales es Verdadera no se puede hacer "verificando" porque nunca vamos a lograr agotar todos los números naturales, sino que hacen falta ciertos mecanismos que garanticen que la demostración está probando la afirmación para todos los números naturales.

Para ejemplificar por qué una simple verificación puede engañar, consideremos el conjunto $A := \{\sqrt{1141n^2+1},\ n \in \mathbb{N}\} \cap \mathbb{N}$. Por ejemplo para $n = 1$, $\sqrt{1141n^2+1} = 33,79\ldots$, luego $1 \notin A$, y para $n = 2$, $\sqrt{1141n^2+1} = 67,56\ldots$, luego $2 \notin A$. Por tiempo se creyó que $A = \emptyset$ pero resulta que no lo es! Lo que ocurre es que el primero número natural $n \in A$ tiene 26 dígitos...

Otro ejemplo es la *Conjetura de Goldbach*, por el matemático prusiano *Christian Goldbach*, 1690-1764 (de quién no se conoce ninguna imagen, como me hizo notar el profesor Román Sasyk luego de que yo pusiera una supuesta foto en estas notas), que afirma que todo número natural par ≥ 4 es la suma de dos números primos (por ejemplo $4 = 2+2$, $8 = 3+5$, $12 = 5+7$, $100 = 3 + 97$).

Se sabe que esta conjetura es cierta para todos los números pares $\leq 4 \cdot 10^{18}$ pero sin embargo aún no está probada, a pesar de la cantidad de esfuerzos invertidos en ella.

En 2013, el matemático peruano Harald Helfgott demostró lo que se conocía como la *Conjetura débil de Goldbach*, completando el trabajo previo de 1937 del soviético Ivan Vinogradov. Ésta afirma que todo número natural impar ≥ 7 es la suma de tres números primos (por ejemplo $7 = 3+2+2$, $9 = 3+3+3$, $17 = 3+7+7$).

Esta conjetura se llamaba débil porque si la anterior es cierta, entonces también es cierta ésta: restándole 3 al número impar ≥ 7 se obtiene un número par ≥ 4 que sería suma de dos primos...

Empecemos con un par de ejemplos muy clásicos e importantes.

2.1 La suma de Gauss y la serie geométrica.

2.1.1 La suma de Gauss.

Supongamos que queremos sumar los 100 primeros números naturales, o sea

$$1+2+3+\cdots+98+99+100.$$

Se puede hacer recursivamente $1+2=3$ luego $1+2+3=3+3=6$ etc. ¡pero eso tarda mucho!

Proponemos aquí la solución presentada por el alemán *Carl-Friedrich Gauss*, 1777-1855, fue uno de los matemáticos, astrónomos y físicos más influyentes de la historia. Se lo conoce como "el príncipe de las matemáticas".

Dice la historia que cuando el maestro les dio ese problema a sus alumnos para tener un poco de paz por un rato, el pequeño Carl-Friedrich contestó inmediatamente 5050 ¡que es la respuesta correcta! ¿Qué fue lo que hizo? Se dio cuenta que si uno sumaba "al derecho y al revés", tenía una forma de sumar de dos maneras distintas:

$$\begin{array}{rcccccccccccccc} S &=& 1 &+& 2 &+& 3 &+& \cdots &+& 98 &+& 99 &+& 100 \\ S &=& 100 &+& 99 &+& 98 &+& \cdots &+& 3 &+& 2 &+& 1 \\ \hline 2S &=& 101 &+& 101 &+& 101 &+& \cdots &+& 101 &+& 101 &+& 101 \end{array} = 100\cdot 101.$$

Luego $S=(100\cdot 101)/2=50\cdot 101=5050$.

Este procedimiento es claramente generalizable a cualquier número natural n, y se obtiene

$$\forall\, n\in\mathbb{N}: \quad 1+2+\cdots+(n-1)+n=\frac{n(n+1)}{2}.$$

Notar que este número siempre es un número natural (como debe ser) ya que $n(n+1)$ siempre es un número par!

2.1.2 La serie geométrica.

Ahora, sea un número q cualquiera, y queremos sumar las $n+1$ primeras potencias de q,

$$1+q+q^2+\cdots+q^{n-1}+q^n.$$

El mecanismo siguiente, parecido al de la suma de Gauss, permite hallar la suma de esta serie geométrica:

$$\begin{array}{rcccccccccccc} Q &=& 1 &+& q &+& q^2 &+& \cdots &+& q^{n-1} &+& q^n \\ q\cdot Q &=& & & q &+& q^2 &+& q^3 &+& \cdots &+& q^n &+& q^{n+1} \\ \hline q\cdot Q-Q &=& -1 & & & & & & + & & & & & & q^{n+1}. \end{array}$$

Luego $(q-1)Q = q^{n+1} - q$ Lo que implica que si $q \neq 1$, $Q = \frac{q^{n+1}-1}{q-1}$. Pero es fácil calcular la suma para $q = 1$: da $n+1$ ¿por qué? Es decir,

$$\forall\, n \in \mathbb{N}: \quad 1 + q + \cdots + q^n = \begin{cases} n+1 & \text{si} \quad q = 1, \\ \dfrac{q^{n+1}-1}{q-1} & \text{si} \quad q \neq 1. \end{cases}$$

2.2 Sumatoria y Productoria.

En la sección anterior consideramos las sumas $1 + 2 + \cdots + 99 + 100$ y $1 + q + \cdots + q^{n-1} + q^n$ donde los puntos suspensivos reemplazan los términos intermedios que se interpretan como "se debe", en la forma natural para completar la secuencia. Pero hay una notación que evita el uso de estos puntos suspensivos y deja claro quiénes son esos términos intermedios. Esta es la notación para la sumatoria.

Sea entonces $(a_i)_{i\in\mathbb{N}} = (a_1, a_2, \dots)$ una sucesión de números $a_i \in A$ que se pueden sumar y multiplicar en el conjunto A (por ejemplo números naturales, enteros, racionales, reales, complejos, pero veremos más ejemplos en lo que sigue del curso).

2.2.1 Sumatoria.

Sea $n \in \mathbb{N}$. La notación $\sum_{i=1}^{n} a_i$, que se lee la *sumatoria* para i de 1 a n de a_i, representa la suma de los n primeros términos de la sucesión $(a_i)_{i\in\mathbb{N}}$:

$$\sum_{i=1}^{n} a_i = a_1 + \cdots + a_n,$$

que se define formalmente *por recurrencia*, para evitar los puntos suspensivos:

$$\sum_{i=1}^{1} a_i = a_1 \quad \text{y} \quad \sum_{i=1}^{n+1} a_i = \sum_{i=1}^{n} a_i \ + a_{n+1}\ , \ \forall\, n \in \mathbb{N}.$$

Aquí el índice i es el índice de sumación que simplemente indica cuáles son los términos de la sucesión que se suman, desde el primer a_i indicado por el valor que toma i cuando dice $i = 1$ abajo del símbolo de la sumatoria, hasta el último a_i indicado por el valor que toma i cuando dice n arriba de la sumatoria, y no tiene importancia si se lo llama i o k o de cualquier forma. Así $\sum_{i=1}^{n} a_i = \sum_{k=1}^{n} a_k$. También se puede escribir $\sum_{1\leq i\leq n} a_i$.

Ejemplos:

- $\sum_{i=1}^{n} i = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}\,,\ \forall\, n \in \mathbb{N}\,.$
- $\sum_{i=1}^{n} 1 = n\,,\ \ \sum_{i=1}^{n} a = n\,a\,,\ \ \sum_{i=1}^{n} n = n^2\,,\ \ \forall\, n \in \mathbb{N}\,.$

Esta definición de sumatoria se extiende tal cual a

$$\sum_{i=n_0}^{n} a_i = a_{n_0} + \cdots + a_n,$$

para $n_0 \leq n$, y de hecho se extiende a $n_0 = 0$ (o sea tiene sentido $\sum_{i=0}^{n} a_i = a_0 + \cdots + a_n$ si el término a_0 está definido) e incluso a índices negativos $n_0 \in \mathbb{Z}$ (si los términos a_i correspondientes están definidos). Por ejemplo:

$$\sum_{i=0}^{n} q^i = 1 + q + \cdots + q^n = \begin{cases} \frac{q^{n+1}-1}{q-1} & \text{si} \quad q \neq 1 \\ n+1 & \text{si} \quad q = 1. \end{cases}\ ,\ \forall\, n \in \mathbb{N}.$$

La sumatoria satisface las dos propiedades siguientes para todo $n \in \mathbb{N}$, para todo par de sucesiones $(a_i)_{i\in\mathbb{N}}$, $(b_i)_{i\in\mathbb{N}}$ en A y para todo $c \in A$:

- $\Big(\sum_{i=1}^{n} a_i\Big) + \Big(\sum_{i=1}^{n} b_i\Big) = \sum_{i=1}^{n} (a_i + b_i)\,.$
- $c \cdot \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} c \cdot a_i\,.$

Así por ejemplo, $\sum_{k=1}^{n^2}(k+n) = \Big(\sum_{k=1}^{n^2} k\Big) + \Big(\sum_{k=1}^{n^2} n\Big) = \frac{n^2(n^2+1)}{2} + n^3\,.$

Un programa recursivo para la sumatoria en Haskell:

Esta definición recursiva está muy en sintonía con la programación funcional.

La función sumatoria de una serie que toma valores enteros en el lenguaje de *programación funcional Haskell*, desarrollado a partir de mediados de los 80, y nombrado así por el matemático y lógico americano *Haskell Brooks Curry*, 1900-1982, usando la *currificación* que vieron en el taller, se puede definir de la manera siguiente:

```
sumatoria :: (Integer → Integer) → Integer → Integer
sumatoria a 0 = 0
sumatoria a n = a n + sumatoria a (n − 1)
```

Un programa iterativo para la sumatoria en Python:

Existen otros lenguajes de programación no funcionales, por ejemplo *imperativos*.

Si escribimos un programa iterativo para la sumatoria en el extensamente usado lenguaje de programación imperativo *Python*, creado a fines de los años 80 por el computador y matemático holandés *Guido van Rossum*, resulta más parecido a la definición de sumatoria que dimos como la suma de todos los términos de la sucesión $(a_i)_{i\in\mathbb{N}}$ hasta el n-ésimo.

Asumimos que la sucesión $(a_i)_{i\in\mathbb{N}}$ está definida por una función $a : \mathbb{N} \to A$, o sea tal que $a(i) = a_i$. Entonces el programa es

```
def sumatoria(n):
    s = 0
    for i in range (1, n+1):
        s = s + a(i)
    return s
```

(La línea $s = 0$ pone en la variable s el valor 0. Luego la instrucción "for i in range $(1, n+1)$" ejecuta la línea que sigue (es decir poner en la variable s el valor que tenía s sumado el valor de a_i) para todos los valores de $i \geq 1$ y $< n+1$, es decir entre 1 y n.)

2.2.2 Productoria.

Sea $n \in \mathbb{N}$. La notación $\prod_{i=1}^{n} a_i$, que se lee la *productoria* para i de 1 a n de a_i, representa el producto de los n primeros términos de la sucesión $(a_i)_{i\in\mathbb{N}}$:

$$\prod_{i=1}^{n} a_i = a_1 \cdots a_n,$$

que se define formalmente *por recurrencia*, para evitar los puntos suspensivos:

$$\prod_{i=1}^{1} a_i = a_1 \quad \text{y} \quad \prod_{i=1}^{n+1} a_i = \Big(\prod_{i=1}^{n} a_i\Big) \cdot a_{n+1} \ , \ \forall\, n \in \mathbb{N}.$$

Ejemplos:

- $\prod_{i=1}^{n} i = 1 \cdot 2 \cdots (n-1) \cdot n$ se nota $n!$, $\forall\, n \in \mathbb{N}$, y se llama n *factorial* o el *factorial de* n. Tiene un símbolo y un nombre para él solito por la importancia que tiene lo que representa, que estudiaremos con más detalle en el capítulo que viene.
- $\prod_{i=1}^{n} c = c^n$, $\forall\, c \in A$, $\forall\, n \in \mathbb{N}$.

La productoria satisface la propiedad siguiente para todo $n \in \mathbb{N}$ y sucesiones $(a_i)_{i\in\mathbb{N}}$, $(b_i)_{i\in\mathbb{N}}$ en A:

- $\Big(\prod_{i=1}^{n} a_i\Big) \cdot \Big(\prod_{i=1}^{n} b_i\Big) = \prod_{i=1}^{n} (a_i \cdot b_i)$.

Un programa recursivo para la productoria en Haskell:

```
productoria :: (Integer → Integer) → Integer → Integer
productoria a 0 = 1
productoria a n = a n ∗ productoria a (n − 1)
```

Un programa iterativo para la productoria en Python:

Supongamos que la sucesión $(a_i)_{i\in\mathbb{N}}$ en A está definida por una función $a : \mathbb{N} \to A$, o sea tal que $f(i) = a_i$. Entonces el programa es

```
def prod (n):
    p = 1
    for i in range (1, n + 1):
        p = p ∗ f(i)
    return p
```

2.3 El conjunto inductivo $\mathbb{N}$ y el principio de inducción.

Como no a todos se nos ocurren los trucos "à la Gauss" para probar que ciertas afirmaciones son válidas para todos los números naturales, o a veces

no hay truco, hay un mecanismo muy útil y que se usa muchísimo para demostrar eso, que se llama el *principio de inducción*.

Este principio fue usado a lo largo del tiempo de distintas maneras desde mucho antes de Cristo, en distintas civilizaciones, aunque la primera formulación explícita de este principio fue introducida en 1665 por el matemático, físico, escritor, inventor y filósofo francés *Blaise Pascal*, 1623-1662.

Lo vamos a aplicar reiteradas veces a lo largo de toda la materia, y lo van a seguir aplicando no solo a lo largo de toda la matemática que hagan, sino también de muchas otras ciencias.

El principio funciona en dos pasos. El primer paso, conocido como *caso base* es probar que la afirmación en cuestión es Verdadera para el 1er número natural. El segundo paso, conocido como *paso inductivo*, es probar que la afirmación para un número natural cualquiera implica la afirmación para el número natural siguiente. El principio de inducción es el principio que infiere de estos dos pasos que la afirmación es Verdadera para todos los números naturales.

Se basa en el hecho que el conjunto de los números naturales $\mathbb{N}$ es un *conjunto inductivo*.

Definición 2.3.1. (Conjunto inductivo.)

Sea $H \subseteq \mathbb{R}$ un conjunto. Se dice que H es un conjunto *inductivo* si se cumplen las dos condiciones siguientes:

- $1 \in H$,
- $\forall\, x\,,\ x \in H \ \Rightarrow\ x+1 \in H$.

<u>*Ejemplos:*</u>

- $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{N}_{\geq -13}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $[1, +\infty)$ son conjuntos inductivos.
- $\mathbb{N} \cup \{1/2\}$, $\mathbb{Z} - \{0\}$, $[1, 2]$ no son conjuntos inductivos.

De hecho, $\mathbb{N}$ es el "más chico" de los conjuntos inductivos, en el sentido que si $H \subseteq \mathbb{R}$ es un conjunto inductivo, entonces $\mathbb{N} \subseteq H$. El principio de inducción se basa en este hecho: Si logramos probar que un conjunto $H \subseteq \mathbb{N}$ es un conjunto inductivo, entonces $H = \mathbb{N}$.

Sea $p(n)$, $n \in \mathbb{N}$, una afirmación sobre los números naturales, y sea H el subconjunto de $\mathbb{N}$ definido como

$$H := \{n \in \mathbb{N} : p(n) \text{ es Verdadera}\}.$$

Si logramos probar que H es un conjunto inductivo, entonces $H = \mathbb{N}$. Es decir $p(n)$ es Verdadera, $\forall\, n \in \mathbb{N}$.

Dicho de otra manera:

Teorema 2.3.2. (Principio de inducción.)

Sea $p(n)$, $n \in \mathbb{N}$, una afirmación sobre los números naturales. Si p satisface

- (Caso base) *$p(1)$ es Verdadera,*
- (Paso inductivo) *$\forall\, h \in \mathbb{N}$, $p(h)$ Verdadera $\Rightarrow$ $p(h+1)$ Verdadera,*

entonces $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$.

Aquí la hipótesis "$p(h)$ Verdadero" para un h dado se denomina la *hipótesis inductiva* (HI).

Retomemos el ejemplo de la suma de Gauss por el que empezamos, probando por inducción que vale la fórmula dada por Gauss (notemos que la desventaja es que tenemos que conjeturar a priori lo que vale la suma para poder probar la afirmación por inducción).

<u>*Ejemplos:*</u>

1. $\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, $\forall\, n \in \mathbb{N}$:

   Aquí la afirmación $p(n)$ para cada número natural n es:

   $$p(n): \quad \sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

   Queremos probar que $p(n)$ es Verdadera para todo $n \in \mathbb{N}$ por inducción. Lo vamos a hacer con todo detalle.

   - Caso base: ¿Es $p(1)$ Verdadera? ¿Es cierto que $\displaystyle\sum_{i=1}^{1} i = \frac{1(1+1)}{2}$?

     Sí, pues $\displaystyle\sum_{i=1}^{1} i = 1$ y $\displaystyle\frac{1(1+1)}{2} = 1$ también. Luego $p(1)$ V.
   - Paso inductivo: Dado $h \in \mathbb{N}$, ¿es cierto que si suponemos que $p(h)$ es Verdadera, podemos deducir que entonces $p(h+1)$ es Verdadera también? O sea, suponiendo la hipótesis inductiva HI "$p(h)$ Verdadera", es decir $\displaystyle\sum_{i=1}^{h} i = \frac{h(h+1)}{2}$, queremos probar

que entonces $p(h+1)$ es Verdadera también, es decir, queremos probar que

$$\sum_{i=1}^{h+1} i = \frac{(h+1)\big((h+1)+1\big)}{2} = \frac{(h+1)(h+2)}{2}.$$

Pero $\displaystyle\sum_{i=1}^{h+1} i = \Big(\sum_{i=1}^{h} i\Big) + (h+1)$. Y por HI, $\displaystyle\sum_{i=1}^{h} i = \frac{h(h+1)}{2}$, luego

$$\begin{aligned}\sum_{i=1}^{h+1} i = \Big(\sum_{i=1}^{h} i\Big) + (h+1) &\underset{\text{HI}}{=} \frac{h(h+1)}{2} + (h+1)\\ &= \frac{h(h+1)+2(h+1)}{2} = \frac{(h+1)(h+2)}{2},\end{aligned}$$

que es lo que se quería probar.

Es decir hemos probado tanto el caso base como el paso inductivo. Se concluye que $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$.

2. $\dfrac{(2n)!}{n!^2} \leq (n+1)!\,,\ \forall\, n \in \mathbb{N}$:

$$p(n): \quad \frac{(2n)!}{n!^2} \leq (n+1)!.$$

- Caso base: ¿$p(1)$ V? Sí, pues $\dfrac{(2\cdot 1)!}{1!^2} = 2 \leq (1+1)!$.
- Paso inductivo: Dado $h \in \mathbb{N}$, ¿$p(h)$ V $\Rightarrow$ $p(h+1)$ V?
  - HI: $\dfrac{(2h)!}{h!^2} \leq (h+1)!$.
  - Qpq (Quiero probar que) $\dfrac{\big(2(h+1)\big)!}{(h+1)!^2} \leq \big((h+1)+1\big)!$, es decir $\dfrac{(2h+2)!}{(h+1)!^2} \leq (h+2)!$.

Pero

$$\begin{aligned}\frac{(2h+2)!}{(h+1)!^2} = \frac{(2h+2)(2h+1)(2h)!}{\big((h+1)h\big)!^2} &= \frac{2(h+1)(2h+1)(2h)!}{(h+1)^2 h!^2}\\ &= \frac{2(2h+1)}{h+1}\,\frac{(2h)!}{h!^2} \underset{HI}{\leq} \frac{2(2h+1)}{h+1}\,(h+1)!\end{aligned}$$

ya que $\dfrac{2(2h+1)}{h+1} > 0$.

Por lo tanto para probar que $\dfrac{(2h+2)!}{(h+1)!^2} \leq (h+2)!$, alcanza con probar que $\dfrac{2(2h+1)}{h+1} \leq h+2$ porque así se tendrá la cadena de desigualdades:

$$\frac{(2h+2)!}{(h+1)!^2} \underset{HI}{\leq} \frac{2(2h+1)}{h+1}\,(h+1)! \leq (h+2)(h+1)! = (h+2)!$$

Mostremos entonces que $\dfrac{2(2h+1)}{h+1} \leq h+2$. Se tiene

$$\frac{2(2h+1)}{h+1} \leq h+2 \underset{h+1>0}{\iff} 2(2h+1) \leq (h+1)(h+2)$$
$$\iff 4h+2 \leq h^2+3h+2 \iff h \leq h^2 \underset{h>0}{\iff} 1 \leq h$$

(donde siempre verificamos que no cambia el sentido de la desigualdad pues se multiplica/divide por cantidades > 0). La última desigualdad es cierta pues $h \in \mathbb{N}$, por lo tanto hemos logrado probar que $\dfrac{2(2h+1)}{h+1} \leq h+2$, como queríamos.
Concluimos que $p(h)$ V $\Rightarrow$ $p(h+1)$ V.

Es decir hemos probado tanto el caso base como el paso inductivo. Se concluye que $p(n)$ es Verdadera, $\forall\, n \in \mathbb{N}$.

3. $\displaystyle\sum_{k=1}^{n} \frac{1}{\sqrt{k}} \geq \sqrt{n}$, $\forall\, n \in \mathbb{N}$. (En particular esto prueba que la serie $\displaystyle\sum_{k=1}^{\infty} \frac{1}{\sqrt{k}}$ diverge...):

$$p(n): \quad \sum_{k=1}^{n} \frac{1}{\sqrt{k}} \geq \sqrt{n}.$$

- Caso base: ¿$p(1)$ V? Sí, pues $\displaystyle\sum_{k=1}^{1} \frac{1}{\sqrt{k}} = 1 \geq \sqrt{1}$.
- Paso inductivo: Dado $h \in \mathbb{N}$, ¿$p(h)$ V $\Rightarrow$ $p(h+1)$ V?
  - HI: $\displaystyle\sum_{k=1}^{h} \frac{1}{\sqrt{k}} \geq \sqrt{h}$.
  - Qpq $\displaystyle\sum_{k=1}^{h+1} \frac{1}{\sqrt{k}} \geq \sqrt{h+1}$.

Pero

$$\sum_{k=1}^{h+1} \frac{1}{\sqrt{k}} = \sum_{k=1}^{h} \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{h+1}} \underset{HI}{\geq} \sqrt{h} + \frac{1}{\sqrt{h+1}}.$$

Por lo tanto para probar que $\sum_{k=1}^{h+1} \frac{1}{\sqrt{k}} \geq \sqrt{h+1}$, alcanza con probar que
$\sqrt{h} + \frac{1}{\sqrt{h+1}} \geq \sqrt{h+1}$ porque así se tendrá la cadena de desigualdades:

$$\sum_{k=1}^{h+1} \frac{1}{\sqrt{k}} \geq \sqrt{h} + \frac{1}{\sqrt{h+1}} \geq \sqrt{h+1}.$$

Mostremos entonces que $\sqrt{h} + \frac{1}{\sqrt{h+1}} \geq \sqrt{h+1}$. Se tiene

$$\begin{aligned}
\sqrt{h} + \frac{1}{\sqrt{h+1}} \geq \sqrt{h+1} &\iff \frac{\sqrt{h}\cdot\sqrt{h+1}+1}{\sqrt{h+1}} \geq \sqrt{h+1} \\
&\iff \sqrt{h}\cdot\sqrt{h+1}+1 \geq (\sqrt{h+1})^2 = h+1 \\
&\iff \sqrt{h}\cdot\sqrt{h+1} \geq h \iff \sqrt{h(h+1)} \geq h \\
&\underset{h(h+1)\geq 0}{\iff} h(h+1) \geq h^2 \iff h^2+h \geq h^2 \\
&\iff h \geq 0
\end{aligned}$$

La última desigualdad es cierta pues $h \in \mathbb{N}$, por lo tanto hemos logrado probar que $\sum_{k=1}^{h+1} \frac{1}{\sqrt{k}} \geq \sqrt{h+1}$, como queríamos.
Concluimos que $p(h)$ V $\Rightarrow$ $p(h+1)$ V.

Es decir hemos probado tanto el caso base como el paso inductivo. Se concluye que $p(n)$ es Verdadera, $\forall\, n \in \mathbb{N}$.

2.3.1 Inducción "corrida".

Supongamos que queremos probar que para todo $n \geq 5$, se tiene $2^n > n^2$.

Este ejemplo plantea el problema de probar una afirmación que no es cierta para todos los números naturales, pero a partir de cierto número. No podemos aplicar directamente el principio de inducción ya que si bien se satisface el caso base $p(1)$ Verdadera (pues $2 = 2^1 > 1^2 = 1$), no se satisface $p(2)$ Verdadera, pues $2^2 = 4$ y por lo tanto no es cierto que para $n = 2$ se tiene $2^n > n^2$. Por lo tanto no vamos a poder deducir de $p(1)$ Verdadera que

$p(2)$ es Verdadera! Notemos que tampoco es cierta la afirmación para $n = 3$ (pues $2^3 = 8 < 9 = 3^2$) ni para $n = 4$ (pues $2^4 = 16 = 4^2$).

También podríamos querer probar que una afirmación es cierta a partir de cierto número entero negativo n_0, por ejemplo $n_0 = -11$. ¿Será cierto que podemos usar el mismo principio de inducción, pero "corriéndolo"? es decir ¿verificando el caso base $n_0 = 5$ en el ejemplo (o $n_0 = -11$) y luego probar $p(h)$ V $\Rightarrow$ $p(h+1)$ V, $\forall\, h \geq n_0$?

La respuesta bastante intuitiva es que "sí", y se puede mostrar que es así mostrando que el conjunto $H = \{n \in \mathbb{N} : p(n-1+n_0) \text{ es Verdadera}\}$ es un conjunto inductivo, pues así $1 \in H \Leftrightarrow p(1-1+n_0) = p(n_0)$ es Verdadero.

De esta manera se prueba que es el análogo "corrido" del Principio de Inducción formulado en el Teorema 2.3.2:

Teorema 2.3.3. (Principio de inducción "corrido".)

Sea $n_0 \in \mathbb{Z}$ y sea $p(n), n \geq n_0$, una afirmación sobre $\mathbb{Z}_{\geq n_0}$. Si p satisface

- (Caso base) *$p(n_0)$ es Verdadera,*
- (Paso inductivo) *$\forall\, h \geq n_0$, $p(h)$ Verdadera $\Rightarrow$ $p(h+1)$ Verdadera,*

entonces $p(n)$ es Verdadero, $\forall\, n \geq n_0$.

<u>*Ejemplos:*</u>

1. Probar que para todo $n \geq 5$ se tiene $2^n > n^2$.

   Vamos a probarlo por medio del principio de inducción corrido.

   $$p(n): \quad 2^n > n^2$$

   - Caso base: ¿$p(5)$ V? Sí, pues $32 = 2^5 > 5^2 = 25$.
   - Paso inductivo: Dado $h \geq 5$, ¿$p(h)$ V $\Rightarrow$ $p(h+1)$ V?
     - HI: $2^h > h^2$ (recordando $h \geq 5$).
     - Qpq $2^{h+1} > (h+1)^2$, es decir $2 \cdot 2^h > h^2 + 2h + 1$.

     Pero por HI, $2 \cdot 2^h > 2\,h^2$. Por lo tanto para probar que $2 \cdot 2^h > h^2 + 2h + 1$, alcanza con probar que $2\,h^2 \geq h^2 + 2h + 1$, pues en ese caso se tendría la cadena de desigualdades

     $$2 \cdot 2^h > 2\,h^2 \geq h^2 + 2h + 1,$$

     y al haber en la cadena una desigualdad estricta $>$, la desigualdad que vale entre el miembro más a la izquierda y el más a la derecha es $>$ también. Se tiene:

     $$2\,h^2 \geq h^2 + 2h + 1 \iff h^2 \geq 2h + 1 \iff h^2 - 2h - 1 \geq 0.$$

Pero al ser $h \geq 5$, se tiene

$$h^2-2h-1 = h\cdot h-2h-1 \geq 5h-2h-1 = 3h-1 \geq 3\cdot 5-1 \geq 14 \geq 0.$$

(Notemos que la desigualdad $h^2-2h-1 \geq 0$ no se cumple para $h=1$ ni para $h=2$, sólo se cumple de hecho a partir de $h=3$.)
Concluimos que para $h \geq 5$, $p(h)$ V $\Rightarrow$ $p(h+1)$ V.

Es decir hemos probado tanto el caso base como el paso inductivo. Se concluye que $p(n)$ es Verdadera, para todo $n \geq 5$.

2. *(El distribuidor automático.)*

Un distribuidor automático sólo tiene billetes de \$ 2 y \$ 5. Mostrar que puede dar cualquier suma n entera de \$, con $n \geq 4$.

$$p(n): \quad \exists\, i,j \in \mathbb{N}_0 \text{ t.q. } \quad n = i\cdot 2 + j\cdot 5.$$

- Caso base: ¿$p(4)$ V? Sí, pues $4 = 2\cdot 2 + 0\cdot 5$.
- Paso inductivo: Dado $h \geq 4$, ¿$p(h)$ V $\Rightarrow$ $p(h+1)$ V?
  - HI: $\exists\, i,j \in \mathbb{N}_0$ tales que $h = i\cdot 2 + j\cdot 5$ (recordando $h \geq 4$).
  - Qpq $\exists\, i',j' \in \mathbb{N}_0$ tales que $h+1 = i'\cdot 2 + j'\cdot 5$.

  Por HI, $\exists\, i,j \in \mathbb{N}_0$ tales que $h = i\cdot 2 + j\cdot 5$.

  - Si se usó algún billete de 5 para obtener h, es decir si $j \geq 1$, reemplazar ese billete de 5 por 3 billetes de 2 (lo que da 6), o sea reemplazar j por $j' = j-1$ (que satisface $j' \geq 0$ pues $j \geq 1$) y reemplazar i por $i' = i+3$:

    $$i'\cdot 2 + j'\cdot 5 = (i+3)\cdot 2 + (j-1)\cdot 5 = i\cdot 2 + j\cdot 5 + 6 - 5 = n+1.$$

  - Si no se usó ningún billete de 5 para obtener h, es decir si $j = 0$, se tiene $h = i\cdot 2$. Pero como $h \geq 4$, entonces $i \geq 2$ y podemos reemplazar dos billetes de 2 por un billete de 5, o sea reemplazar i por $i' = i-2$ (que satisface $i' \geq 0$ pues $i \geq 2$) y reemplazar $j = 0$ por $j' = 1$:

    $$i'\cdot 2 + j'\cdot 5 = (i-2)\cdot 2 + 5 = i\cdot 2 + 5 - 4 = h+1.$$

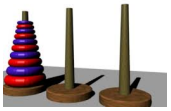
  Concluimos que en todos los casos logramos mostrar que existen $i',j' \in \mathbb{N}_0$ tales que $h+1 = i'\cdot 2 + j'\cdot 5$. Así probamos el paso inductivo.

Es decir hemos probado tanto el caso base como el paso inductivo. Se concluye que $p(n)$ es Verdadera, $\forall\, n \geq 4$.

2.4 Sucesiones definidas por recurrencia.

Los ejemplos siguientes muestran sucesiones definidas por recurrencia, de la misma manera que fueron definidos por recurrencia la sumatoria y la productoria.

Las torres de Hanoi.



El problema de las torres de Hanoi fue inventado por el matemático francés Edouard Lucas en 1883.

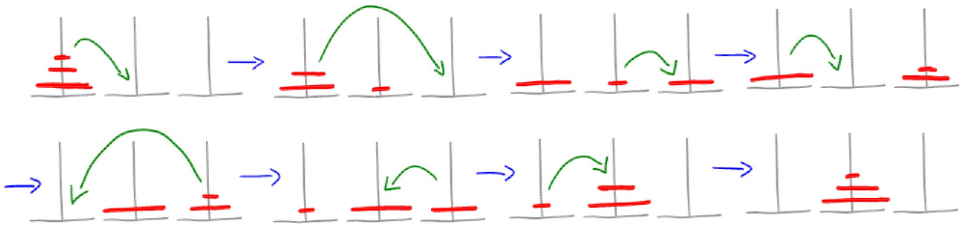
Tenemos 3 estacas, y un cierto número n de discos de distinto diámetro ensartados en la primer estaca, ordenados por tamaño, de mayor a menor estando el menor encima, como en la foto arriba.

El objetivo del juego es lograr mover toda la pila de discos a otra estaca, con las condiciones siguientes:

- no se puede mover más de un disco a la vez
- sólo se puede sacar el disco de la parte superior de cada pila de discos
- en todo momento los discos de cada estaca deben estar ordenados por tamaño, de mayor a menor con el menor encima.

¿Cuántos movimientos alcanzan para realizar esta operación? Por ejemplo para 2 discos podemos realizar los movimientos siguientes:

O sea alcanza con 3 movimientos. Y para 3 discos podemos hacer lo siguiente:



Y por lo tanto nos alcanza con 7 movimientos. También nos podemos dar cuenta a este nivel que saber cómo mover 3 discos ayuda a mover 4 discos, ya que para mover los 4 discos, podemos primero pasar los 3 discos de arriba a otra estaca, realizando 7 movimientos (ya que aquí al quedar el disco más grande abajo en la primer estaca, podemos usar tranquilamente esa estaca sin contradecir las reglas del juego), luego mover el disco más grande que quedó solo a la estaca libre (1 movimiento), y luego volver a mover la pila de los 3 discos arriba del más grande realizando nuevamente 7 movimientos. Así para mover 4 discos nos alcanzan $2 \cdot 7 + 1 = 15$ movimientos.

Este razonamiento se generaliza para $n+1$ discos: Llamemos a a_n una cantidad de movimientos suficientes para mover n discos. Por ejemplo $a_1 = 1,\ a_2 = 3, a_3 = 7$.

Para mover los $n+1$ discos podemos empezar moviendo los n de arriba a otra estaca, con a_n movimientos, luego pasar el disco grande a la estaca libre, con 1 movimiento, y luego mover la pila de los n discos arriba del disco grande, con nuevamente a_n movimiento. Así obtenemos $a_{n+1} = 2a_n + 1$.

Notemos que si queremos deducir de esta definición cuánto vale a_7 vamos a necesitar conocer cuánto vale a_6, luego a_5, etc. hasta necesitar conocer a_1.

Una sucesión definida de esta manera, como aquí:

$$a_1 = 1, \quad a_{n+1} = 2a_n + 1,\ \forall\, n \in \mathbb{N}$$

es una sucesión definida *por recurrencia*, ya que para calcular un término necesitamos conocer el anterior. Además de necesitar conocer el caso base $n = 1$ obviamente, sino no sabríamos por donde empezar.

Observación 2.4.1. Esta definición por recurrencia permite obtener el valor de a_n para cualquier $n \in \mathbb{N}$: si queremos ser formales, podemos observar que el conjunto

$$H = \{n \in \mathbb{N} :\ a_n \text{ está definida}\}$$

es un subconjunto inductivo de $\mathbb{N}$ (pues $1 \in H$ ya que $a_1 = 1$, y si $h \in H$, entonces $h+1 \in H$ pues $a_{h+1} = 2a_h + 1$), y por lo tanto coincide con $\mathbb{N}$. (Así definimos en forma recursiva la sumatoria $\displaystyle\sum_{i=1}^{n} a_n$ y la productoria $\displaystyle\prod_{i=1}^{n} a_n$.)

Ahora nos interesa deshacernos de la recurrencia: habrá una fórmula que me diga quién es el término general a_n de la sucesión, sin tener que calcular el término anterior y el anterior y el anterior?

Veamos:

$$a_1 = 1, a_2 = 3, a_3 = 7, a_4 = 15, a_5 = 31, a_6 = 63.$$

Pareciera ser que puede valer $a_n = 2^n - 1\,,\ \forall\, n \in \mathbb{N}$. Conjeturemos luego que la sucesión definida por recurrencia como

$$a_1 = 1, \quad a_{n+1} = 2a_n + 1,\ \forall\, n \in \mathbb{N}$$

satisface

$$a_n = 2^n - 1,\ \forall\, n \in \mathbb{N}.$$

Lo podemos probar por inducción:

$$p(n): \quad a_n = 2^n - 1,\ \forall\, n \in \mathbb{N}.$$

- Caso base: ¿$p(1)$ V? Sí, pues $2^1 - 1 = 1 = a_1$.
- Paso inductivo: Dado $h \in \mathbb{N}$, ¿$p(h)$ V $\Rightarrow$ $p(h+1)$ V?
  - HI: $a_h = 2^h - 1$
  - Qpq $a_{h+1} = 2^{h+1} - 1$.

  Pero por definición de la sucesión, sabemos que $a_{h+1} = 2a_h + 1$. Luego

  $$a_{h+1} \;=\; 2a_h + 1 \underset{HI}{=} 2(2^h - 1) + 1 \;=\; 2^{h+1} - 2 + 1 \;=\; 2^{h+1} - 1$$

  como se quería probar.

Es decir hemos probado tanto el caso base como el paso inductivo. Se concluye que $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$.

Pregunta 1: Acabamos de probar que con $2^n - 1$ movimientos se puede resolver el problema de las torres de Hanoi con n discos. ¿Será éste el mínimo número posible?

Pregunta 2: Con cuál de las dos formulaciones: $a_1 = 1,\ a_{n+1} = 2a_n + 1,\ \forall\, n \in \mathbb{N}$, o $a_n = 2^n - 1,\ \forall\, n \in \mathbb{N}$ se logra hacer menos cuentas si se quiere calcular por ejemplo a_{256}? La respuesta se encuentra en el capítulo sobre enteros, cuando se introducen los sistemas de numeración, en particular el sistema binario.

Un ejemplo más.

Sea la sucesión definida por recurrencia como

$$a_1 = 1, \quad a_{n+1} = \left(\sqrt{a}_n - (n+1)\right)^2,\ \forall\, n \in \mathbb{N}.$$

O sea

$$a_1 = 1, a_2 = (\sqrt{1}-2)^2 = 1,\ a_3 = (\sqrt{1}-3)^2 = 4,\ a_4 = (\sqrt{4}-4)^2 = 4,$$
$$a_5 = (\sqrt{4}-5)^2 = 9,\ a_6 = (\sqrt{9}-6)^2 = 9,\ \ldots.$$

Pareciera que va dando los cuadrados, repetidos dos veces cada uno, o sea $a_{2n-1} = a_{2n} = n^2$, $\forall\, n \in \mathbb{N}$. Escrito en términos de a_n, para todo $n \in \mathbb{N}$ se tiene

$$a_n = \begin{cases} \left(\frac{n+1}{2}\right)^2 & \text{si} \quad n \text{ es impar} \\ \left(\frac{n}{2}\right)^2 & \text{si} \quad n \text{ es par.} \end{cases}$$

Probemoslo por inducción.

$$p(n): \quad a_n = \begin{cases} \left(\frac{n+1}{2}\right)^2 & \text{si} \quad n \text{ es impar} \\ \left(\frac{n}{2}\right)^2 & \text{si} \quad n \text{ es par} \end{cases}$$

- Caso base: ¿$p(1)$ V? Sí, pues como 1 es impar, $\left(\frac{1+1}{2}\right)^2 = 1 = a_1$.
- Paso inductivo: Dado $h \in \mathbb{N}$, ¿$p(h)$ V $\Rightarrow$ $p(h+1)$ V?
  - HI: $a_h = \left(\frac{h+1}{2}\right)^2$ si h es impar y $a_h = \left(\frac{h}{2}\right)^2$ si h es par.
  - Qpq $a_{h+1} = \left(\frac{h+2}{2}\right)^2$ si $h+1$ es impar y $a_{h+1} = \left(\frac{h+1}{2}\right)^2$ si $h+1$ es par.

  Pero por definición de la sucesión, sabemos que $a_{h+1} = \left(\sqrt{a_h} - (h+1)\right)^2$. Luego:
  - Si $h+1$ es impar, es que h es par, y por lo tanto por HI, $a_h = \left(\frac{h}{2}\right)^2$. Así,

$$a_{h+1} = \left(\sqrt{a_h} - (h+1)\right)^2 \underset{HI}{=} \left(\sqrt{\left(\frac{h}{2}\right)^2} - (h+1)\right)^2$$
$$= \left(\frac{h}{2} - (h+1)\right)^2 = \left(-\frac{(h+2)}{2}\right)^2 = \left(\frac{h+2}{2}\right)^2.$$

  - Si $h+1$ es par, es que h es impar, y por lo tanto por HI, $a_h = \left(\frac{h+1}{2}\right)^2$. Así,

$$a_{h+1} = \left(\sqrt{a_h} - (h+1)\right)^2 \underset{HI}{=} \left(\sqrt{\left(\frac{h+1}{2}\right)^2} - (h+1)\right)^2$$
$$= \left(\frac{h+1}{2} - (h+1)\right)^2 = \left(-\frac{(h+1)}{2}\right)^2 = \left(\frac{h+1}{2}\right)^2.$$

Es decir hemos probado tanto el caso base como el paso inductivo. Se concluye que $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$.

2.5 Inducción completa.

2.5.1 Inducción completa – Un caso particular.

Empecemos considerando la sucesión $(a_n)_{n\in\mathbb{N}}$ definida recursivamente de la manera siguiente:

$$a_1 = 5, \quad a_{n+2} = 5a_{n+1} - 6a_n, \ \forall\, n \in \mathbb{N}.$$

¿Se puede decidir quién es a_2 ? Se ve que en este caso no, ya que la sucesión requiere saber lo que valen dos términos anteriores cada vez: para conocer a_2 necesitaríamos conocer a_1 y a_0, y no sabemos quién es a_0. Pero si definimos la sucesión a_n como

$$a_1 = 5, \ a_2 = 13, \quad a_{n+2} = 5a_{n+1} - 6a_n, \ \forall\, n \in \mathbb{N}, \tag{2.1}$$

al tener los dos primeros términos de la sucesión dados, podemos recursivamente deducir el valor de todos los demás:

$$a_1 = 5, \ a_2 = 13, \ a_3 = 5 \cdot 13 - 6 \cdot 5 = 35, \ a_4 = 5 \cdot 35 - 6 \cdot 13 = 97 \ \ldots$$

Observación 2.5.1. Cuando una sucesión está definida por recurrencia usando los dos términos anteriores, y se dan los valores de los dos términos iniciales a_1 y a_2, entonces a_n está definido para cualquier $n \in \mathbb{N}$: si queremos ser formales, podemos observar que el conjunto

$$H = \{n \in \mathbb{N} : \ a_n \ \text{ está definida}\}$$

coincide con $\mathbb{N}$. Pues supongamos que no: entonces existe un $n_0 \in \mathbb{N}$ tal que a_{n_0} no está definido, y podemos tomar el más chico de todos con esa propiedad de no estar definido. Se sabe que $n_0 \geq 3$ pues a_1 y a_2 están definidos. Pero si $n_0 \geq 3$, se tiene que a_{n_0} está definido por medio de los dos términos anteriores (que están definidos pues a_{n_0} era el más chico de todos los que no estaban definidos. Por lo tanto a_{n_0} está definido. Esto contradice el hecho que a_{n_0} no estaba definido, o sea que $H \neq \mathbb{N}$.

En este razonamiento no probamos directamente que H era un conjunto inductivo, sino usamos lo que se llama *el principio de buena ordenación* (que vale para $\mathbb{N}$) y que es equivalente al Principio de Inducción, como comentaremos en el Apéndice.

Volviendo al Ejemplo (2.1), alguien muy avezado, o un pajarito, o un "oráculo" me puede decir "Oiga, esto da $2^n + 3^n$"!

Supongamos que queremos probar entonces, por inducción, que el término general de la sucesión definida por $a_1 = 5$, $a_2 = 13$, $a_{n+2} = 5a_{n+1} - 6a_n$, $\forall\, n \in \mathbb{N}$, es $a_n = 2^n + 3^n$, $\forall\, n \in \mathbb{N}$.

El caso base $a_1 = 2^1 + 3^1$ es correcto, pero cuando queremos deducir de la HI $a_h = 2^h + 3^h$ que entonces $a_{h+1} = 2^{h+1} + 3^{h+1}$, nos vemos en problemas porque necesitaríamos una HI para a_h y una para a_{h-1}. Por suerte hay una variante del principio de inducción que soluciona ese problema:

Teorema 2.5.2. (Principio de inducción - II)

Sea $p(n)$, $n \in \mathbb{N}$, una afirmación sobre los números naturales. Si p satisface

- (Casos base) *$p(1)$ y $p(2)$ son Verdaderas,*
- (Paso inductivo) *$\forall\, h \in \mathbb{N}$, $p(h)$ y $p(h+1)$ Verdaderas $\Rightarrow$ $p(h+2)$ Verdadera,*

entonces $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$.

<u>*Ejemplo:*</u> Probar que el término general de la sucesión $(a_n)_{n\in\mathbb{N}}$ definida por

$$a_1 = 5,\ a_2 = 13 \quad a_{n+2} = 5a_{n+1} - 6a_n,\ \forall\, n \in \mathbb{N},$$

es $a_n = 2^n + 3^n$, $\forall\, n \in \mathbb{N}$.

Por inducción, aplicando el Teorema 2.5.2.

$$p(n): \quad a_n = 2^n + 3^n.$$

- Casos base: ¿$p(1)$ y $p(2)$ V? Sí, pues $2^1 + 3^1 = 5 = a_1$ y $2^2 + 3^2 = 13 = a_2$.
- Paso inductivo: Dado $h \in \mathbb{N}$, ¿$p(h)$ V y $p(h+1)$ V $\Rightarrow$ $p(h+2)$ V?
  - HI: $a_h = 2^h + 3^h$ y $a_{h+1} = 2^{h+1} + 3^{h+1}$.
  - Qpq $a_{h+2} = 2^{h+2} + 3^{h+2}$.

  Pero por definición de la sucesión, sabemos que para $h \geq 1$, $a_{h+2} = 5a_{h+1} - 6a_h$. Luego

$$\begin{aligned} a_{h+2} = \ & 5a_{h+1} - 6a_h \underset{HI}{=} 5\,(2^{h+1} + 3^{h+1}) - 6\,(2^h + 3^h) \\ = \ & 10 \cdot 2^h + 15 \cdot 3^h - 6 \cdot 2^h - 6 \cdot 3^h \ = \ 4 \cdot 2^h + 9 \cdot 3^h \ = \ 2^{h+2} + 3^{h+2} \end{aligned}$$

  como se quería probar.

Es decir hemos probado tanto los casos base como el paso inductivo. Se concluye que $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$.

Observación 2.5.3. Notar que por como está definida la sucesión (por medio de los dos términos anteriores) es indispensable verificar que la afirmación $p(n)$ es Verdadera para los dos casos base $p(1)$ y $p(2)$, pues si no la verificáramos para 2 no podríamos deducir que $p(3)$ es Verdadera. Y podríamos –al hacer ese error– deducir algo completamente falso: que la sucesión definida por $a_1 = 5,\ a_2 = 0,\ a_{n+2} = 5a_{n+1} - 6a_n,\ \forall\, n \in \mathbb{N}$, también tiene como término general $a_n = 2^n + 3^n$.

Este principio de inducción admite la misma versión "corrida" que el que vimos en la sección anterior:

Teorema 2.5.4. (Principio de inducción - II "corrido")

Sea $n_0 \in \mathbb{Z}$ *y sea* $p(n), n \geq n_0$, *una afirmación sobre* $\mathbb{Z}_{\geq n_0}$. *Si* p *satisface*

- (Casos base) $p(n_0)$ *y* $p(n_0 + 1)$ *son Verdaderas,*
- (Paso inductivo) $\forall\, h \geq n_0$, $p(h)$ *y* $p(h+1)$ *Verdaderas* $\Rightarrow$ $p(h+2)$ *Verdadera,*

entonces $p(n)$ *es Verdadero,* $\forall\, n \geq n_0$.

2.5.2 La sucesión de Fibonacci.

La famosa sucesión de Fibonacci debe su nombre a *Leonardo Pisano Bigollo*, más conocido como *Fibonacci*, $\sim$ 1170-1240, famoso también por haber difundido en Europa el sistema de numeración indo-arábigo que utilizamos, que emplea una notación posicional y el cero para marcar una posición nula.

Fibonacci publicó Liber Abaci en el año 1202, donde entre otras cosas propuso el siguiente problema: si colocamos una pareja de conejos bebés en un área cerrada, ¿cuántos conejos habrá luego de n meses si

- los conejos nunca mueren,
- cada pareja de conejos produce una nueva pareja de conejos cada mes
- y comienza a tener parejitas luego de dos meses de nacida?

En el mes 0, no hay conejos (porque todavía no los colocamos). En el mes 1, tenemos una pareja de conejos bebés (que colocamos). En el mes 2, tenemos la misma única pareja de conejos, pero ya son adultos y van a empezar a tener parejitas. En el mes 3, tenemos la pareja original (adulta) más una pareja bebé (hijos de la pareja original), o sea tenemos dos parejas. En el mes 4, la pareja original tiene otra pareja de bebés, y además la pareja bebé

del mes 3 se convierte en adulta (tenemos 3 parejas). En el mes 5, las dos parejas adultas que hay tienen parejas bebés y la pareja bebé que había se convierte en adulta: tenemos 5 parejas. Si calculamos algunos números más, vemos que los siguientes meses tenemos: 8, 13, 21, 34 ...

Para encontrar una fórmula para esta sucesión, llamenos A_n al número de parejas adultas en el mes n y B_n al número de parejas bebés en el mes n. Llamamos también F_n al total de parejas en el mes n, o sea $F_n = A_n + B_n$. Obtenemos la tabla siguiente:

Mes	A_n	B_n	F_n
0	0	0	0
1	0	1	1
2	1	0	1
3	1	1	2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	A_n	B_n	$A_n + B_n$
$n+1$	$A_n + B_n$	A_n	$2A_n + B_n$
$n+2$	$2A_n + B_n$	$A_n + B_n$	$3A_n + 2B_n$

Notemos que el número total de parejas de conejos en el mes $n+2$ es el número que había en el mes $n+1$ más el número de parejas adultas del mes $n+1$, que coincide con el número de parejas del mes n. Luego la sucesión F_n satisface la recurrencia $F_{n+2} = F_{n+1} + F_n$, para todo $n \geq 0$. Además, los primeros dos valores de la sucesión son $F_0 = 0$ y $F_1 = 1$. Estas condiciones definen una única sucesión, que se llama la sucesión de Fibonacci $(F_n)_{n\in\mathbb{N}_0}$:

$$F_0 = 0,\ F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n,\ \forall\, n \in \mathbb{N}_0,$$

cuyos primeros términos son

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233$$

Esta sucesión está fuertemente relacionada con el *Número de Oro*, o *Número de la proporción divina*, o *de la proporción áurea,* que aparece mucho en la naturaleza, en el arte, en la arquitectura, en medicina. Este número surge de preguntarse, si tenemos un segmento dividido en dos partes de longitudes Φ y 1, con $\Phi \geq 1$, ¿cómo tiene que ser Φ para que la proporción entre esas dos partes Φ y 1 sea la misma que la proporción entre todo el segmento $\Phi + 1$ y Φ. Se tiene

$$\frac{\Phi}{1} = \frac{\Phi + 1}{\Phi}, \quad \text{i.e.} \quad \Phi^2 = \Phi + 1, \quad \text{i.e.} \quad \Phi^2 - \Phi - 1 = 0.$$

Las dos raíces de la ecuación $X^2 - X - 1 = 0$ son

$$\Phi = \frac{1+\sqrt{5}}{2} \sim 1,61803\ \geq 1 \quad \text{y} \quad \overline{\Phi} = \frac{1-\sqrt{5}}{2}\ < 0$$

(aquí $\overline{\Phi}$ es solo una notación, no significa que es el conjugado en el sentido de número complejo). Notemos que vale que $\Phi^2 = \Phi + 1$ y $\overline{\Phi}^2 = \overline{\Phi} + 1$, pues ambas cantidades satisfacen la ecuación $X^2 - X - 1 = 0$. Además se satisfacen las relaciones

$$\Phi^0 - \overline{\Phi}^0 = 1 - 1 = 0 \quad \text{y} \quad \Phi^1 - \overline{\Phi}^1 = \frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2} = \frac{2\sqrt{5}}{2} = \sqrt{5}. \tag{2.2}$$

De distintas maneras se puede probar el resultado siguiente, que describe el término general de la sucesión de Fibonacci. Veremos algunas a continuación. Pero aprovechemos ahora para practicar un poco más el principio de inducción con esta afirmación.

Proposición 2.5.5. (Término general de la Sucesión de Fibonacci.)

$$F_n = \frac{1}{\sqrt{5}}(\Phi^n - \overline{\Phi}^n), \quad \forall\, n \in \mathbb{N}_0.$$

Demostración. Lo probamos por el principio de inducción corrido a $n \geq 0$ presentado en el Teorema 2.5.4.

$$p(n): \quad F_n = \frac{1}{\sqrt{5}}\left(\Phi^n - \overline{\Phi}^n\right).$$

- Casos base: ¿$p(0)$ y $p(1)$ V? Sí, pues por las relaciones (2.2),

$$\frac{1}{\sqrt{5}} \cdot 0 = 0 = F_0 \ \text{ y } \ \frac{1}{\sqrt{5}}(\Phi^1 - \overline{\Phi}^1) = \frac{1}{\sqrt{5}} \cdot \sqrt{5} = 1 = F_1.$$

- Paso inductivo: Dado $h \in \mathbb{N}$, ¿$p(h)$ V y $p(h+1)$ V $\Rightarrow$ $p(h+2)$ V?
  - HI: $F_h = \frac{1}{\sqrt{5}}\left(\Phi^h - \overline{\Phi}^h\right)$ y $F_{h+1} = \frac{1}{\sqrt{5}}\left(\Phi^{h+1} - \overline{\Phi}^{h+1}\right)$.
  - Qpq $F_{h+2} = \frac{1}{\sqrt{5}}\left(\Phi^{h+2} - \overline{\Phi}^{h+2}\right)$.

  Pero por definición de la sucesión, sabemos que para $h \geq 0$, $F_{h+2} = F_{h+1} + F_h$. Luego

$$\begin{aligned} F_{h+2} = \ F_{h+1} + F_h \ &\underset{HI}{=} \ \frac{1}{\sqrt{5}}\left(\Phi^h - \overline{\Phi}^h\right) + \frac{1}{\sqrt{5}}\left(\Phi^{h+1} - \overline{\Phi}^{h+1}\right) \\ &= \ \frac{1}{\sqrt{5}}\Big(\Phi^h - \overline{\Phi}^h + \Phi^{h+1} - \overline{\Phi}^{h+1}\Big) \ = \ \frac{1}{\sqrt{5}}\Big(\Phi^h(1+\Phi) - \overline{\Phi}^h(1+\overline{\Phi})\Big) \\ &= \frac{1}{\sqrt{5}}\Big(\Phi^h \cdot \Phi^2 - \overline{\Phi}^h \cdot \overline{\Phi}^2\Big) \ = \ \frac{1}{\sqrt{5}}\Big(\Phi^{h+2} - \overline{\Phi}^{h+2}\Big) \end{aligned}$$

  como se quería probar.

Es decir hemos probado tanto los casos base como el paso inductivo. Se concluye que $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$. □

Una propiedad (a priori sorprendente) de la sucesión de Fibonacci, que permite de hecho mostrar por qué el Número de Oro Φ aparece naturalmente en este contexto, es la *Identidad de Cassini*, que fue descubierta en 1680 por el astrónomo francés de origen italiano *Gian Domenico Cassini*, 1625-1712.

Proposición 2.5.6. (Identidad de Cassini.)

$$F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n, \quad \forall\, n \in \mathbb{N}.$$

Por ejemplo,

$$F_2F_0 - F_1^2 = 1 \cdot 0 - 1 = (-1)^1,\ F_3F_1 - F_2^2 = 2 \cdot 1 - 1^2 = 1 = (-1)^2.$$

Demostración. Lo probamos por inducción:

$$p(n): \quad F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n.$$

- Caso base: ¿$p(1)$ V? Sí, lo verificamos arriba.
- Paso inductivo: Dado $h \in \mathbb{N}$, ¿$p(h)$ V $\Rightarrow$ $p(h+1)$ V?
  - HI: $F_{h+1} \cdot F_{h-1} - F_h^2 = (-1)^h$.
  - Qpq $F_{h+2} \cdot F_h - F_{h+1}^2 = (-1)^{h+1}$.

  Pero por definición de la sucesión, sabemos que para $h \geq 1$, $F_{h+2} = F_{h+1} + F_h$ y $F_{h+1} = F_h + F_{h-1}$ (pues en este último caso, $h \geq 1$ implica $h - 1 \geq 0$, luego F_{h-1} está definida). Luego

$$\begin{aligned} F_{h+2} \cdot F_h - F_{h+1}^2 &= (F_{h+1} + F_h) \cdot F_h - (F_h + F_{h-1}) \cdot F_{h+1} \\ &= F_{h+1} \cdot F_h + F_h^2 - F_h \cdot F_{h+1} - F_{h-1} \cdot F_{h+1} \\ &= F_h^2 - F_{h-1} \cdot F_{h+1} \ = \ -\big(F_{h-1} \cdot F_{h+1} - F_h^2\big) \\ &\underset{HI}{=} -(-1)^h \ = \ (-1)^{h+1} \end{aligned}$$

  como se quería probar.

Es decir hemos probado tanto los casos base como el paso inductivo. Se concluye que $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$. □

Esto implica que $\dfrac{F_{n+1}}{F_n} - \dfrac{F_n}{F_{n-1}} = \dfrac{(-1)^n}{F_{n-1}F_n}$. Así,

$$\left|\frac{F_{n+1}}{F_n} - \frac{F_n}{F_{n-1}}\right| = \frac{1}{F_{n-1}F_n}.$$

Esto implica que para $m > n$,

$$\begin{aligned}\left|\frac{F_{m+1}}{F_m} - \frac{F_n}{F_{n-1}}\right| &\leq \sum_{i=n}^{m}\left|\frac{F_{i+1}}{F_i} - \frac{F_i}{F_{i-1}}\right| \leq \sum_{i=n}^{m}\frac{1}{F_{i-1}F_i} \\ &\leq \sum_{i=n}^{m}\frac{1}{(i-1)i} = \sum_{i=n}^{m}\Big(\frac{1}{i-1} - \frac{1}{i}\Big) = \frac{1}{n-1} - \frac{1}{m} \\ &= \frac{m-n+1}{(n-1)m} \underset{n\to\infty}{\to} 0.\end{aligned}$$

ya que es fácil ver que $F_i \geq i$, y esto implica $\dfrac{1}{F_{i-1}F_i} \leq \dfrac{1}{(i-1)i}$. Por lo tanto, para los que saben un poco de Análisis, la sucesión $(\dfrac{F_{n+1}}{F_n})_{n\in\mathbb{N}}$ es de Cauchy, y luego converge.

Sea entonces $F := \lim_{n\to\infty}\frac{F_{n+1}}{F_n}$. Se observa que $F \geq 1$ dado que $F_{n+1} \geq F_n$. Entonces

$$F = \lim_{n\to\infty}\frac{F_{n+1}}{F_n} = \lim_{n\to\infty}\frac{F_n + F_{n-1}}{F_n} = \lim_{n\to\infty}\big(1 + \frac{F_{n-1}}{F_n}\big) = 1 + \lim_{n\to\infty}\frac{F_{n-1}}{F_n} = 1 + \frac{1}{F}.$$

Por lo tanto el límite F satisface la ecuación $F = 1 + \frac{1}{F}$, o equivalentemente la ecuación $F^2 = F + 1$. Se concluye que $F = \Phi$, ya que es la raíz ≥ 1 del polinomio $X^2 - X - 1$.

¿No es esto fantástico? ¡La proporción entre dos números de Fibonacci consecutivos tiende a la proporción divina $\Phi = \dfrac{1+\sqrt{5}}{2} \sim 1,61803$! Por ejemplo $\dfrac{F_{12}}{F_{11}} = \dfrac{144}{89} \sim 1,61798$ y $\dfrac{F_{13}}{F_{12}} = \dfrac{233}{144} \sim 1,61806$.

2.5.3 Sucesiones de Lucas.

Veamos ahora un método muy clásico que permite determinar el término general de todas las sucesiones de Lucas, que son sucesiones "de tipo Fibonacci" definidas recursivamente mediante los dos términos inmediato anteriores.

Una *sucesión de Lucas* es una sucesión $(a_n)_{n\in\mathbb{N}_0}$ definida recursivamente por

$$a_0 = a,\ a_1 = b, \quad a_{n+2} = c\,a_{n+1} + d\,a_n,\ \forall\, n \in \mathbb{N}_0,$$

donde $a, b, c, d \in \mathbb{C}$ son números dados.

En lo que sigue desarrollamos un método que permite determinar el término general a_n de la sucesión de Lucas definida arriba.

Consideremos la ecuación $X^2 - cX - d = 0$ asociada a la sucesión de Lucas (que se obtiene de la expresión $a_2 - c\,a_1 - d\,a_0 = 0$ y luego reemplazando a_2 por X^2, a_1 por X y a_0 por 1).

Observemos que en el caso de la sucesión de Fibonacci, la ecuación asociada es $X^2 - X - 1 = 0$, *justamente la ecuación que tiene como raíces a* Φ *y* $\overline{\Phi}$.

Supongamos que estamos en el caso en que $X^2 - cX - d$ tiene dos raíces distintas r y $\overline{r}$. Observemos que estas dos raíces r y $\overline{r}$ satisfacen las relaciones

$$r^2 = c\,r + d \quad \text{y} \quad \overline{r}^2 = c\,\overline{r} + d. \tag{2.3}$$

Afirmación 1: Las sucesiones $(r^n)_{n\in\mathbb{N}_0}$, $(\overline{r}^n)_{n\in\mathbb{N}_0}$, y más aún cualquier combinación lineal de ellas

$$(\gamma_n)_{n\in\mathbb{N}_0} = (\alpha\, r^n + \beta\, \overline{r}^n)_{n\in\mathbb{N}_0}$$

satisfacen la misma recurrencia

$$\gamma_{n+2} = c\,\gamma_{n+1} + d\,\gamma_n,\ \forall\, n \in \mathbb{N}$$

que la sucesión de Lucas $(a_n)_{n\in\mathbb{N}_0}$ original, de la cuál queremos determinar el término general.

Esto es cierto pues

$$\begin{aligned}\gamma_{n+2} \underset{def}{=}\ & \alpha\, r^{n+2} + \beta\, \overline{r}^{n+2} \ =\ \alpha\, r^2\, r^n + \beta\, \overline{r}^2\, \overline{r}^n \\ =\ & \alpha(cr+d)r^n + \beta(c\overline{r}+d)\overline{r}^n \ =\ c(\alpha r^{n+1} + \beta \overline{r}^{n+1}) + d\,(\alpha r^n + \beta \overline{r}^n) \\ =\ & c\gamma_{n+1} + d\gamma_n.\end{aligned}$$

(Aquí se aplicaron las relaciones (2.3).)

Afirmación 2: Existe una única sucesión $(\gamma_n)_{n\in\mathbb{N}_0} = (\alpha\, r^n + \beta\, \overline{r}^n)_{n\in\mathbb{N}_0}$ que satisface las condiciones iniciales $\gamma_0 = a$, $\gamma_1 = b$.

Esto es cierto pues para ello hay que resolver el sistema lineal

$$\left\{ \begin{array}{ccccc} \alpha & + & \beta & = & a \\ \alpha\, r & + & \beta\, \overline{r} & = & b \end{array} \right.$$

que tiene solución y es única pues $r \neq \overline{r}$ por hipótesis: se obtiene

$$\alpha = \frac{b - a\,\overline{r}}{r - \overline{r}} \quad \text{y} \quad \beta = \frac{a\,r - b}{r - \overline{r}}.$$

Se concluye que esta sucesión $(\gamma_n)_{n\in\mathbb{N}_0} = (\alpha\, r^n + \beta\, \overline{r}^n)_{n\in\mathbb{N}_0}$ coincide con la sucesión de Lucas original $(a_n)_{n\in\mathbb{N}_0}$, ya que satisface las mismas condiciones iniciales y la misma recurrencia. Por lo tanto el término general de la sucesión $(a_n)_{n\in\mathbb{N}_0}$ es

$$a_n = \alpha\, r^n + \beta\, \overline{r}^n,\ \forall n \in \mathbb{N}_0.$$

En el caso de la sucesión de Fibonacci, se tiene $r = \Phi$, $\overline{r} = \overline{\Phi}$, *y al resolver el sistema*

$$\begin{cases} \alpha & + & \beta & = & 0 \\ \alpha\,\Phi & + & \beta\,\overline{\Phi} & = & 1 \end{cases},$$

se obtiene

$$\alpha = \frac{1}{\Phi - \overline{\Phi}} = \frac{1}{\sqrt{5}} \quad y \quad \beta = \frac{-1}{\Phi - \overline{\Phi}} = -\frac{1}{\sqrt{5}},$$

o sea

$$F_n = \frac{1}{\sqrt{5}}\,(\Phi^n - \Phi^n),\ \forall\, n \in \mathbb{N}_0,$$

que coincide obviamente con el resultado que probamos en la Proposición 2.5.5.

Pregunta: ¿Qué podemos hacer en el caso en que la ecuación asociada $X^2 - cX - d = 0$ tiene una única raíz r, o sea $X^2 - cX - d = (X - r)^2$? En este caso se puede probar, usando que $c = 2r$ (¿por qué?), que las sucesiones $(r^n)_{n\in\mathbb{N}_0}$ y $(nr^{n-1})_{n\in\mathbb{N}_0}$ satisfacen la misma recurrencia, y también cualquier combinación lineal de ellas. Así, resolviendo el sistema lineal con las condiciones iniciales $\gamma_0 = a$ y $\gamma_1 = b$ deducimos que el término general a_n de la sucesión, cuando $r \neq 0$, es

$$a_n = a\,r^n + (b - a\,r)\,n\,r^{n-1},\ \forall\, n \in \mathbb{N}_0.$$

Cuando $r = 0$, la sucesión está dada simplemente por $a_0 = a$, $a_1 = b$, $a_{n+2} = 0, \forall\, n \in \mathbb{N}_0$.

2.5.4 Inducción completa – Formulación general.

El principio de inducción admite una formulación equivalente a las de los Teoremas 2.3.2 y 2.5.2 que es la que resulta útil cuando al querer probar el paso inductivo, no sabemos para cuál $k \leq h$, o para cuáles, vamos a tener que suponer que la hipótesis inductiva se cumple, o cuando necesitamos que la hipótesis inductiva se cumpla para todo $k \leq h$.

Consideremos el ejemplo siguiente: sea $(a_n)_{n\in\mathbb{N}}$ la sucesión definida por recurrencia como

$$a_1 = 1, \quad a_{n+1} = 1 + \sum_{k=1}^{n} \frac{n + a_k}{n + k + 1},\ \forall\, n \in \mathbb{N}.$$

Probar que $a_n \leq n$, $\forall\, n \in \mathbb{N}$. Pero si queremos probar esta afirmación por inducción, resulta que no nos alcanza suponer verdadera la hipótesis inductiva $a_h \leq h$ para lograr probar que $a_{h+1} \leq h + 1$, pues como la sucesión está definida utilizando todos los términos a_k con $k \leq h$ y no podemos definirla utilizando solo a_h, necesitaremos asumir que la hipótesis inductiva es verdadera para todos los términos a_k con $k \leq h$.

Teorema 2.5.7. (Principio de inducción completa.)

Sea $p(n)$, $n \in \mathbb{N}$, *una afirmación sobre los números naturales. Si* p *satisface*

- (Caso base) $p(1)$ *es Verdadera,*
- (Paso inductivo) $\forall\, h \in \mathbb{N}$, $p(1), \ldots, p(h)$ *Verdaderas* $\Rightarrow$ $p(h+1)$ *Verdadera,*

entonces $p(n)$ *es Verdadero,* $\forall\, n \in \mathbb{N}$.

(El paso inductivo en este caso también suele escribirse en la forma: $\forall\, h \in \mathbb{N}$, $p(k)$ Verdadera para $1 \leq k \leq h \;\Rightarrow\; p(h+1)$ Verdadera.)

<u>*Ejemplo:*</u> Sea $(a_n)_{n\in\mathbb{N}}$ la sucesión definida por recurrencia como

$$a_1 = 1, \quad a_{n+1} = 1 + \sum_{k=1}^{n} \frac{n + a_k}{n+k+1},\ \forall\, n \in \mathbb{N}.$$

Probar que $a_n \leq n$, $\forall\, n \in \mathbb{N}$.

Demostración. Aplicaremos aquí (por necesidad) el principio de inducción completa enunciado en el Teorema 2.5.7.

$$p(n): \quad a_n \leq n.$$

- Caso base: ¿$p(1)$ V? Sí, pues efectivamente $a_1 \underset{def}{=} 1 \leq 1$.
- Paso inductivo: Dado $h \in \mathbb{N}$, ¿$p(1), \ldots, p(h)$ Verdaderas $\Rightarrow$ $p(h+1)$ Verdadera?
  - HI: $a_1 \leq 1, \ldots, a_h \leq h$, o sea $a_k \leq k$ para $1 \leq k \leq h$.
  - Qpq $a_{h+1} \leq h+1$.

  Pero para $h \geq 1$ se tiene

  $$a_{h+1} \underset{def}{=} 1 + \sum_{k=1}^{h} \frac{h + a_k}{h+k+1} \underset{HI}{\leq} 1 + \sum_{k=1}^{h} \frac{h+k}{h+k+1}$$

  pues por HI, $a_k \leq k$ implica $h + a_k \leq h + k$ y por lo tanto, dado que $h + k + 1 > 0$, $\frac{h+a_k}{h+k+1} \leq \frac{h+k}{h+k+1}$ pues no cambia el sentido de la desigualdad.
  Así, para concluir que $a_{h+1} \leq h+1$, alcanza con probar que

  $$1 + \sum_{k=1}^{h} \frac{h+k}{h+k+1} \leq h+1, \quad \text{o equivalentemente} \quad \sum_{k=1}^{h} \frac{h+k}{h+k+1} \leq h.$$

Pero notemos que cada uno de los h términos $\frac{h+k}{h+k+1}$ tiene el numerador $h+k$ positivo y menor que el denominador $h+k+1$, o sea

$$1 \leq h+k < h+k+1 \quad \Longrightarrow \quad \frac{h+k}{h+k+1} < 1$$

y por lo tanto

$$\sum_{k=1}^{h} \frac{h+k}{h+k+1} < \sum_{k=1}^{h} 1 = h,$$

como se quería probar. (Notar que probamos algo más fuerte que lo que necesitamos: que $\sum_{k=1}^{h} \frac{h+k}{h+k+1} < h$, pero esto claramente implica que $\sum_{k=1}^{h} \frac{h+k}{h+k+1} \leq h$ como nos alcanza. En realidad la proposición dice $\leq$ por el término $a_1 = 1$ pero a partir de a_2 vale la desigualdad estricta.)

Es decir hemos probado tanto el caso base como el paso inductivo. Se concluye que $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$. □

Demos otro ejemplo en este capítulo del curso donde se puede usar el principio de inducción completa, corrido esta vez.

Ejemplo: Probar que si se tienen estampillas de 4 y 5 \$, se pueden mandar cartas de cualquier precio n entero, con $n \geq 12$.

Demostración.

$$p(n): \quad \text{existen } j,k \in \mathbb{N} \ tq \ n = j \cdot 4 + k \cdot 5.$$

- Caso base: ¿$p(12)$ V? Sí, pues $12 = 3 \cdot 4$: se necesitan 3 estampillas de 4 \$.
- Paso inductivo: Dado $h \geq 12$, ¿$p(k)$ V para $12 \leq k \leq h \ \Rightarrow \ p(h+1)$ V?

  Inmediatamente se ve que para obtener $h+1$ con estampillas de 4 y 5 \$, conviene obtener $h-3$ con estampillas de 4 y 5 \$, y luego agregarle una estampilla de 4 \$, ya que $h+1 = (h-3)+4$. O sea necesitamos aplicar la hipótesis inductiva para $h-3$, y de ella podremos deducir que $p(h+1)$ es Verdadero.

  La hipótesis inductiva permite suponer que $p(k)$ es V para $12 \leq k \leq h$. Entonces debemos verificar que $h-3$ está en las condiciones de la HI.

  Está claro que $h-3 \leq h$. Pero $h-3 \geq 12 \ \Leftrightarrow \ h+1 \geq 16$. O sea la HI nos permite probar que $p(h+1)$ es V a partir de $h+1 = 16$. Por lo tanto tenemos que verificar los casos $h = 13$, $h = 14$ y $h = 15$

aparte (porque para ellos la HI requerida sería $p(10)$ V, $p(11)$ y $p(12)$ V, que no se cumple.

- ¿$p(13)$ V? Sí, pues $13 = 2 \cdot 4 + 1 \cdot 5$: se necesitan 2 estampillas de 4 \$ y una de 5 .
- ¿$p(14)$ V? Sí, pues $14 = 1 \cdot 4 + 2 \cdot 5$: se necesitan 1 estampilla de 4 \$ y 2 de 5 .
- ¿$p(15)$ V? Sí, pues $15 = 3 \cdot 5$: se necesitan 3 estampillas de 5 \$.

Así terminamos de probar el paso inductivo.

Es decir hemos probado tanto los casos base como el paso inductivo. Se concluye que $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$. □

Aquí otro ejemplo, que tiene que ver con la cantidad de cortes necesarios para separar todas las cartas de un mazo de n cartas.

Ejemplo: Dado $n \in \mathbb{N}$, probar que si se tiene un mazo de n cartas, se necesitan hacer $n-1$ cortes para separar todas las cartas independientemente de la manera que se hagan los cortes. ¿Se entiende, no? se trata de pasar de un pilón vertical de cartas a todas cartas separadas, o sea a n pilones individuale de una carta... (El número $n-1$ es bastante intuitivo en este caso ya que hay que separar todas las cartas, pero nos va a servir formalizarlo con inducción completa para entender mejor el ejemplo suguiente.)

Demostración.

$p(n)$: Se necesitan $n-1$ cortes para separar completamente n cartas.

- Caso base: ¿$p(1)$ V? Sí, pues no hay que separar nada: no se necesita hacer ningún corte.
- Paso inductivo: Dado $h \in \mathbb{N}$, ¿$p(k)$ V para $1 \leq k \leq h \;\Rightarrow\; p(h+1)$ V? (Es decir, si para un mazo de k cartas con $1 \leq k \leq h$ necesito $k-1$ cortes, ¿puedo deducir que para un mazo de $h+1$ cartas se necesitan h cortes?)

  Haga lo que haga tengo que hacer un primer corte, que va a separar mi mazo de $h+1$ cartas en dos mazos: uno de j cartas y otro de k cartas, con $1 \leq j, k \leq h$ y $j + k = h + 1$. Ahora bien, tanto para j y k puedo aplicar la HI, ya que $1 \leq j, k \leq h$: para separar el mazo de j cartas necesito $j-1$ cortes y para el mazo de k cartas necesito $k-1$ cortes. Luego necesito en total

  $$1 + (j-1) + (k-1) = j + k - 1 = (h+1) - 1 = h$$

  cortes como queriá probar.

  Así terminamos de probar el paso inductivo.

Es decir hemos probado tanto el caso base como el paso inductivo. Se concluye que $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$. □

Ejemplo: Hagamos ahora una modificación del ejemplo anterior, donde los cortes tienen un costo y donde la conclusión no es tan obvia ni tan intuitiva: ahora cada corte que separa el mazo de n cartas en dos mazos de j y k cartas, con $j + k = n$, cuesta jk. La pregunta es si hay una estrategia ganadora, o sea que cueste menos, para separar completamente el mazo de n cartas, o si todas las estrategias tienen el mismo costo.

Antes de proponer una solución, hagamos un ejemplo no obvio. Por ejemplo tenemos un mazo de 8 cartas.
Una primera estrategia que podríamos pensar que es ingenua, es ir sacando las cartas de arriba de a una: esto nos cuesta $7+6+5+4+3+2+1 = 28$ ¿Se entiende por qué? el primer corte cuesta $1 \cdot 7$, el segundo $1 \cdot 6$, etc., hasta el último que cuesta $1 \cdot 1$, y se suman los costos.
Otra estrategia que puede parecer más inteligente, y se llama "dividir y conquistar", consiste en cortar cada vez los mazos por la mitad. El primer corte cuesta entonces $4 \cdot 4$ y nos quedan 2 mazos de 4 cartas para separar. Cada uno aplicando la misma estrategia cuesta $2 \cdot 2$, y nos quedan 4 mazos de 2 cartas cada uno, y separar cada uno de ellos cuesta $1 \cdot 1$. Así el costo total es $16 + 2 \cdot 4 + 4 \cdot 1 = 28$ también! ¿Será que siempre da lo mismo? o sea, ¿será que independientemente de la estrategia elegida,

$$p(n) = 1 + 2 + \cdots + (n-1) = \frac{(n-1)n}{2}$$

que es el costo de la estrategia ingenua? Intentemos ver si lo podemos probar.

Demostración.

$$p(n): \quad \text{El costo de cualquier estrategia es } \frac{(n-1)n}{2}.$$

- Caso base: ¿$p(1)$ V? Sí, pues no hay que separar nada: no se necesita hacer ningún corte, y $\frac{0\cdot 1}{2} = 0$. O sea en este caso cualquier estrategia tiene costo 0.

- Paso inductivo: Dado $h \in \mathbb{N}$, ¿$p(k)$ V para $1 \le k \le h \;\Rightarrow\; p(h+1)$ V? (Es decir, si para un mazo de k cartas con $1 \le k \le h$ el costo de cualquier estrategia es $\frac{(k-1)k}{2}$, ¿ puedo deducir que para un mazo de $h+1$ cartas el costo es $\frac{h(h+1)}{2}$?)

  Como antes, haga lo que haga tengo que hacer un primer corte, que va a separar mi mazo de $h+1$ cartas en dos mazos: uno de j cartas y otro de k cartas, con $1 \le j, k \le h$ y $j + k = h + 1$, y esto tiene un

costo jk. Ahora bien, tanto para j y k puedo aplicar la HI, ya que $1 \leq j, k \leq h$: el costo de cualquier estrategia para el mazo de j cartas va a de $\frac{(j-1)j}{2}$ y el costo para el mazo de k cartas es $\frac{(k-1)k}{2}$, donde no olvidamos que $j + k = h + 1$. Así , haga lo que haga el costo para mi mazo de $h + 1$ cartas es (haciendo la cuenta)

$$jk + \frac{(j-1)j}{2} + \frac{(k-1)k}{2} = \frac{2jk + (j-1)j + (k-1)k}{2}$$
$$= \frac{(j+k-1)(j+k)}{2} = \frac{h(h+1)}{2},$$

como se quería probar.

Así terminamos de probar el paso inductivo.

Es decir hemos probado tanto el caso base como el paso inductivo. Se concluye que $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$. □

Durante este curso veremos varios ejemplos más donde usaremos esta versión del principio de inducción, o su variante corrida, por ejemplo para probar el Algoritmo de División entera en $\mathbb{Z}$, o para probar el Teorema de Gauss que dice que todo número natural $n \neq 1$ es divisible por algún número primo, o para probar el teorema fundamental de la aritmética.

2.6 Apéndice

2.6.1 Los axiomas de Peano.

A fines del siglo XIX, el matemático, lógico y filósofo italiano *Giuseppe Peano*, 1858-1932, dio una definición axiomática de los números naturales. La clave de la definición de Peano es la noción de *sucesor* S que es la función de $S : \mathbb{N} \to \mathbb{N}$, $S(n) = n + 1$, y las propiedades que satisface.

El conjunto $\mathbb{N}$ de números naturales es un conjunto $\mathcal{N}$ que satisface los axiomas siguientes:

1. $1 \in \mathcal{N}$.
2. Existe una función "sucesor" S definida sobre $\mathcal{N}$ que satisface:
   - Para todo $n \in \mathcal{N}$, $S(n) \in \mathcal{N}$ (es decir S es una función de $\mathcal{N}$ en $\mathcal{N}$).
   - Para todo $n \in \mathcal{N}$, $S(n) = 1$ es Falso (es decir, 1 no es el sucesor de ningún $n \in \mathcal{N}$).

- Para todo par de números $n, m \in \mathcal{N}$, si $S(n) = S(m)$, entonces $n = m$ (es decir la función S es inyectiva).

3. Si K es un conjunto cualquiera que satisface las dos propiedades siguientes

   - $1 \in K$,
   - para todo $n \in \mathcal{N}$, $n \in K \;\Rightarrow\; S(n) \in K$,

   entonces $\mathcal{N} \subset K$.

Los Axiomas 1 y 2 implican que el conjunto $\mathcal{N}$ contiene a los elementos $1, S(1), S\big(S(1)\big), \dots$, que son todos distintos entre sí, y es por lo tanto infinito. Pero hay que garantizar que no es más "grande" que el conjunto $\{1, S(1), S\big(S(1)\big), \dots\}$: éste es papel que juega el Axioma 3, que es de hecho el axioma de Inducción. Por ejemplo el conjunto $\mathcal{N} := \mathbb{N} \cup \{\frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \dots\}$ satisface los tres primeros axiomas pero no el 3ro, ya que si tomamos $K = \mathbb{N}$ (los números naturales que conocemos) tendríamos que deducir que $\mathcal{N} \subset K$, es decir $\mathbb{N} \cup \{\frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \dots\} \subseteq \mathbb{N}$, lo que es claramente falso.

2.6.2 El Principio de Buena Ordenación y los Principios de Inducción.

El *Principio de Buena Ordenación* dice que todo subconjunto no vacío del conjunto de los números naturales $\mathbb{N}$ contiene un *primer elemento*, es decir un elemento que es menor o igual que todos los demás.

De hecho, sabiendo que $\mathbb{N} = \{1, 2, \dots\}$, este resultado es bastante natural ya que si el subconjunto $A \subseteq \mathbb{N}$ es finito y no vacío, podemos comparar sus elementos y quedarnos con el más chico, y si el conjunto $A \subseteq \mathbb{N}$ es infinito y no vacío, podemos considerar un elemento $n_0 \in A$ y quedarnos con $A \cap \mathbb{N}_{\leq n_0}$, que es finito y no vacío: el menor elemento de este conjunto es el menor elemento de A.

Pero se puede probar un resultado más potente: se puede probar que de hecho el Principio de Inducción (P.I., Teorema 2.3.2), el Principio de Inducción completa (P.I.C., Teorema 2.5.7) y el Principio de Buena Ordenación (P.B.O.) son todos equivalentes entre sí, es decir si vale cualquier de ellos valen los otros.

Para demostrar ese tipo de afirmaciones donde hay más de dos proposiciones que son equivalentes, se acostumbra mostrar implicaciones en forma de ciclo: por ejemplo aquí lo se puede probar la sucesión de implicaciones

$$\text{P.I.} \implies \text{P.I.C.} \implies \text{P.B.O.} \implies \text{P.I.}$$

Así por ejemplo para ver que P.B.O $\Rightarrow$ P.I.C. se utiliza el hecho que P.B.O. $\Rightarrow$ P.I. $\Rightarrow$ P.I.C.

Estas demostraciones son bastante sutiles. El lector inquieto las puede encontrar sin dificultad en internet, o en distintos libros, o en las notas de Pacetti-Graña que aparecen en la bibliografía del curso.

2.7 Ejercicios.

Sumatoria y Productoria

1. i) Reescribir cada una de las siguientes sumas usando el símbolo de sumatoria

   (a) $1 + 2 + 3 + 4 + \cdots + 100$

   (b) $1 + 2 + 4 + 8 + 16 + \cdots + 1024$

   (c) $1 + (-4) + 9 + (-16) + 25 + \cdots + (-144)$

   (d) $1 + 9 + 25 + 49 + \cdots + 441$

   (e) $1 + 3 + 5 + \cdots + (2n + 1)$

   (f) $n + 2n + 3n + \cdots + n^2$

   ii) Reescribir cada una de los siguientes productos usando el símbolo de productoria y/o de factorial

   (a) $5 \cdot 6 \cdots 99 \cdot 100$

   (b) $1 \cdot 2 \cdot 4 \cdot 8 \cdot 16 \cdots 1024$

   (c) $n \cdot 2n \cdot 3n \cdots n^2$

2. Escribir los dos primeros y los dos últimos términos de las expresiones siguientes

   i) $\displaystyle\sum_{i=6}^{n} 2(i-5)$ iii) $\displaystyle\sum_{i=1}^{n} \frac{n+i}{2i}$ v) $\displaystyle\prod_{i=1}^{n} \frac{n+i}{2i-3}$

   ii) $\displaystyle\sum_{i=n}^{2n} \frac{1}{i(i+1)}$ iv) $\displaystyle\sum_{i=1}^{n^2} \frac{n}{i}$

3. Calcular

   i) $\sum_{i=1}^{n}(4i+1)$ ii) $\sum_{i=6}^{n}2(i-5)$

4. Calcular

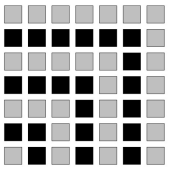
   i) $\sum_{i=0}^{n}2^i$ iii) $\sum_{i=0}^{n}q^{2i}\,,\ q\in\mathbb{R}$

   ii) $\sum_{i=1}^{n}q^i\,,\ q\in\mathbb{R}$ iv) $\sum_{i=n}^{2n}q^i\,,\ q\in\mathbb{R}$

Inducción

5. Probar que, $\forall\, n\in\mathbb{N}\,,\ \sum_{i=1}^{n}(2i-1)=n^2$:

   i) contando de dos maneras la cantidad total de cuadraditos del diagrama

   ii) usando la suma aritmética (o suma de Gauss).

   iii) usando el principio de inducción.

6. *(Suma de cuadrados y de cubos)*
   Probar que para todo $n\in\mathbb{N}$ se tiene

   i) $\sum_{i=1}^{n}i^2=\frac{n(n+1)(2n+1)}{6}$ ii) $\sum_{i=1}^{n}i^3=\frac{n^2(n+1)^2}{4}$

7. Probar que para todo $n\in\mathbb{N}$ se tiene

   i) $\sum_{i=1}^{n}(-1)^{i+1}\,i^2=\frac{(-1)^{n+1}n(n+1)}{2}$

   ii) $\sum_{i=1}^{n}(2i+1)\,3^{i-1}=n\,3^n$

iii) $\displaystyle\sum_{i=1}^{n} \frac{i\,2^i}{(i+1)(i+2)} = \frac{2^{n+1}}{n+2} - 1$

iv) $\displaystyle\prod_{i=1}^{n} \left(1 + a^{2^{i-1}}\right) = \frac{1-a^{2^n}}{1-a}, \quad a \in \mathbb{R} - \{1\}$

v) $\displaystyle\prod_{i=1}^{n} \frac{n+i}{2i-3} = 2^n(1-2n)$

8. Sea $a, b \in \mathbb{R}$. Probar que para todo $n \in \mathbb{N}$,

$$a^n - b^n = (a-b)\sum_{i=1}^{n} a^{i-1}b^{n-i}.$$

Deducir la fórmula de la serie geométrica: para todo $a \neq 1$,

$$\sum_{i=0}^{n} a^i = \frac{a^{n+1}-1}{a-1}.$$

9. i) Sea $(a_n)_{n\in\mathbb{N}}$ una sucesión de números reales. Probar que

$$\sum_{i=1}^{n}(a_{i+1} - a_i) = a_{n+1} - a_1.$$

ii) Calcular $\displaystyle\sum_{i=1}^{n} \frac{1}{i(i+1)}$ (Sugerencia: $\displaystyle\frac{1}{i(i+1)} = \frac{1}{i} - \frac{1}{i+1}$).

iii) Calcular $\displaystyle\sum_{i=1}^{n} \frac{1}{(2i-1)(2i+1)}$
(Sugerencia: calcular $\displaystyle\frac{1}{2i-1} - \frac{1}{2i+1}$).

10. Probar que las siguientes desigualdades son verdaderas para todo $n \in \mathbb{N}$

i) $3^n + 5^n \geq 2^{n+2}$

ii) $3^n \geq n^3$

iii) $\displaystyle\sum_{i=1}^{n} \frac{n+i}{i+1} \leq 1 + n(n-1)$

iv) $\displaystyle\sum_{i=n}^{2n} \frac{i}{2^i} \leq n$

v) $\displaystyle\sum_{i=1}^{2^n} \frac{1}{2i-1} > \frac{n+3}{4}$

vi) $\displaystyle\sum_{i=1}^{n} \frac{1}{i!} \leq 2 - \frac{1}{2^{n-1}}$

vii) $\displaystyle\prod_{i=1}^{n} \frac{4i-1}{n+i} \geq 1$

11. i) Sea $(a_n)_{n\in\mathbb{N}}$ una sucesión de números reales todos del mismo signo y tales que $a_n > -1$ para todo $n \in \mathbb{N}$. Probar que

$$\prod_{i=1}^{n}(1+a_i) \geq 1 + \sum_{i=1}^{n} a_i.$$

¿En qué paso de la demostración se usa que $a_n > -1$ para todo $n \in \mathbb{N}$? ¿Y que todos los términos de la sucesión $(a_n)_{n\in\mathbb{N}}$ tienen el mismo signo?

ii) Deducir que si $a \in \mathbb{R}$ tal que $a > -1$, entonces $(1+a)^n \geq 1+na$.

12. Probar que

i) $n! \geq 3^{n-1}$, $\forall\, n \geq 5$

ii) $3^n - 2^n > n^3$, $\forall\, n \geq 4$

iii) $\displaystyle\sum_{i=1}^{n} \frac{3^i}{i!} < 6n - 5$, $\forall\, n \geq 3$

13. Hallar todos los valores de $n \in \mathbb{N}$ tales que $n^2 + 1 < 2^n$ y demostrar la validez de su conclusión.
<u>*Sugerencia:*</u> para el paso inductivo, tener presente que $n^2+1 < 2^n$ es equivalente a $2^n > n^2 + 1$.

14. Probar que para todo $n \geq 3$ vale que

i) la cantidad de diagonales de un polígono de n lados es $\dfrac{n(n-3)}{2}$

ii) la suma de los ángulos interiores de un polígono de n lados es $\pi\,(n-2)$

<u>*Recurrencia*</u>

15. i) Sea $(a_n)_{n\in\mathbb{N}}$ la sucesión de números reales definida recursivamente por

$$a_1 = 2 \qquad \text{y} \qquad a_{n+1} = 2\,n\,a_n + 2^{n+1}n!, \quad \forall\, n \in \mathbb{N}$$

Probar que $a_n = 2^n\, n!$.

ii) Sea $(a_n)_{n\in\mathbb{N}}$ la sucesión de números reales definida recursivamente por

$$a_1 = 0 \qquad \text{y} \qquad a_{n+1} = a_n + n(3n+1), \quad \forall\, n \in \mathbb{N}$$

Probar que $a_n = n^2(n-1)$.

16. Hallar una fórmula para el término general de las sucesiones $(a_n)_{n\in\mathbb{N}}$ definidas a continuación y probar su validez.

    i) $a_1 = 1$ y $a_{n+1} = (1+\sqrt{a_n})^2,\ \forall\, n \in \mathbb{N}$

    ii) $a_1 = 3$ y $a_{n+1} = 2a_n + 3^n,\ \forall\, n \in \mathbb{N}$

    iii) $a_1 = 1$ y $a_{n+1} = n\, a_n,\ \forall\, n \in \mathbb{N}$

    iv) $a_1 = 2$ y $a_{n+1} = 2 - \frac{1}{a_n},\ \forall\, n \in \mathbb{N}$

17. i) Sea $(a_n)_{n\in\mathbb{N}}$ la sucesión definida por

$$a_1 = 1 \quad \text{y} \quad a_{n+1} = a_n + n \cdot n!,\ \forall\, n \in \mathbb{N}$$

    Probar que $a_n = n!$, y, aplicando el Ej. 9i), calcular $\displaystyle\sum_{i=1}^{n} i \cdot i!$.

    ii) Sea $(a_n)_{n\in\mathbb{N}}$ la sucesión definida por

$$a_1 = 1 \quad \text{y} \quad a_{n+1} = a_n + 3n^2 + 3n + 1,\ \forall\, n \in \mathbb{N}$$

    Probar que $a_n = n^3$ y, aplicando el Ej. 9i), calcular de otra forma $\displaystyle\sum_{i=1}^{n} i^2$ (comparar con Ej 6).

18. Hallar una fórmula para el término general de las sucesiones $(a_n)_{n\in\mathbb{N}}$ definidas a continuación y probar su validez.

    i) $a_1 = 1, \quad a_2 = 2 \quad \text{y} \quad a_{n+2} = n\, a_{n+1} + 2(n+1)a_n,\ \forall\, n \in \mathbb{N}$

    ii) $a_1 = 1, \quad a_2 = 4 \quad \text{y} \quad a_{n+2} = 4\sqrt{a_{n+1}} + a_n,\ \forall\, n \in \mathbb{N}$

    iii) $a_1 = 1, \quad a_2 = 3 \quad \text{y} \quad 2a_{n+2} = a_{n+1} + a_n + 3n + 5,\ \forall\, n \in \mathbb{N}$

    iv) $a_1 = -3, \quad a_2 = 6 \quad \text{y} \quad a_{n+2} = \begin{cases} -a_{n+1} - 3 & \text{si } n \text{ es impar} \\ a_{n+1} + 2a_n + 9 & \text{si } n \text{ es par} \end{cases}$

19. i) Sea $(a_n)_{n\in\mathbb{N}}$ la sucesión definida por

$$a_1 = 1, \quad a_2 = 3 \quad \text{y} \quad a_{n+2} = a_{n+1} + 5a_n \qquad (n \in \mathbb{N})$$

    (a) Probar que $a_n < 1 + 3^{n-1}$ para todo $n \in \mathbb{N}$.

    (b) Hallar una fórmula para el término general de la sucesión $(a_n)_{n\in\mathbb{N}}$ y probar su validez.

    ii) Hallar una fórmula para el término general de la sucesión definida por

$$a_0 = 1, \quad a_1 = 4 \quad \text{y} \quad a_{n+2} = 4\, a_{n+1} - 4\, a_n,\ \forall\, n \in \mathbb{N}_0$$

    y probar su validez.

20. Sea $(a_n)_{n\in\mathbb{N}}$ la sucesión definida por

$$a_1 = 1, \quad a_2 = \frac{3}{2} \quad \text{y} \quad a_{n+2} = a_{n+1} + \frac{2n+1}{n+2}\, a_n \qquad (n \in \mathbb{N})$$

Probar que $a_n > n + \dfrac{1}{3}$ para todo $n \in \mathbb{N}$, $n \geq 4$.

21. Hallar una fórmula para el término general de las sucesiones $(a_n)_{n\in\mathbb{N}}$ definidas a continuación y probar su validez.

i) $a_1 = 1 \quad \text{y} \quad a_{n+1} = 1 + \displaystyle\sum_{i=1}^{n} i\, a_i, \ \forall\, n \in \mathbb{N}$

ii) $a_1 = \dfrac{1}{2} \quad \text{y} \quad a_{n+1} = \dfrac{1}{2}\Big(1 - \displaystyle\sum_{i=1}^{n} a_i\Big), \ \forall\, n \in \mathbb{N}$

22. Sea $f : \mathbb{R}\setminus\{1\} \longrightarrow \mathbb{R}$ definida por $f(x) = \frac{1}{1-x}$. Para $n \in \mathbb{N}$ se define:

$$f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ veces}}$$

Probar que $f^{3k}(x) = x$ para todo $k \in \mathbb{N}$.

23. Sea $f : \mathbb{N} \longrightarrow \mathbb{N}$ la función definida como:

$$f(n) = \begin{cases} \sqrt{n} & \text{si } n \text{ es un cuadrado} \\ 2n & \text{si no} \end{cases}$$

Probar que para todo $k \in \mathbb{N}$ existe $m_k \in \mathbb{N}$ tal que $f^{m_k}(2^k) = 2$.

24. Probar que todo número natural n se escribe como suma de distintas potencias de 2, incluyendo $2^0 = 1$.

25. Probar que para cualquier $n \in \mathbb{N}$ si se tienen números $a_1, a_2, \ldots, a_n$ y se desea calcular su producto, entonces sin importar cómo se inserten los paréntesis en el producto, se requieren exactamente $n-1$ multiplicaciones para calcularlo.
<u>*Comentarios*</u>:

- Recordar que la multiplicación es una operación binaria: está definida para dos números.
- Si queremos multiplicar tres números a, b, c, el enunciado afirma que se requieren dos productos. En efecto, se puede hacer $a\cdot(b\cdot c)$, o bien $(a \cdot b) \cdot c$.
- Si queremos multiplicar cuatro números a, b, c, d, el enunciado afirma que se requieren tres productos. En efecto, se puede hacer $\big((a \cdot b) \cdot c\big) \cdot d$, o bien $\big(a \cdot b\big) \cdot \big(c \cdot d\big)$, o bien $\big(a \cdot (b \cdot c)\big) \cdot d$, o bien $a \cdot \big((b \cdot c) \cdot d\big)$, o bien $a \cdot \big(b \cdot (c \cdot d)\big)$.

Capítulo 3

Combinatoria de conjuntos, relaciones y funciones.

3.1 Cardinal de conjuntos y cantidad de relaciones.

La combinatoria es el arte de contar (en el sentido de enumerar, no de contar un cuento).

Definición 3.1.1. (Cardinal de un conjunto.)

Sea A un conjunto, se llama *cardinal de* A a la cantidad de elementos *distintos* que tiene A, y se nota $\#A$. Cuando el conjunto no tiene un número finito de elementos, se dice que es *infinito*, y se nota $\#A = \infty$.

Ejemplos: $\#\emptyset = 0$, $\#\{a, b, c\} = 3 = \#\{1, 2, 3\}$, $\#\mathbb{N} = \infty$.

Notar que si A es un conjunto finito, $\#A \in \mathbb{N} \cup \{0\} =: \mathbb{N}_0$.

Observación 3.1.2. (Cardinal de un subconjunto.)

Sea A es un conjunto finito y sea $B \subseteq A$. Entonces $\#B \leq \#A$. (Esto vale también para conjuntos infinitos, como verán más adelante los matemáticos.)

Si $A = \{1, 2, 3\}$ y $B = \{4, 5, 6, 7, 8, 9\}$, $\#(A \cup B) = \#\{1, \ldots, 9\} = 9 = 3 + 6 = \#A + \#B$, pero si $A = \{1, 2, 3, 4, 5\}$ y $B = \{4, 5, 6, 7, 8, 9\}$, $\#(A \cup B) = \#\{1, \ldots, 9\} = 9 = 5 + 6 - 2 = \#A + \#B - \#(A \cap B)$ pues los elementos 4 y 5 de la intersección están contados dos veces. Esto vale en general:

Observación 3.1.3. (Cardinal de la unión y del complemento.)

Sean A, B conjuntos finitos dentro de un conjunto referencial U.

- Si A y B son conjuntos disjuntos, entonces $\#(A \cup B) = \#A + \#B$.

- En general $\#(A \cup B) = \#A + \#B - \#(A \cap B)$.
- Si U es un conjunto finito, entonces $\#(A^c) = \#U - \#A$.

Se deduce por ejemplo

$$\#(A - B) = \#A - \#(A \cap B) \quad \text{y} \quad \#(A \triangle B) = \#A + \#B - 2\#(A \cap B).$$

3.1.1 Cardinal de un producto cartesiano y del conjunto de partes.

Veamos ahora en un ejemplo como se comporta el cardinal del producto cartesiano y del conjunto de partes. Sean $A = \{a, b, c\}$ y $B = \{1, 2\}$. Entonces

$A \times B = \{(a,1), (a,2), (b,1), (b,2), (c,1), (c,2)\}$ y por lo tanto $\#(A \times B) = 6 = 3 \cdot 2 = \#A \cdot \#B$. Y $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, A\}$ y por lo tanto $\#(\mathcal{P}(A)) = 8 = 2^3 = 2^{\#A}$. En general

Proposición 3.1.4. (Cardinal del producto cartesiano y del conjunto de partes.)

1. *Sean A y B conjuntos finitos. Entonces $\#(A \times B) = \#A \cdot \#B$.*
2. *Sean $A_1, \ldots, A_n, A$ conjuntos finitos. Entonces*

$$\#(A_1 \times \cdots \times A_n) = \#A_1 \cdots \#A_n = \prod_{i=1}^{n} \#A_i,$$
$$\#(A^n) = (\#A)^n.$$

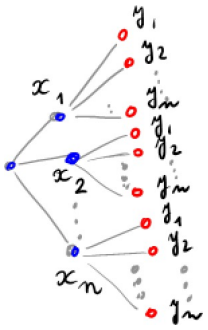
3. *Sea A un conjunto finito, entonces $\#(\mathcal{P}(A)) = 2^{\#A}$.*

Demostración. Haremos una demostración informal pero muy intuitiva. Con los elementos que se vieron en el capítulo anterior, se puede formalizar la demostración si se quiere.

1. Si $A = \{x_1, \ldots, x_n\}$ y $B = \{y_1, \ldots, y_m\}$, entonces

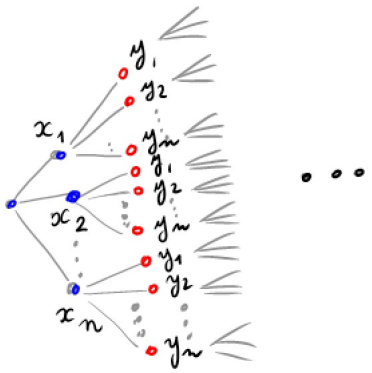
   $A \times B = \{(x_1, y_1), \ldots, (x_1, y_m), (x_2, y_1), \ldots, (x_2, y_m), \ldots, (x_n, y_1), \ldots, (x_n, y_m)\}$,

   y alcanza con contar los elementos. Esto también se puede representar con un árbol:



Lo informal aquí es el uso de los $\ldots$, la demostración formal usa inducción.

2. Esto se formaliza también por inducción, aunque nuevamente se corresponde con un árbol:



3. A cada subconjunto B de $A = \{x_1, \ldots, x_n\}$ se le puede asociar un elemento del producto cartesiano $\{0,1\}^n = \underbrace{\{0,1\} \times \cdots \times \{0,1\}}_{n}$: se asocia a $B \subseteq A$ la n-upla $(e_1, \ldots, e_n) \in \{0,1\}^n$ definida por $e_i = 1$ si $a_i \in B$ y $e_i = 0$ si $a_i \notin B$. Por ejemplo, al subconjunto $\emptyset$ se le asocia la n-upla $(0, \ldots, 0)$, al subconjunto A la n-upla $(1, \ldots, 1)$, y al subconjunto $\{x_1\}$ la n-upla $(1, 0, \ldots, 0)$. Está claro que esta asociación define para cada subconjunto $B \subseteq A$ un elemento del producto cartesiano $\{0,1\}^n$, y recíprocamente a cada elemento del producto cartesiano $\{0,1\}^n$ le corresponde un subconjunto $B \subseteq A$ (esta asociación es un ejemplo de función biyectiva entre el conjunto $\mathcal{P}(A)$ y el conjunto $\{0,1\}^n$) y por lo tanto los dos conjuntos tienen el mismo cardinal, pero $\#(\{0,1)\}^n) = 2^n$ por el inciso anterior.

□

3.1.2 Cantidad de relaciones y de funciones.

¿Cuántas relaciones de $A = \{a, b, c\}$ en $B = \{1, 2\}$ hay? Sabemos que hay una relación por cada subconjunto de $A \times B$, o sea por cada elemento de $\mathcal{P}(A \times B)$. Es decir, hay tantas relaciones como elementos en $\mathcal{P}(A \times B)$. Luego la cantidad de relaciones es igual a $\#\big(\mathcal{P}(A \times B)\big)$. Como, por la Proposición 3.1.4, el conjunto $\mathcal{P}(A \times B)$ tiene en este caso 2^6 elementos, hay 2^6 relaciones de A en B. Este mismo razonamiento vale para conjuntos finitos cualesquiera:

Proposición 3.1.5. (Cantidad de relaciones.)

Sean A_m y B_n conjuntos finitos, con m y n elementos respectivamente. Entonces la cantidad de relaciones que hay de A_m en B_n es igual a $2^{m \cdot n}$.

Hemos visto que si $A = \{a, b, c\}$ y $B = \{1, 2\}$, hay $2^6 = 64$ relaciones de A en B. Nos podemos preguntar cuántas de estas relaciones son funciones $f : A \to B$. Esto se puede pensar en términos de producto cartesiano (o de árboles): para definir una función $f : A \to B$ tenemos que determinar $f(a) \in \{1, 2\}$, $f(b) \in \{1, 2\}$ y $f(c) \in \{1, 2\}$. Por cada elección de $f(a)$, $f(b)$ y $f(c)$ en el conjunto $\{1, 2\}$, tendremos una función distinta. Como tenemos 2 elecciones posibles para $f(a)$, 2 para $f(b)$ y 2 para $f(c)$ tenemos en total $2 \cdot 2 \cdot 2 = 2^3 = 8$ funciones (bastante menos que las 64 relaciones que hay de A en B). Dicho de otra manera la cantidad de funciones es igual al cardinal del producto cartesiano $\{1, 2\} \times \{1, 2\} \times \{1, 2\}$. Este razonamiento vale en general para funciones entre conjuntos finitos:

Proposición 3.1.6. (Cantidad de funciones.)

Sean A_m y B_n conjuntos finitos, con m y n elementos respectivamente. Entonces la cantidad de funciones f que hay de A_m en B_n es igual a n^m.

De las definiciones de función inyectiva, sobreyectiva y biyectiva se desprenden las propiedades siguientes sobre cardinales.

Proposición 3.1.7. (Cardinal de conjuntos y funciones.)

Sean A y B conjuntos finitos.

- *Sea $f : A \to B$ una función* inyectiva. *Entonces $\#A \leq \#B$.*
- *Sea $f : A \to B$ una función* sobreyectiva. *Entonces $\#A \geq \#B$.*
- *Sea $f : A \to B$ una función* biyectiva. *Entonces $\#A = \#B$.*

3.2 El factorial.

Cuando A, B son conjuntos finitos con n elementos, se puede contar la cantidad de funciones biyectivas $f : A \to B$ distintas que hay.

Por ejemplo si $A_2 = \{x_1, x_2\}$ y $B_2 = \{y_1, y_2\}$ tienen ambos 2 elementos, hay 2 funciones funciones biyectivas de A_2 en B_2: la función f_1 definida como $f_1(x_1) = y_1, f_1(x_2) = y_2$, y la función f_2 dada por $f_2(x_1) = y_2, f_2(x_2) = y_1$. Esto se puede pensar nuevamente con un árbol: primero se fija dónde va a parar el elemento x_1 que tiene 2 posibilidades (y_1 o y_2), y en este caso haber fijado dónde va a parar x_1 determina automáticamente dónde va a parar x_2 (al elemento de B_2 que quedó libre). Estas 2 funciones biyectivas se pueden pensar como las 2 *permutaciones* de y_1, y_2, que son y_1, y_2 e y_2, y_1.

Y si $A_3 = \{x_1, x_2, x_3\}$ y $B_3 = \{y_1, y_2, y_3\}$ tienen 3 elementos, hay $6 = 3 \cdot 2$ funciones biyectivas de A_3 en B_3: primero se fija dónde va a parar el elemento x_1 que tiene 3 posibilidades (y_1, y_2 o y_3), luego se fija dónde va a parar x_2, a quién le quedan 2 posibilidades en B_3 (según dónde fue a parar x_1) y luego queda automáticamente determinado dónde va a parar x_3 (al elemento de B_3 que quedó libre). Estas 6 funciones biyectivas se pueden pensar como las 6 *permutaciones* de y_1, y_2, y_3) que son:

$$y_1, y_2, y_3 \ ; \ y_1, y_3, y_2 \ ; \ y_2, y_1, y_3 \ ; \ y_2, y_3, y_1 \ ; \ y_3, y_1, y_2 \ \text{ e } \ y_3, y_2, y_1.$$

En general si $A_n = \{x_1, \ldots, x_n\}$ y $B_n = \{y_1, \ldots, y_n\}$ son conjuntos con n elementos, se puede probar formalmente (por inducción) que hay

$$n \cdot (n-1) \cdots 2 \cdot 1$$

funciones biyectivas de A_n en B_n. Esta cantidad de funciones biyectivas que hay entre conjuntos con n elementos (o de permutaciones de los elementos de un conjunto de n elementos) resulta ser tan importante en matemática que se le da un nombre y una notación particulares.

Definición 3.2.1. (El factorial, o la cantidad de funciones biyectivas.)

Sea $n \in \mathbb{N}$. El *factorial* de n, que se nota $n!$, es el número natural definido como

$$n! = n \cdot (n-1) \cdots 2 \cdot 1 = \prod_{i=1}^{n} i,$$

que coincide con la cantidad de funciones biyectivas que hay entre dos conjuntos con n elementos, o con la cantidad de permutaciones de elementos en un conjunto de n elementos.
Esta definición se extiende a $\mathbb{N}_0$ definiendo $0! = 1$.

Así,

$0! = 1,\ 1! = 1,\ 2! = 2,\ 3! = 6,\ 4! = 24,\ 5! = 120,\ 6! = 720,\ 7! = 5040,\ 8! = 40320,$
$9! = 362880,\ 10! = 3628800,\ 11! = 39916800,\ 12! = 479001600,\ \ldots$

y este número crece muy rápido!

La definición matemática formal, por recurrencia, del factorial es

$$0! = 1 \quad \text{y} \quad n! = n \cdot (n-1)!\ ,\ \forall\, n \in \mathbb{N}.$$

Un programa recursivo para el factorial en Haskell:

```
factorial :: Integer → Integer
factorial 0 = 1
factorial n = n * factorial(n − 1)
```

Un programa iterativo para el factorial en Python:

```
def factorial(n) :
    f = 1
    for i in range (1, n + 1) :
        f = f * i
    return f
```

(La línea $f = 1$ pone en la variable f el valor 1. Luego la instrucción "for i in range $(1, n+1)$" ejecuta la línea que sigue (es decir poner en la variable f el valor que tenía f multiplicado por el valor de i) para todos los valores de $i \geq 1$ y $< n + 1$, es decir entre 1 y n.)

3.2.1 Cantidad de funciones inyectivas.

Ahora que sabemos contar funciones biyectivas entre conjuntos finitos, también podemos contar, con el mismo razonamiento de árbol, la cantidad de funciones inyectivas que hay de un conjunto $A_m = \{x_1, \ldots, x_m\}$ con m elementos en un conjunto $B_n = \{y_1, \ldots, y_n\}$ con n elementos, donde $m \leq n$ para que pueda haber funciones inyectivas.

Por ejemplo supongamos $A_3 = \{x_1, x_2, x_3\}$ y $B_5 = \{y_1, y_2, y_3, y_4, y_5\}$. ¿Cuántas funciones inyectivas $f : A_3 \to B_5$ hay?

Nuevamente, primero se fija dónde va a parar el elemento x_1 que tiene 5 posibilidades (y_1, y_2, y_3, y_4 o y_5), luego se fija dónde va a parar x_2, a

quién le quedan 4 posibilidades en B_5 (según dónde fue a parar x_1, ya que no se puede repetir) y luego se fija dónde va a parar x_3 (a quién le quedan 3 posibilidades). Por lo tanto hay $5 \cdot 4 \cdot 3 = 5!/2!$ funciones inyectivas de A_3 en B_5. Este razonamiento se puede hacer en general (y probar rigurosamente por inducción).

Proposición 3.2.2. (Cantidad de funciones inyectivas.)

Sean A_m y B_n conjuntos finitos, con m y n elementos respectivamente, donde $m \leq n$. Entonces la cantidad de funciones inyectivas $f : A_m \to B_n$ que hay es

$$n \cdot (n-1) \cdots (n-m+1) = \frac{n!}{(n-m)!}.$$

Cabe mencionar que no hay una fórmula tan simple como las anteriores para contar la cantidad de funciones sobreyectivas que hay de un conjunto A_n de n elementos en un conjunto B_m de m elementos, con $n \geq m$ cualesquiera. Existen fórmulas pero son mucho más complicadas e involucran en general contar la cantidad de elementos de muchos conjuntos.

3.3 El número combinatorio.

Hasta ahora contamos distintas cosas relacionadas con conjuntos y funciones, pero no contamos aún cuántos subconjuntos con un número dado k de elementos tiene un conjunto de n elementos, o lo que es lo mismo, cuántas formas tengo de elegir k elementos en un conjunto de n elementos (sin que importe el orden). Concentrémonos ahora en ese problema.

Notación 3.3.1. (El número combinatorio $\binom{n}{k}$.)

Sea $A_n = \{a_1, \ldots, a_n\}$ un conjunto con n elementos. Para $0 \leq k \leq n$, se nota con el símbolo $\binom{n}{k}$, que se llama el *número combinatorio* $\binom{n}{k}$, la cantidad de subconjuntos con k elementos que tiene A_n (o lo que es lo mismo, la cantidad de formas que tenemos de elegir k elementos en un conjunto A_n con n elementos).

Ejemplos:

- Sea $A_4 = \{a_1, a_2, a_3, a_4\}$ un conjunto con 4 elementos. Entonces
  - $\binom{4}{0} = 1$ pues el único subconjunto con 0 elementos de A_4 es el subconjunto vacío $\emptyset$.
  - $\binom{4}{1} = 4$ pues los subconjuntos con 1 elemento de A_4 son $\{a_1\}$, $\{a_2\}$, $\{a_3\}$ y $\{a_4\}$.

- $\binom{4}{2} = 6$ pues los subconjuntos con 2 elementos de A_4 son

$$\{a_1, a_2\}, \{a_1, a_3\}, \{a_1, a_4\}, \{a_2, a_3\}, \{a_2, a_4\}, \{a_3, a_4\}.$$

- $\binom{4}{3} = 4$ pues los subconjuntos con 3 elementos de A_4 son

$$\{a_1, a_2, a_3\}, \{a_1, a_2, a_4\}, \{a_1, a_3, a_4\}, \{a_2, a_3, a_4\}.$$

- $\binom{4}{4} = 1$ pues el único subconjunto con 4 elementos de A_4 es el conjunto A_4.

- Para disipar dudas $\binom{0}{0} = 1$ porque el conjunto vacío $\emptyset$ tiene un único subconjunto, el $\emptyset$, con 0 elementos.

Mucho de lo observado en el ejemplo anterior vale en general:

Observación 3.3.2.

- $\binom{n}{0} = \binom{n}{n} = 1$ pues el único subconjunto de A_n con 0 elementos es el conjunto $\emptyset$, y el único subconjunto de A_n con n elementos es A_n mismo.

- $\binom{n}{1} = n$ pues los subconjuntos de A_n con 1 elemento son los subconjuntos

$$\{a_1\}, \{a_2\}, \ldots, \{a_{n-1}\}, \{a_n\}.$$

- Podemos darnos cuenta que $\binom{n}{n-1} = n$ también ya que dar un subconjunto de A_n con $n-1$ elementos es lo mismo que elegir cuál elemento a_i quedó afuera del subconjunto: por ejemplo el subconjunto $\{a_1, \ldots, a_{n-1}\}$ es el que corresponde a haber dejado a_n afuera.

- Con el mismo razonamiento, $\binom{n}{k} = \binom{n}{n-k}$, $\forall\, k, 0 \leq k \leq n$, ya que a cada subconjunto B_k de A_n con k elementos, podemos asignarle el subconjunto complemento B_k^c que tiene $n-k$ elementos, y esta asignación es una función biyectiva... O lo que es lo mismo, cada vez que elegimos k elementos en A_n estamos dejando de elegir los $n-k$ elementos complementarios.

- Más aún, dado que $\binom{n}{k}$, $0 \leq k \leq n$, cuenta la cantidad de subconjuntos con k elementos en el conjunto A_n con n elementos, y que sabemos que la cantidad total de subconjuntos que hay en A_n es 2^n, se tiene:

$$2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k}, \quad \forall n \in \mathbb{N}_0.$$

3.3.1 El triángulo de Pascal: una fórmula recursiva para $\binom{n}{k}$.

Queremos encontrar una forma de calcular $\binom{n}{k}$ sin listar todos los subconjuntos con k elementos de A_n, con un razonamiento del tipo del que aplicamos para resolver el problema de las torres de Hanoi.

Sea $A_5 = \{a_1, a_2, a_3, a_4, a_5\}$ un conjunto con 5 elementos. Supongamos que queremos calcular $\binom{5}{3}$ sin listar todos los subconjuntos con 3 elementos de A_5. Podemos razonar de la manera siguiente:

Sea B_3 un subconjunto con 3 elementos de A_5. Entonces

- O bien $a_5 \in B_3$, con lo cual para determinar B_3 hay que elegir los 2 elementos que faltan en el conjunto $A_4 = \{a_1, a_2, a_3, a_4\}$. Y ya sabemos que hay $\binom{4}{2} = 6$ formas de elegir 2 elementos en A_4.

- O bien $a_5 \notin B_3$, con lo cual para determinar B_3 hay que elegir los 3 elementos en el conjunto $A_4 = \{a_1, a_2, a_3, a_4\}$. Y ya sabemos que hay $\binom{4}{3} = 4$ formas de elegir 3 elementos en A_4.

Como estos dos casos son disjuntos (o bien $a_5 \in B_3$ o bien $a_5 \notin B_3$), la cantidad total de subconjuntos B_3 con 3 elementos de A_5 es igual a la suma $6 + 4 = 10$, es decir

$$\binom{5}{3} = \binom{4}{2} + \binom{4}{3}.$$

Y este razonamiento se generaliza sin dificultad a un conjunto $A_{n+1} = \{a_1, \ldots, a_{n+1}\}$ con $n+1$ elementos. Ya sabemos que $\binom{n+1}{0} = \binom{n+1}{n+1} = 1$. Queremos ahora calcular $\binom{n+1}{k}$ para un k cualquiera, $1 \leq k \leq n$.

Sea B_k un subconjunto con k elementos de A_{n+1}. Entonces

- O bien $a_{n+1} \in B_k$, con lo cual para determinar B_k hay que elegir los $k-1$ elementos que faltan en el conjunto $A_n = \{a_1, \ldots, a_n\}$. Y ya sabemos que hay $\binom{n}{k-1}$ formas de elegir $k-1$ elementos en A_n. (Aquí interviene la condición $k \geq 1$ pues tiene que ser $k - 1 \geq 0$ para que esto tenga sentido.)

- O bien $a_{n+1} \notin B_k$, con lo cual para determinar B_k hay que elegir los k elementos en el conjunto $A_n = \{a_1, \ldots, a_n\}$. Y ya sabemos que hay $\binom{n}{k}$ formas de elegir k elementos en A_n. (Aquí interviene la condición $k \leq n$ para que esto tenga sentido.)

Como estos dos casos son disjuntos (o bien $a_{n+1} \in B_k$ o bien $a_{n+1} \notin B_k$), la cantidad total de subconjuntos B_k con k elementos de A_{n+1} es igual a la suma $\binom{n+1}{n-1} + \binom{n+1}{k}$, es decir se satisface

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}, \quad \text{para} \quad 1 \leq k \leq n.$$

Así obtuvimos el resultado siguiente:

Proposición 3.3.3. (Una fórmula recursiva para el número combinatorio.)

Se tiene

$$\binom{0}{0} = 1, \ \binom{n+1}{0} = \binom{n+1}{n+1} = 1 \qquad y$$

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \ \textit{para} \ 1 \leq k \leq n, \forall\, n \in \mathbb{N}.$$

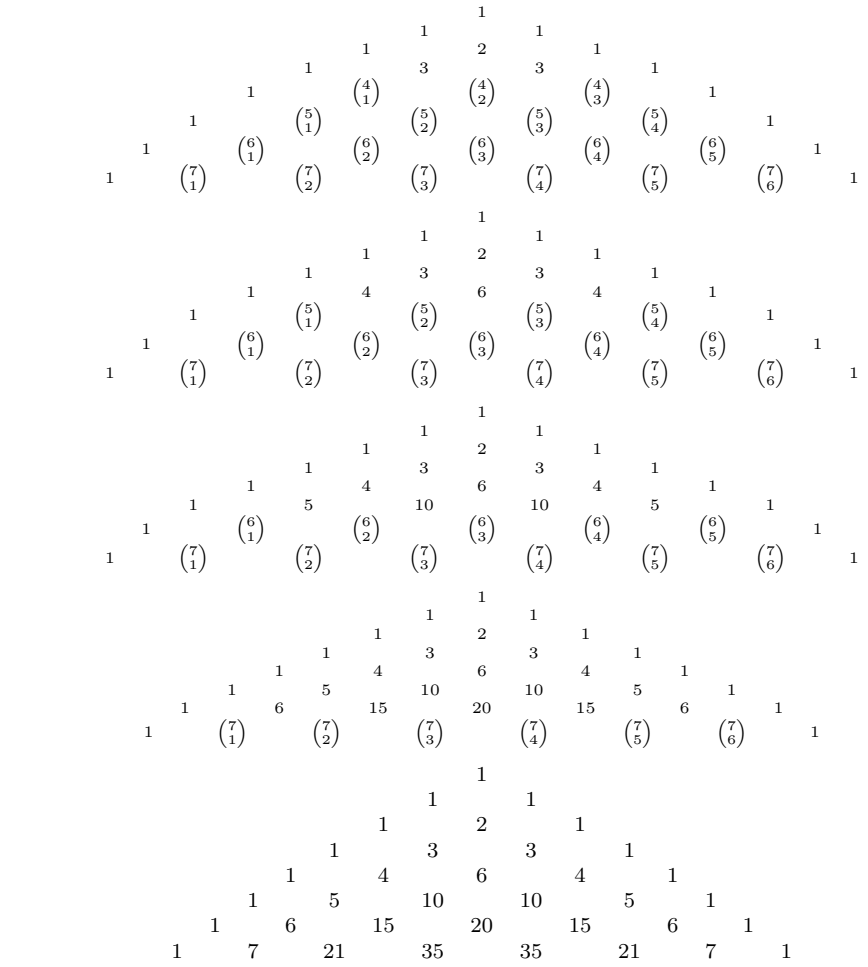
Esto da el siguiente triángulo, conocido como el *triángulo de Pascal* (y vuelve a aparecer Pascal!), que empieza con:

$$\begin{array}{ccccccccccccccc}
 & & & & & & \binom{0}{0} & & & & & & & & \\
 & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & & & \\
 & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & & & \\
 & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & & & \\
 & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & & & \\
 & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & & & \\
\binom{6}{0} & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6} & & \\
 & \binom{7}{1} & & \binom{7}{2} & & \binom{7}{3} & & \binom{7}{4} & & \binom{7}{5} & & \binom{7}{6} & & \binom{7}{7} &
\end{array}$$

Y como ya sabemos que los dos bordes de ese triángulo siempre valen 1, y que cada término de una fila, o sea $\binom{n+1}{k}$, se obtiene como la suma de los 2 términos de la fila anterior que están "encima", o sea $\binom{n}{k-1}$ y $\binom{n}{k}$, esto permite ir deduciendo fila a fila los valores:

$$\begin{array}{ccccccccccccccc}
 & & & & & & 1 & & & & & & & & \\
 & & & & & 1 & & 1 & & & & & & & \\
 & & & & 1 & & \binom{2}{1} & & 1 & & & & & & \\
 & & & 1 & & \binom{3}{1} & & \binom{3}{2} & & 1 & & & & & \\
 & & 1 & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & 1 & & & & \\
 & 1 & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & 1 & & & \\
1 & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & 1 & & \\
 & \binom{7}{1} & & \binom{7}{2} & & \binom{7}{3} & & \binom{7}{4} & & \binom{7}{5} & & \binom{7}{6} & & 1 &
\end{array}$$

$$\begin{array}{ccccccccccccccc}
 & & & & & & 1 & & & & & & & & \\
 & & & & & 1 & & 1 & & & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & & & \\
 & & & 1 & & \binom{3}{1} & & \binom{3}{2} & & 1 & & & & & \\
 & & 1 & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & 1 & & & & \\
 & 1 & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & 1 & & & \\
1 & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & 1 & & \\
 & \binom{7}{1} & & \binom{7}{2} & & \binom{7}{3} & & \binom{7}{4} & & \binom{7}{5} & & \binom{7}{6} & & 1 &
\end{array}$$



Vale mencionar que el triángulo de Pascal, que lleva ese nombre en Occidente en honor a las investigaciones que hizo Blaise Pascal sobre él, era conocido mucho antes, por ejemplo por el matemático italiano *Niccolò Fontana Tartaglia*, 1500-1557.

¡O incluso mucho antes por el matemático chino *Yang Hui*, 1238–1298 !

3.3.2 La expresión del número combinatorio.

Busquemos ahora cuál es el término general (no recursivo) del número combinatorio $\binom{n}{k}$ conjeturando una fórmula y probándola por inducción.

Si queremos contar la cantidad de subconjuntos B_3 con 3 elementos que tiene el conjunto $A_5 = \{a_1, a_2, a_3, a_4, a_5\}$ con 5 elementos, tenemos que elegir los 3 elementos que van a formar parte del subconjunto B_3. Pongamosle por ahora un orden a esos elementos (ya que esto lo sabemos contar, como cuando contamos las funciones inyectivas): para el 1er elemento de B_3 tenemos 5 posibilidades: cualquiera de los elementos a_1 hasta a_5. Pero luego para el 2do elemento nos quedan 4 posibilidades (uno de los que no hayamos elegido como 1er elemento) y para el 3er elemento nos quedan solo 3 posibilidades. Así tenemos $5 \cdot 4 \cdot 3 = 5!/2!$ elecciones. Pero en realidad al hacer esto estamos contando las ternas ordenadas de elementos (b_1, b_2, b_3) formadas con elementos distintos de A_5, y no los subconjuntos (donde no importa el orden). Por ejemplo el subconjunto $\{a_1, a_2, a_3\}$ aparece aquí $6 = 3!$ veces si contamos las ternas formadas por estos elementos:

$$(a_1, a_2, a_3), (a_1, a_3, a_2), (a_2, a_1, a_3), (a_2, a_3, a_1), (a_3, a_1, a_2), (a_3, a_2, a_1).$$

Cada subconjunto $\{b_1, b_2, b_3\}$ fue así contado $3!$ veces, luego:

$$3!\binom{5}{3} = \frac{5!}{(5-3)!} \quad \Longrightarrow \quad \binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{5 \cdot 4}{2} = 10,$$

que coincide con el valor calculado en la sección anterior.

Con el mismo razonamiento para el caso general, podemos conjeturar entonces para todo $n \in \mathbb{N}_0$ la fórmula:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}, \quad \text{para } 0 \leq k \leq n.$$

Teorema 3.3.4. (Número combinatorio.)

Sea $n \in \mathbb{N}_0$ y sea A_n un conjunto con n elementos. Para $0 \leq k \leq n$, la cantidad de subconjuntos con k elementos del conjunto A_n (o equivalentemente, la cantidad de maneras que hay de elegir k elementos en el conjunto A_n) es igual a

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Demostración. Probaremos esta fórmula por inducción corrida a $n \geq 0$, usando la recurrencia de la Proposición 3.3.3 establecida en la sección anterior. Para $n \geq 0$, se tiene

$$p(n): \quad \binom{n}{k} = \frac{n!}{k!(n-k)!}, \quad \text{para } 0 \leq k \leq n.$$

- Caso base: ¿Es $p(0)$ V? Sí, pues para $n = 0$ solo hay que verificar qué pasa para $k = 0$ y $\dfrac{0!}{0!0!} = 1 = \binom{0}{0}$.

- Paso inductivo: Dado $h \geq 0$, ¿$p(h)$ V $\Rightarrow$ $p(h+1)$ V?
  - HI: Para $0 \leq k \leq h$ se tiene $\binom{h}{k} = \dfrac{h!}{k!(h-k)!}$.
  - Qpq para $0 \leq k \leq h+1$ se tiene $\binom{h+1}{k} = \dfrac{(h+1)!}{k!(h+1-k)!}$.

  Pero por la Proposición 3.3.3, sabemos que para $1 \leq k \leq h$ se tiene

$$\begin{aligned}
\binom{h+1}{k} &= \binom{h}{k-1} + \binom{h}{k} \\
&\underset{HI}{=} \frac{h!}{(k-1)!(h-(k-1))!} + \frac{h!}{k!(h-k))!} \\
&= \frac{k \cdot h!}{k(k-1)!(h+1-k))!} + \frac{(h+1-k)h!}{k!(h+1-k)(h-k))!} \\
&= \frac{k \cdot h! + (h+1-k)h!}{k!(h+1-k))!} = \frac{\big(k+(h+1-k)\big)h!}{k!(h+1-k))!} \\
&= \frac{(h+1)h!}{k!(h+1-k))!} = \frac{(h+1)!}{k!(h+1-k))!}
\end{aligned}$$

  como se quería probar.

  Faltan entonces los casos $k = 0$ y $k = h+1$: en esos casos sabemos que

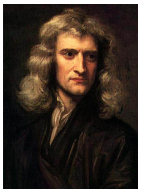
$$\binom{h+1}{0} = 1 = \binom{h+1}{h+1}$$

  que coinciden con

$$\frac{(h+1)!}{0!(h+1-0)!} \quad \text{y} \quad \frac{(h+1)!}{(h+1)!\big(h+1-(h+1)\big)!}$$

Es decir hemos probado tanto el caso base como el paso inductivo. Se concluye que $p(n)$ es Verdadera, $\forall\, n \in \mathbb{N}_0$. □

3.3.3 El Binomio de Newton.



Es hora de que entre en escena el que es considerado el matemático y físico más grande de la historia, el inglés *Isaac Newton*, 1642-1727. En este caso relacionado con la expansión de la expresión

$$(x+y)^n,\ n \in \mathbb{N}_0.$$

Por ejemplo, si calculamos los desarrollos para los primeros valores de n,

$$\begin{aligned}
(x+y)^0 &= 1,\\
(x+y)^1 &= x+y,\\
(x+y)^2 &= x^2+2xy+y^2,\\
(x+y)^3 &= x^3+3x^2y+3xy^2+y^3,\\
(x+y)^4 &= x^4+4x^3y+6x^2y^2+4xy^3+y^4,\\
(x+y)^5 &= x^5+5x^4y+10x^3y^2+10x^2y^3+5xy^4+y^5.
\end{aligned}$$

Pareciera que van apareciendo como coeficientes de los monomios x^iy^j los números combinatorios que aparecen en el tríángulo de Pascal! O sea pareciera que se tiene

Teorema 3.3.5. (El binomio de Newton).

$$\begin{aligned}
(x+y)^n &= x^n+\binom{n}{1}x^{n-1}y+\binom{n}{2}x^{n-2}y^2+\cdots+\binom{n}{n-1}xy^{n-1}+y^n\\
&= \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k,\ \forall\, n\in\mathbb{N}_0,
\end{aligned}$$

o lo que es lo mismo, ya que los números combinatorios son simétricos ($\binom{n}{k}=\binom{n}{n-k}$)*:*

$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^ky^{n-k},\ \forall\, n\in\mathbb{N}_0.$$

Demostración. Haremos una demostración combinatoria, o sea "contando". Pensemos que

$$(x+y)^n=\underbrace{(x+y)\cdot(x+y)\cdots(x+y)\cdot(x+y)}_{n\text{ factores}}.$$

Cuando aplicamos la distributividad, en cada paréntesis podemos elegir un x o un y (pero no los dos a la vez). Como en total hay n paréntesis terminaremos eligiendo k veces x y $n-k$ veces y, para algún valor de k, $0\le k\le n$. Por ejemplo si no elegimos ninguna vez x y n veces y, obtenemos –al realizar el producto– el monomio y^n, y si elegimos 1 vez x y $n-1$ veces y, obtenemos el monomio xy^{n-1}. ¿Pero cuántas veces aparece cada uno de estos monomios?

- ¿Cuántas veces se obtiene el monomio y^n? Para ello tenemos que elegir solo el y de cada uno de los paréntesis: hay una única forma de hacer eso, y por lo tanto se obtiene una vez el monomio y^n.

- ¿Cuántas veces se obtiene el monomio xy^{n-1}? Para ello tenemos que elegir en alguno de los paréntesis el x y en todos los demás paréntesis el y: como hay n paréntesis, hay n formas de elegir el x (o bien del 1er paréntesis, o bien del 2do, o bien del 3ro, etc.) y de los demás paréntesis saco el y. Por lo tanto se obtiene $n = \binom{n}{1}$ veces el monomio xy^{n-1}.

- En general, dado k, $0 \leq k \leq n$, ¿cuántas veces se obtiene el monomio $x^k y^{n-k}$? Para ello tenemos que elegir en k paréntesis el x y en todos los $n-k$ paréntesis restantes el y: como hay n paréntesis y tenemos que elegir de cuáles k paréntesis extraemos un x, hay $\binom{n}{k}$ formas de elegir de qué paréntesis saco x (y de los demás paréntesis saco el y). Por lo tanto se obtiene $\binom{n}{k}$ veces el monomio $x^k y^{n-k}$.

En definitiva, tenemos la suma de $n+1$ términos de la forma $\binom{n}{k} x^k y^{n-k}$, lo que prueba el teorema. □

Observación 3.3.6.

- Con la fórmula del Binomio de Newton, se recupera fácilmente la expresión

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k \cdot 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k},$$

que habíamos notado al definir el número combinatorio.

- ¿ Cuánto da $\displaystyle\sum_{k=0}^{n} (-1)^k \binom{n}{k}$?

- Propongo que prueben por inducción que $\binom{2n}{n} \leq (n+1)!$, $\forall\, n \in \mathbb{N}$. Pero fijense que en la práctica hay un ejercicio que pide probar que $\binom{2n}{n} < 4^n$, $\forall\, n \in \mathbb{N}$, como consecuencia de que $\displaystyle\sum_{k=0}^{2n} \binom{2n}{k} = 4^n$ (¿por qué?). Notemos que $4^n < (n+1)!$ para $n \geq 6$ con lo cual la desigualdad que se obtiene aplicando el binomio de Newton es más precisa a partir de $n = 6$ que la primera que les propuse.

- Como una aplicación del binomio y un poco de trabajo, se puede probar por inducción que se tiene

$$\frac{n^n}{3^n} \leq n! \leq \frac{n^n}{2^n}, \quad \forall\, n \geq 6,$$

una forma bastante precisa de ubicar el factorial entre dos potencias.

3.4 Ejercicios.

Cardinal de conjuntos y cantidad de relaciones y funciones

1. Dado el conjunto referencial $V = \{n \in \mathbb{N} : n \text{ es múltiplo de } 15\}$, determinar el cardinal del complemento del subconjunto A de V definido por $A = \{n \in V : n \geq 132\}$.

2. ¿Cuántos números naturales hay menores o iguales que 1000 que no son ni múltiplos de 3 ni múltiplos de 5?

3. Dados subconjuntos finitos A, B, C de un conjunto referencial V, calcular $\#(A \cup B \cup C)$ en términos de los cardinales de A, B, C y sus intersecciones.

4. i) En el listado de inscripciones de un grupo de 150 estudiantes, figuran 83 inscripciones en Análisis y 67 en Álgebra. Además se sabe que 45 de los estudiantes se anotaron en ambas materias. ¿Cuántos de los estudiantes no están inscriptos en ningún curso?

   ii) En un instituto de idiomas donde hay 110 alumnos, las clases de inglés tienen 63 inscriptos, las de alemán 30 y las de francés 50. Se sabe que 7 alumnos estudian los tres idiomas, 30 solo estudian inglés, 13 solo estudian alemán y 25 solo estudian francés. ¿Cuántos alumnos estudian exactamente dos idiomas? ¿Cuántos inglés y alemán pero no francés? ¿Cuántos no estudian ninguno de esos idiomas?

5. Si hay 3 rutas distintas para ir de Buenos Aires a Rosario, 4 rutas distintas para ir de Rosario a Santa Fe, y 2 para ir de Santa Fe a Reconquista ¿cuántos formas distintas hay para ir de Buenos Aires a Reconquista pasando por las dos ciudades intermedias?

6. i) ¿Cuántos números de exactamente 4 cifras (no pueden empezar con 0) hay que no contienen al dígito 5?

   ii) ¿Cuántos números de exactamente 4 cifras hay que contienen al dígito 7?

7. María tiene una colección de 17 libros distintos que quiere guardar en 3 cajas: una roja, una amarilla y una azul. ¿De cuántas maneras distintas puede distribuir los libros en las cajas?

8. Un estudiante puede elegir qué cursar entre 5 materias que se dictan este cuatrimestre. ¿De cuántas maneras distintas puede elegir qué materias cursar, incluyendo como posibilidad no cursar ninguna materia? ¿Y si tiene que cursar al menos dos materias?

9. Si A es un conjunto con n elementos ¿Cuántas relaciones en A hay? ¿Cuántas de ellas son reflexivas? ¿Cuántas de ellas son simétricas? ¿Cuántas de ellas son reflexivas y simétricas?

10. Sean $A = \{1, 2, 3, 4, 5\}$ y $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. Sea $\mathcal{F}$ el conjunto de todas las funciones $f : A \to B$.

    i) ¿Cuántos elementos tiene el conjunto $\mathcal{F}$?

    ii) ¿Cuántos elementos tiene el conjunto $\{f \in \mathcal{F} : 10 \notin \mathrm{Im}(f)\}$?

    iii) ¿Cuántos elementos tiene el conjunto $\{f \in \mathcal{F} : 10 \in \mathrm{Im}(f)\}$?

    iv) ¿Cuántos elementos tiene el conjunto $\{f \in \mathcal{F} : f(1) \in \{2, 4, 6\}\}$?

11. Sean $A = \{1, 2, 3, 4, 5, 6, 7\}$ y $B = \{8, 9, 10, 11, 12, 13, 14\}$.

    i) ¿Cuántas funciones biyectivas $f : A \to B$ hay?

    ii) ¿Cuántas funciones biyectivas $f : A \to B$ hay tales que $f(\{1, 2, 3\}) = \{12, 13, 14\}$?

12. ¿Cuántos números de 5 cifras distintas se pueden armar usando los dígitos del 1 al 5? ¿Y usando los dígitos del 1 al 7? ¿Y usando los dígitos del 1 al 7 de manera que el dígito de las centenas no sea el 2?

13. Sean $A = \{1, 2, 3, 4, 5, 6, 7\}$ y $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

    i) ¿Cuántas funciones inyectivas $f : A \to B$ hay?

    ii) ¿Cuántas de ellas son tales que $f(1)$ es par?

    iii) ¿Cuántas de ellas son tales que $f(1)$ y $f(2)$ son pares?

14. ¿Cuántas funciones biyectivas $f : \{1, 2, 3, 4, 5, 6, 7\} \to \{1, 2, 3, 4, 5, 6, 7\}$ tales que $f(\{1, 2, 3\}) \subseteq \{3, 4, 5, 6, 7\}$ hay?

15. Sea $A = \{f : \{1, 2, 3, 4\} \to \{1, 2, 3, 4, 5, 6, 7, 8\} : f \text{ inyectiva}\}$.

    Sea $\mathcal{R}$ la relación de equivalencia en A definida por:

    $$f \mathcal{R} g \iff f(1) + f(2) = g(1) + g(2)$$

    Sea $f \in A$ la función definida por $f(n) = n + 2$.

    ¿Cuántos elementos tiene su clase de equivalencia?

16. Determinar cuántas funciones $f : \{1, 2, \ldots, 8\} \to \{1, 2, \ldots, 12\}$ satisfacen simultáneamente las condiciones

    - f es inyectiva,
    - $f(5) + f(6) = 6$,
    - $f(1) \leq 6$.

Número combinatorio

17. i) ¿Cuántos subconjuntos de 4 elementos tiene el conjunto $\{1,2,3,4,5,6,7\}$?
    ii) ¿Y si se pide que 1 pertenezca al subconjunto?
    iii) ¿Y si se pide que 1 no pertenezca al subconjunto?
    iv) ¿Y si se pide que 1 o 2 pertenezcan al subconjunto pero no simultáneamente los dos?

18. Sea $A = \{n \in \mathbb{N} : n \leq 20\}$. Calcular la cantidad de subconjuntos $B \subseteq A$ que cumplen las siguientes condiciones:
    i) B tiene 10 elementos y contiene exactamente 4 múltiplos de 3.
    ii) B tiene 5 elementos y no hay dos elementos de B cuya suma sea impar.

19. Dadas dos rectas paralelas en el plano, se marcan n puntos distintos sobre una y m puntos distintos sobre la otra. ¿Cuántos triángulos se pueden formar con vértices en esos puntos?

20. Determinar cuántas funciones $f : \{1,2,\ldots,11\} \to \{1,2,\ldots,16\}$ satisfacen simultáneamente las condiciones
    - f es inyectiva,
    - Si n es par, $f(n)$ es par,
    - $f(1) \leq f(3) \leq f(5) \leq f(7)$.

21. ¿Cuántos anagramas tienen las palabras *estudio*, *elementos* y *combinatorio*?

22. ¿Cuántas palabras se pueden formar permutando las letras de *cuadros*
    i) con la condición de que todas las vocales estén juntas?
    ii) con la condición de que las consonantes mantengan el orden relativo original?
    iii) con la condición de que nunca haya dos (o más) consonantes juntas?

23. Con la palabra *polinomios*,
    i) ¿Cuántos anagramas pueden formarse en los que las dos letras i no estén juntas?

ii) ¿Cuántos anagramas pueden formarse en los que la letra n aparezca a la izquierda de la letra s y la letra s aparezca a la izquierda de la letra p (no necesariamente una al lado de la otra)?

24. Pedro compró 14 unidades de fruta: 6 duraznos, 2 naranjas, 1 banana, 1 pera, 1 higo, 1 kiwi, 1 ciruela y 1 mandarina. Su propósito es comer una fruta en cada desayuno y merienda. Determinar de cuántas formas puede organizar sus refrigerios de esa semana si no quiere consumir más de una naranja por día.

25. Un grupo de 15 amigos organiza un asado en un club al que llegarán en 3 autos distintos (4 por auto) y 3 irán caminando. Sabiendo que solo importa en qué auto están o si van caminando, determinar de cuántas formas pueden viajar si se debe cumplir que al menos uno entre Lucía, María y Diego debe ir en auto, y que Juan y Nicolás tienen que viajar en el mismo auto.

26. Probar que $\binom{2n}{n} > n\,2^n\,, \quad \forall\, n \geq 4\,.$

27. Sea $(a_n)_{n\in\mathbb{N}}$ la sucesión definida por

$$a_1 = 2 \quad \text{y} \quad a_{n+1} = 4a_n - 2\frac{(2n)!}{(n+1)!\,n!} \qquad (n \in \mathbb{N})$$

Probar que $a_n = \binom{2n}{n}$.

28. En este ejercicio no hace falta usar inducción.

i) Probar que $\displaystyle\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$ $\left(\text{sug: } \binom{n}{k} = \binom{n}{n-k}\right)$.

ii) Probar que $\displaystyle\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0\,.$

iii) Probar que $\displaystyle\sum_{k=0}^{2n} \binom{2n}{k} = 4^n$ y deducir que $\binom{2n}{n} < 4^n\,.$

iv) Calcular $\displaystyle\sum_{k=0}^{2n+1} \binom{2n+1}{k}$ y deducir $\displaystyle\sum_{k=0}^{n} \binom{2n+1}{k}$.

29. Sea $X = \{1, 2, \ldots, 20\}$, y sea $\mathcal{R}$ la relación de orden en $\mathcal{P}(X)$ definida por:

$$A\,\mathcal{R}\,B \iff A - B = \emptyset$$

¿Cuántos conjuntos $A \in \mathcal{P}(X)$ cumplen simultáneamente $\#A \geq 2$ y $A\,\mathcal{R}\,\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$?

30. Sea $X = \{1, 2, 3, 4, 5, 5, 7, 8, 9, 10\}$, y sea $\mathcal{R}$ la relación de equivalencia en $\mathcal{P}(X)$ definida por:

$$A \mathcal{R} B \iff A \cap \{1, 2, 3\} = B \cap \{1, 2, 3\}.$$

¿Cuántos conjuntos $B \in \mathcal{P}(X)$ de exactamente 5 elementos tiene la clase de equivalencia $\overline{A}$ de $A = \{1, 3, 5\}$?

31. Sean $X = \{n \in \mathbb{N} : n \leq 100\}$ y $A = \{1\}$ ¿Cuántos subconjuntos $B \subseteq X$ satisfacen que el conjunto $A \Delta B$ tiene a lo sumo 2 elementos?

32. i) Sea A un conjunto con $2n$ elementos. ¿Cuántas relaciones de equivalencia pueden definirse en A que cumplan la condición de que para todo $a \in A$ la clase de equivalencia de a tenga n elementos?

    ii) Sea A un conjunto con $3n$ elementos. ¿Cuántas relaciones de equivalencia pueden definirse en A que cumplan la condición de que para todo $a \in A$ la clase de equivalencia de a tenga n elementos?

Capítulo 4

Enteros – Primera parte.

4.1 Hechos generales.

El conjunto de los *números enteros* es:

$$\mathbb{Z} \;=\; \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} \;=\; -\mathbb{N} \cup \{0\} \cup \mathbb{N},$$

donde $-\mathbb{N} := \{\, -n; n \in \mathbb{N}\,\})$.

Una de las razones de la necesidad de trabajar con estos números es que en $\mathbb{N}$ no se puede restar (en general), es decir la ecuación $x+a=b$ con $a > b \in \mathbb{N}$ no tiene solución en $\mathbb{N}$. Así $\mathbb{Z}$ se obtiene a partir de $\mathbb{N}$ agregándole los números negativos.

En $\mathbb{Z}$ la operación $+$ cumple que para todo $a, b \in \mathbb{Z}$, $a+b \in \mathbb{Z}$, y satisface además las siguientes propiedades, que le dan una estructura de *Grupo Conmutativo*:

- *Conmutatividad:* Para todo $a, b \in \mathbb{Z}$, $a+b = b+a$.
- *Asociatividad:* Para todo $a, b, c \in \mathbb{Z}$, $(a+b)+c = a+(b+c)$ (y por lo tanto, se puede escribir $a+b+c$ sin aclarar qué se suma primero).
- *Existencia de Elemento Neutro:* Existe un elemento en $\mathbb{Z}$ (que resulta único), el 0, que satisface que para todo $a \in \mathbb{Z}$, $a+0 = a$.
- *Existencia de Opuesto:* Para todo $a \in \mathbb{Z}$, existe un (único) elemento, que se nota $-a$, que satisface que $a+(-a) = 0$.

A los grupos conmutativos, se los suele llamar *grupos abelianos*, por el matemático noruego *Niels Henrik Abel*, 1802-1829, y en honor a quién se otorga anualmente desde el año 2003 el Premio Abel, distinción matemática comparable a los Premios Nobel. (¿Sabía que no hay Premio Nobel de Matemática?)

O sea $(\mathbb{Z}, +)$ es un grupo abeliano. La razón por la que se le da un nombre a los conjuntos con una operación que sastisface las 4 propiedades mencionadas, es que se observó que hay muchísimos conjuntos que, junto con una operación, satisfacen esas propiedades (por ejemplo, con la suma, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^2$, $\mathbb{R}[X]$, ...) y entonces, a fin de estudiar las consecuencias de esas propiedades, conviene hacerlo de una vez por todos en el caso abstracto general y luego aplicarlo en cada caso en lugar de estudiarlas para cada conjunto en particular.

En $\mathbb{Z}$ también se puede multiplicar: la operación $\cdot$ cumple que para todo $a, b \in \mathbb{Z}$, $a \cdot b \in \mathbb{Z}$. Y además cumple propiedades parecidas a $+$, aunque no todas:

- *Conmutatividad:* Para todo $a, b \in \mathbb{Z}$, $a \cdot b = b \cdot a$.
- *Asociatividad:* Para todo $a, b, c \in \mathbb{Z}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c) (= a \cdot b \cdot c = a\, b\, c)$.
- *Existencia de Elemento Neutro:* Existe un elemento en $\mathbb{Z}$ (único) que es el 1, que satisface que para todo $a \in \mathbb{Z}$, $1 \cdot a = a$.

La propiedad siguiente relaciona el producto con la suma:

- *Distributividad del producto sobre la suma:* Para todo $a, b, c \in \mathbb{Z}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

Estas propiedades de la suma y el producto en $\mathbb{Z}$ hacen que $\mathbb{Z}$ tenga una estructura de lo que se llama *anillo conmutativo* (estructura que conviene estudiar en general por las mismas razones que conviene estudiar la de grupo). O sea $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo.

El conjunto de los números enteros $\mathbb{Z}$ con el producto también cumple otra importante propiedad,

$$\forall\, a, b \in \mathbb{Z}: \quad a \cdot b = 0 \implies a = 0 \text{ o } b = 0,$$

que lo convierte en un *dominio íntegro*. Esta propiedad es la que permite simplificar un factor común no nulo:

$$a \cdot b = a \cdot c \text{ y } a \neq 0 \implies b = c,$$

ya que $ab = ac \Leftrightarrow a(b - c) = 0$, y si $a \neq 0$ entonces $b - c = 0$, o sea $b = c$.

El conjunto $\mathbb{Z}$ se diferencia del conjunto de los números racionales $\mathbb{Q}$ (que como veremos más adelante tiene una estructura de cuerpo) ya que como veremos enseguida, en general los números enteros no tienen inverso multiplicativo: los únicos elementos inversibles a de $\mathbb{Z}$ para el producto, o sea

que satisfacen que existe $a^{-1} \in \mathbb{Z}$ de manera que $a \cdot a^{-1} = 1$, son el 1 y el -1.

Recordemos otras propiedades que ya conocemos de $\mathbb{Z}$ o también de subconjuntos de $\mathbb{Z}$:

- $\mathbb{Z}$ es un conjunto inductivo, que contiene estrictamente a $\mathbb{N}$ y para el cual no vale así nomás el principio de inducción ya que no tiene primer elemento por el cual empezar la inducción.
- Si fijamos $n_0 \in \mathbb{Z}$, en $\mathbb{Z}_{n_0} := \{m \in \mathbb{Z}; m \geq n_0\}$ vale el principio de inducción empezando en n_0. Por ejemplo en $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ vale el principio de inducción.
- Equivalentemente, $\mathbb{Z}_{n_0}$ y $\mathbb{N}_0$ son conjuntos bien ordenados, o sea, cualquier subconjunto no vacío de $\mathbb{Z}_{n_0}$ o $\mathbb{N}_0$ tiene primer elemento o mínimo (un elemento en el subconjunto menor o igual que todos los demás).

4.2 Divisibilidad.

El hecho que los números enteros no son divisibles (con cociente entero) por cualquier otro número entero hace interesante estudiar la noción y consecuencias de la *divisibilidad*. Este estudio no se justifica por ejemplo de la misma manera en $\mathbb{Q}$ o $\mathbb{R}$ donde todo número racional o real es divisible (con cociente racional o real) por cualquier otro número racional o real no nulo.

Definición 4.2.1. (Divisibilidad.)

Sean $a, d \in \mathbb{Z}$ con $d \neq 0$. Se dice que d *divide* a a, y se nota $d \mid a$, si existe un elemento $k \in \mathbb{Z}$ tal que $a = k \cdot d$ (o sea si el cociente $\frac{a}{d}$ es un número entero). También se dice en ese caso que a es divisible por d, o que a es múltiplo de d. O sea:

$$d \mid a \iff \exists\, k \in \mathbb{Z} : a = k \cdot d.$$

En caso contrario, se dice que d no divide a a, y se nota $d \nmid a$. Eso es cuando el cociente $\frac{a}{d} \notin \mathbb{Z}$, o sea no existe ningún entero $k \in \mathbb{Z}$ tal que $a = k \cdot d$.

El conjunto de los divisores positivos y negativos de un entero a se notará por $\mathrm{Div}(a)$ y el de los divisores positivos por $\mathrm{Div}_+(a)$.

<u>*Nota:*</u> En algunos textos o clases no excluyen el caso $d = 0$ pero se conviene que 0 divide únicamente al 0, pues $a = k \cdot 0$ implica $a = 0$. Igualmente en estas notas excluiremos el caso $d = 0$ para no "dividir por 0".

Ejemplos:

- $7 \mid 56$ pues $56 = 8 \cdot 7$.
- $7 \mid -56$, $-7 \mid 56$, $-7 \mid -56$.
- $7 \nmid 54$.
- $\mathrm{Div}(-12) = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$,
  $\mathrm{Div}_+(-12) = \{1, 2, 3, 4, 6, 12\}$.
- $\mathrm{Div}(1) = \{-1, 1\}$.

Propiedades 4.2.2. (De la divisibilidad.)

- Todo número entero $d \neq 0$ satisface que $d \mid 0$ pues $0 = 0 \cdot d$ (aquí $k = 0$). Así el 0 tiene infinitos divisores : $\mathrm{Div}(0) = \mathbb{Z} \setminus \{0\}$.
- $d \mid a \Leftrightarrow -d \mid a$ (pues $a = k \cdot d \Leftrightarrow a = (-k) \cdot (-d)$).

  De la misma manera $d \mid a \Leftrightarrow d \mid -a \Leftrightarrow -d \mid -a$.

  Se concluye que $d \mid a \Leftrightarrow |d| \mid |a|$ (donde $|x|$ denota el módulo o valor absoluto de x).

  En particular a cada divisor negativo de a le corresponde un divisor positivo.
- Si $a \neq 0$, $d \mid a \Rightarrow |d| \leq |a|$ (pues $|a| = k|d|$ con $|a| \neq 0$ implica k es un entero no nulo y positivo, es decir $k \geq 1$; por lo tanto, $|a| = k|d| \geq |d|$).

  En particular, todo número entero a *no nulo* tiene sólo un número finito de divisores, todos pertenecientes al conjunto

  $$\{-|a|, \ldots, -1, 1, \ldots, |a|\}.$$

  O sea $\mathrm{Div}_+(a) \subset \{1, \ldots, |a|\}$.

  Además, por la observación del inciso anterior, el número total de divisores de a es el doble del número de divisores positivos.
- Ahora podemos probar fácilmente que los únicos números enteros que son inversibles son 1 y -1. Es claro que tanto 1 como -1 son inversibles (sus inversas son ellos mismos). Por otro lado, si $a \in \mathbb{Z}$ inversible, entonces existe $b \in \mathbb{Z}$ tal que $ab = 1$. Esto implica que $a \neq 0$ (pues $0 \cdot b = 0$, $\forall b \in \mathbb{Z}$), y por lo tanto $a \mid 1$. Pero por lo anterior, esto implica que $|a| \leq 1$, es decir $a = \pm 1$.
- $d \mid a$ y $a \mid d \Leftrightarrow a = \pm d$ (pues $a = k \cdot d$ y $d = j \cdot a$ implica que $a = (k \cdot j) \cdot a$, por lo tanto k y j son dos números enteros que satisfacen $k \cdot j = 1$, o sea, $k = \pm 1$).

- Para todo $a \in \mathbb{Z}$, se tiene $1 \mid a$ y $-1 \mid a$, y también $a \mid a$ y $-a \mid a$.

  Así, si $a \neq \pm 1$, a tiene por lo menos 4 divisores distintos $(\pm 1, \pm a)$, o 2 divisores positivos distintos $(1, |a|)$.

  Hay números enteros que tienen únicamente esos 4 divisores, que son los asegurados, otros tienen más. Esto motiva la separación de los números enteros (distintos de 0, 1 y -1) en dos categorías, la de los números *primos* y la de los números *compuestos* :

Definición 4.2.3. (Números primos y compuestos.)

- Se dice que $a \in \mathbb{Z}$ es un número *primo* si $a \neq 0, \pm 1$ y tiene únicamente 4 divisores (o 2 divisores positivos). Por ejemplo $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11$.

  (En general los números primos se notan con las letras p, q,...)

- Se dice que a es un número *compuesto* si $a \neq 0, \pm 1$ y tiene más que 4 divisores (o más que 2 divisores positivos). Por ejemplo $\pm 4, \pm 6, \pm 8, \pm 9$.

  Se observa que a es compuesto si y sólo si tiene un divisor positivo d que satisface $2 \leq d \leq |a| - 1$ (pues ya vimos que $\mathrm{Div}_+(a) \subset \{1, \ldots, |a|\}$ y si a tiene más que 2 divisores positivos, tiene que haber uno en "algún lugar en el medio").

<u>*Nota:*</u> Esta definición de número primo es la histórica que aprendemos todos en el colegio y está en todos lados. Pero de hecho en matemática se hace una distinción, cuando se trabaja en dominios íntegros arbitrarios, entre los conceptos de *irreducible* (que es tener únicamente los divisores triviales, o sea lo que acá llamamos primo), y *primo*, que corresponde a una propiedad crucial que veremos más adelante. En el caso de los números enteros, como estos dos conceptos coinciden, adoptamos en estas notas el nombre tradicional.

Más adelante, se trabajará mucho más con los números primos, que cumplen propiedades importantísimas, y constituyen los ladrillos de base para construir todos los números, en el sentido que cualquier número entero (distinto de 0 y ± 1) se escribe en forma única como $\pm$ un producto de primos positivos.

Se verán ahora algunas propiedades importantes de la divisibilidad :

Propiedades 4.2.4. (De la divisibilidad.)

Sean $a, b, d \in \mathbb{Z}$, $d \neq 0$.

- $d \mid a$ y $d \mid b \Rightarrow d \mid a + b$.

  (Pues si $a = k \cdot c$ y $b = j \cdot c$ con $k, j \in \mathbb{Z}$, entonces $a + b = (k + j) \cdot c$, donde $k + j \in \mathbb{Z}$.)

- $d \mid a$ y $d \mid b \Rightarrow d \mid a-b$.
- $d \mid a+b$ no implica que $d \mid a$ y $d \mid b$: Por ejemplo, $6 \mid 4+8$ pero $6 \nmid 4$ y $6 \nmid 8$.
- Sin embargo si $d \mid a+b$ y *se sabe que* $d \mid a$, entonces $d \mid b$.

  (Pues $d \mid (a+b)-a$.)
- $d \mid a \Rightarrow d \mid c \cdot a, \ \forall c \in \mathbb{Z}$.
- $d \mid a \Rightarrow d^2 \mid a^2$ y $d^n \mid a^n, \ \ \forall n \in \mathbb{N}$.

  (Pues si $a = k \cdot d$, entonces $a^2 = k^2 \cdot d^2$ y $a^n = k^n \cdot d^n$.)

  Veremos más adelante que vale la recíproca también: si $d^2 \mid a^2$ entonces $d \mid a$, etc.)
- $d \mid a \cdot b$ no implica $d \mid a$ o $d \mid b$: Por ejemplo, $6 \mid 3 \cdot 4$ pero $6 \nmid 3$ y $6 \nmid 4$.

  Veremos más adelante que la propiedad $d \mid a \cdot b \Rightarrow d \mid a$ o $d \mid b$ se cumple cuando d es un número primo (es la propiedad más importante que cumplen los números primos). Si d no es primo, siempre se pueden econtrar a y b tales que $d \mid a \cdot b$ pero $d \nmid a$ y $d \nmid b$. ¿Quiénes?

<u>*Ejemplos:*</u>

- Hallar todos los $a \in \mathbb{Z}, a \neq 1$, tales que $a-1 \mid a^2+5$.

  Para resolver esto, se trata de poner a la derecha del símbolo $\mid$ un número fijo, de manera de trabajar después con los divisores de ese número. Para ello se puede usar por ejemplo que se sabe que $a-1 \mid a-1$, por lo tanto $a-1 \mid c\,(a-1)$ para todo $c \in \mathbb{Z}$, y en particular $a-1 \mid (a+1)(a-1)$. Así se tiene $a-1 \mid a^2+5$ y $a-1 \mid a^2-1$, por lo tanto $a-1$ divide a la diferencia, es decir $a-1 \mid 6$. Es decir $a-1 \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Por lo tanto $a \in \{-5, -2, -1, 0, 2, 3, 4, 7\}$, y se concluye verificando que para cada valor de ese conjunto es cierto que $a-1 \mid a^2+5$, o bien verificando y mostrando que en realidad todas las implicaciones usadas son equivalencias.
- Probar que para todo $a \in \mathbb{Z}, a \neq 1$, y para todo $n \in \mathbb{N}$ vale que $a-1 \mid a^n-1$.

  Esto ya se puede hacer a este nivel de distintas formas (despues veremos otra incluso) :

  – Usando la Serie Geométrica :

$$\sum_{i=0}^{n-1} a^i = \frac{a^n-1}{a-1}$$

Por lo tanto

$$a^n - 1 = (a-1)\sum_{i=0}^{n-1} a^i$$

y dado que la sumatoria da un número entero (pues es una suma de potencias de enteros) resulta que $a-1 \mid a^n - 1$.

– Usando el Binomio de Newton :

$$\begin{aligned} a^n = ((a-1)+1)^n &= \sum_{i=0}^{n} \binom{n}{i}(a-1)^i \\ &= 1 + n(a-1) + \binom{n}{2}(a-1)^2 + \cdots + (a-1)^n. \end{aligned}$$

Por lo tanto

$$a^n - 1 = (a-1)\Big(n + \binom{n}{2}(a-1) + \cdots + (a-1)^{n-1}\Big) = k\,(a-1)$$

donde $k \in \mathbb{Z}$ es la sumatoria que está dentro del gran paréntesis.

– Por inducción en n. La proposición es $p(n)$: "$a-1 \mid a^n - 1$"
$p(1)$ es Verdadera pues $a-1 \mid a-1$.
$p(h)$ Verdadera $\Rightarrow p(h+1)$ Verdadera :
HI : $a-1 \mid a^h - 1$. Se quiere probar que $a-1 \mid a^{h+1} - 1$.
Pero $a^{h+1} - 1 = a(a^h - 1) + (a-1)$, y por HI, $a-1 \mid a^h - 1$, y por otro lado, $a-1 \mid a-1$, por lo tanto $a-1$ divide a la suma, como se quería probar.

(Las dos primeras tienen la ventaja sobre la última de dar también la expresión del cociente, y la primera es la más sencilla.)

- Sean $m, n \in \mathbb{N}$. Probar que si $m \mid n$, entonces para todo $a \neq \pm 1$, $a^m - 1 \mid a^n - 1$.

  Se tiene $n = k \cdot m$, luego $a^n = (a^m)^k$. Si ponemos $A := a^m$, por el inciso anterior se tiene que $A - 1 \mid A^k - 1$, es decir $a^m - 1 \mid a^n - 1$.

4.2.1 Congruencia.

Introducimos ahora una notación debida a Carl Friedrich Gauss. La notación facilita mucho la forma de escribir y trabajar con los números enteros y la divisibilidad, además de ofrecer una clasificación muy importante de los números, como veremos en este curso.

Definición 4.2.5. (Congruencia.)

Sea $d \in \mathbb{Z}$, $d \neq 0$. Dados $a, b \in \mathbb{Z}$, se dice que a *es congruente* a b *módulo* d si $d \mid a - b$.

Se nota $a \equiv b \pmod{d}$ o también $a \equiv b\ (d)$. O sea:

$$a \equiv b \pmod{d} \iff d \mid a - b.$$

En caso contrario se nota $a \not\equiv b \pmod{d}$ o $a \not\equiv b\ (d)$.

Ejemplos:

- $5 \equiv 3 \pmod{2}$, $5 \equiv -1 \pmod{2}$, $5 \equiv 1 \pmod{2}$, $5 \not\equiv 2 \pmod{2}$, $4 \equiv 0 \pmod{2}$,
  $\forall\, k \in \mathbb{Z},\ 2k \equiv 0 \pmod{2}$ y $2k + 1 \equiv 1 \pmod{2}$.
- $13 \equiv 8 \pmod{5}$ y $13 \equiv 3 \pmod{5}$.
- Observemos que $a \equiv 0 \pmod{d} \iff d \mid a$.

Sea $d \in \mathbb{Z}$, $d \neq 0$. Se verá ahora que la relación de congruencia módulo d es una relación de equivalencia en $\mathbb{Z}$.

Proposición 4.2.6. (La congruencia es una relación de equivalencia.)

Sea $d \in \mathbb{Z}$, $d \neq 0$. *Sea* $\mathcal{R}$ *la relación en* $\mathbb{Z}$ *dada por*

$$a\ \mathcal{R}\ b \iff a \equiv b \pmod{d}, \quad \forall\, a, b \in \mathbb{Z}.$$

Entonces $\mathcal{R}$ *es una relación de equivalencia.*

Demostración.

- *Reflexividad :* Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{d}$ pues $d \mid a - a$.
- *Simetría :* Hay que probar que para todo $a, b \in \mathbb{Z}$ tales que $a \equiv b \pmod{d}$, entonces $b \equiv a \pmod{d}$. Pero $a \equiv b \pmod{d}$ significa que $d \mid a - b$, y por lo tanto $d \mid -(a - b) = b - a$, luego $b \equiv a \pmod{d}$.
- *Transitividad :* Hay que probar que para todo $a, b, c \in \mathbb{Z}$ tales que $a \equiv b \pmod{d}$ y $b \equiv c \pmod{d}$ entonces $a \equiv c \pmod{d}$. Pero $a \equiv b \pmod{d}$ significa que $d \mid a - b$, y $b \equiv c \pmod{d}$ significa que $d \mid b - c$. Por lo tanto $d \mid (a - b) + (b - c) = a - c$, es decir $a \equiv c \pmod{d}$.

□

La proposición anterior implica que la relación de equivalencia $\equiv \pmod d$ parte a los números enteros en clases de equivalencia, subconjuntos de elementos congruentes entre sí, que se "identifican" de esa manera. Por ejemplo si se toma congruencia módulo 2, quedan por un lado los pares (que son todos congruentes entre sí y también congruentes a 0 módulo 2), y por otro lado los impares (que son congruentes entre sí y congruentes a 1 módulo 2). Cuando se toma congruencia módulo 3, $\mathbb{Z}$ queda subdividido en 3 subconjuntos : los que son de la forma $3\,k$, $k \in \mathbb{Z}$, por un lado, por otro lado los que son de la forma $3\,k+1$ y por último los que se escriben como $3\,k+2$. Enseguida veremos el Algoritmo de División, y se verá que la congruencia módulo d clasifica (e identifica) los números enteros según su resto módulo d.

A continuación, se enuncian propiedades de la congruencia con respecto a la suma y al producto, que son muy útiles para trabajar.

Proposición 4.2.7. (Propiedades de la congruencia.)

Sea $d \in \mathbb{Z}$, $d \neq 0$. *Entonces :*

1. $\forall\, a_1, a_2, b_1, b_2 \in \mathbb{Z}$,

$$a_1 \equiv b_1 \pmod d \ y\ a_2 \equiv b_2 \pmod d \ \Rightarrow\ a_1 + a_2 \equiv b_1 + b_2 \pmod d.$$

2. *Para todo* $n \in \mathbb{N}$, $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$,

$$\left\{ \begin{array}{rcl} a_1 & \equiv & b_1 \pmod d \\ & \vdots & \\ a_n & \equiv & b_n \pmod d \end{array} \right. \quad \Longrightarrow \quad a_1 + \cdots + a_n \ \equiv\ b_1 + \cdots + b_n \pmod d.$$

3. $\forall\, a, b, c \in \mathbb{Z}$,

$$a \equiv b \pmod d \ \Longrightarrow\ c\,a \equiv c\,b \pmod d.$$

4. $\forall\, a_1, a_2, b_1, b_2 \in \mathbb{Z}$,

$$a_1 \equiv b_1 \pmod d \ y\ a_2 \equiv b_2 \pmod d \ \Rightarrow\ a_1\,a_2 \equiv b_1\,b_2 \pmod d.$$

5. *Para todo* $n \in \mathbb{N}$, $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$,

$$\left\{ \begin{array}{rcl} a_1 & \equiv & b_1 \pmod d \\ & \vdots & \\ a_n & \equiv & b_n \pmod d \end{array} \right. \quad \Longrightarrow \quad a_1 \cdots a_n \ \equiv\ b_1 \cdots b_n \pmod d.$$

6. $\forall\, a, b \in \mathbb{Z}$, $n \in \mathbb{N}$,

$$a \equiv b \pmod d \ \Rightarrow\ a^n \equiv b^n \pmod d.$$

Demostración. 1. $a_1 \equiv b_1 \pmod{d}$ y $a_2 \equiv b_2 \pmod{d}$ implican por definición $d \mid a_1 - b_1$ y $d \mid a_2 - b_2$. Por lo tanto $d \mid (a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$, es decir $a_1 + a_2 \equiv b_1 + b_2 \pmod{d}$.

2. Por inducción en n.

3. Se deja como ejercicio.

4. Para probar esto se puede usar por ejemplo el inciso (1) y la transitividad : como $a_1 \equiv b_1 \pmod{d}$, entonces $a_1\, a_2 \equiv b_1\, a_2 \pmod{d}$ (multiplicando por a_2), y por otro lado, como $a_2 \equiv b_2 \pmod{d}$, se tiene $b_1\, a_2 \equiv b_1\, b_2 \pmod{d}$ (multiplicando por b_2), y finalmente por transitividad, se concluye que $a_1\, a_2 \equiv b_1\, b_2 \pmod{d}$.

5. Por inducción en n.

6. Se ve tomando en el inciso anterior $a_1, \ldots, a_n$ todos iguales a un mismo número a y $b_1, \ldots, b_n$ todos iguales a un mismo número b.

□

Ejemplos:

- Probemos ahora usando congruencia que $\forall\, a \in \mathbb{Z}, a \neq 1$, $\forall\, n \in \mathbb{N}$, $a - 1 \mid a^n - 1$:

$$\begin{aligned} a - 1 \mid a - 1 \Rightarrow\ & a \equiv 1 \pmod{(a-1)} \\ \Rightarrow\ & a^n \equiv 1^n \pmod{(a-1)} \\ \Rightarrow\ & a - 1 \mid a^n - 1. \end{aligned}$$

- Probar que para todo $n \in \mathbb{N}_0$ vale que $64 \mid 49^n + 16n - 1$:

  Se probará por inducción en n.

$$p(n): \quad 64 \mid 49^n + 16n - 1.$$

  - $p(0)$ es Verdadera pues $64 \mid 49^0 + 16 \cdot 0 - 1 = 0$.
  - $p(h)$ Verdadera $\Longrightarrow p(h+1)$ Verdadera :
    HI : $64 \mid 49^h + 16h - 1$, o sea $49^h \equiv -16h + 1 \pmod{64}$.
    Se quiere probar que $64 \mid 49^{h+1} + 16(h+1) - 1$.
    Por HI, $49^{h+1} = 49 \cdot 49^h \equiv 49\,(-16h + 1) \pmod{64}$.
    Por lo tanto,

$$49^{h+1} + 16(h+1) - 1 \equiv 49\,(-16h + 1) + 16(h+1) - 1 \pmod{64}.$$

    Distribuyendo y factorizando, resulta :

$$49^{h+1} + 16(h+1) - 1 \equiv -48 \cdot 16h + 64 \pmod{64}.$$

Pero $64 \equiv 0 \pmod{64}$ (pues $64 \mid 64$) y $-48 \cdot 16h \equiv 0 \pmod{64}$ (pues $64 \mid -48 \cdot 16h$), por lo tanto $-48 \cdot 16h + 64 \equiv 0 + 0 \pmod{64}$, y, de nuevo por transitividad, resulta

$$49^{h+1} + 16(h+1) - 1 \equiv 0 \pmod{64},$$

o sea $64 \mid 49^{h+1} + 16(h+1) - 1$ como se quería probar.

Se concluye que $64 \mid 49^n + 16n - 1$ para todo $n \in \mathbb{N}$.

4.3 Algoritmo de división.

Vamos a enunciar y demostrar ahora el bien conocido algoritmo de división entera.

Teorema 4.3.1. (Algoritmo de división.)

Dados $a, d \in \mathbb{Z}$ *con* $d \neq 0$, existen $k, r \in \mathbb{Z}$ *que satisfacen*

$$a = k \cdot d + r \quad \text{con} \quad 0 \leq r < |d|.$$

Además, k *y* r *son* únicos *en tales condiciones.*

Se dice que k es el *cociente* y r es el *resto* de la división de a por d (a es el *dividendo* y d el *divisor*). Al resto r lo notaremos $r_d(a)$ para especificar que es el "resto de a al dividir por d".

Antes de pasar a la demostración, hagamos algunos ejemplos:

Ejemplos:

- $a = 1038, d = 14$:

  $k = 74, r = r_{14}(1038) = 2$ ya que $1038 = 74 \cdot 14 + 2$ con $0 \leq 2 < 14 = |d|$.

- $a = 1038, d = -14$:

  $k = -74, r = r_{-14}(1038) = 2$ ya que $1038 = 74 \cdot 14 + 2 = (-74) \cdot (-14) + 2$

  con $0 \leq 2 < 14 = |d|$.

- $a = -1038, d = 14$:

  $$1038 = 74 \cdot 14 + 2 \implies -1038 = -74 \cdot 14 - 2 \quad \text{pero} \quad -2 < 0.$$

  Hay que corregirlo, se hace restando y sumando el (módulo del) divisor 14:

  $$-1038 = (-74 \cdot 14 - 14) + (14 - 2) = -75 \cdot 14 + 12,$$

  y por lo tanto $k = -75, r = r_{14}(-1038) = 12$ ya que $0 \leq 12 < 14 = |d|$.

- $a = -1038, d = -14$:

  $$1038 = 74 \cdot 14 + 2 \implies -1038 = 74 \cdot (-14) - 2 \quad \text{pero} \quad -2 < 0.$$

  Se corrige nuevamente como arriba restando y sumando el módulo del divisor -14:

  $$-1038 = (74 \cdot (-14) - 14) + (14 - 2) = 75 \cdot (-14) + 12,$$

  y por lo tanto $k = 75, r = r_{-14}(-1038) = 12$ ya que $0 \leq 12 < 14 = |d|$.

La conclusión —como veremos en la demostración del teorema— es que para saber dividir números positivos o negativos por divisores positivos o negativos, alcanza saber hacerlo para números y divisores positivos y luego corregir cociente y/o resto en cada caso.

Demostración. (Del algoritmo de división.)

El teorema consta de dos afirmaciones, la parte existencial, que requiere mostrar que existen k y r en las condiciones del teorema, y luego la unicidad: mostrar que no puede haber dos pares distintos de cociente y resto para a y d dados.

Existencia: Vamos a probar primero en detalle el caso $a \geq 0, d > 0$, ya que, como nos sugieren los ejemplos, los otros casos se reducen a ese.

- Caso $a \geq 0, d > 0$:

  Aquí, $|d| = d$. La idea intuitiva es considerar los elementos

  $$a,\ a - d,\ a - 2d,\ a - 3d, \ldots$$

  hasta que caigamos en algún elemento menor que d pero aún mayor o igual que cero. Este será el resto. Formalizamos esta idea de la manera siguiente:

  Sea A el subconjunto de $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ formado por los números de la forma $a - j\,d$ para algún $j \in \mathbb{Z}$, es decir:

  $$A = \{\, a - j\,d,\ j \in \mathbb{Z}\} \cap \mathbb{N}_0.$$

  Claramente A es un subconjunto de $\mathbb{N}_0$ que no es vacío ya que $a = a - 0 \cdot d$ pertenece a A (estamos considerando el caso $a \geq 0$). Luego, el conjunto A tiene un mínimo. Llamemos r a ese mínimo. Se tiene que $r \in A$ por un lado, y por otro lado r es menor o igual que todos los demás elementos de A.

Como $r \in A$, existe un entero, llamémoslo k, que satisface que $r = a - k\,d$, o sea $a = k\,d + r$.

Falta probar que $0 \leq r < d$ (ya que $|d| = d$ en el caso que estamos considerando):

Claramente $r \geq 0$ ya que pertenece a A que es un subconjunto de $\mathbb{N}_0$.

Si r fuese mayor o igual que d, entonces $r - d \geq 0$ aún. Luego se tendría que el elemento $r - d = a - k\,d - d = a - (k+1)\,d$ está también en el conjunto A pero es menor que r ! Eso contradice que r sea el mínimo. Así, se concluye que no puede ocurrir que $r \geq d$, luego $r < d$.

- Caso $a \geq 0, d < 0$:

  En este caso, $-d > 0$ (y por lo tanto $|d| = -d$) y se tiene que por el caso anterior, existen k', r' tal que $a = k'\,(-d) + r'$ con $0 \leq r' < |d|$. Se obtiene directamente $a = (-k')\,d + r'$, luego $k = -k', r = r'$.

- Caso $a < 0$:

  En este caso, tenemos $-a > 0$, y de los casos anteriores existen k', r' tal que $-a = k'\,d + r'$ con $0 \leq r' < |d|$. Luego $a = (-k')\,d - r'$.

  Si $r' = 0$, r' cumple la condición de resto y se obtiene $k = -k', r = r' = 0$.

  Pero si $r' \neq 0$, hay que corregirlo restando y sumando $|d|$ a la expresión:

  $$a = (-k')\,d - r' = ((-k')\,d - |d|) + (|d| - r').$$

  Así, si se define $k := -k' \pm 1$ según si $d < 0$ o $d > 0$, y $r := |d| - r'$, se tiene $a = k\,d + r$ con $0 < r < |d|$, ya que

  $$\begin{aligned} 0 < r' < |d| &\iff -|d| < -r' < 0 \\ &\implies |d| - |d| < |d| - r' < |d| - 0 \\ &\implies 0 < r < |d|. \end{aligned}$$

Unicidad: Supongamos que tenemos dos pares de cocientes y restos, k, r y k', r'. Vamos a probar que entonces $k = k'$ y $r = r'$.

Sin perdida de generalidad, podemos suponer que $r \leq r'$, y luego:

$$a = k\,d + r = k'\,d + r' \text{ con } 0 \leq r \leq r' < |d|.$$

Así, $(k - k')\,d = r' - r \;\Rightarrow\; d \,|\, r' - r \;\Rightarrow\; |d| \,|\, r' - r$. Como $r' - r \geq 0$ por ser $r' \geq r$, si $r' - r \neq 0$, se tiene, por lo que vimos en divisibilidad, que $|d| \leq r' - r$. Pero es fácil verificar que, dado que $r' < |d|$, $r' - r < |d| - r < |d|$ (ya que $r \geq 0$). Luego no puede ser $r' - r \neq 0$, es decir tiene que ser $r' = r$.

Se concluye que $(k-k')\,d=0$ y como $d\neq 0$, $k-k'=0$, es decir $k=k'$ también. □

Observación 4.3.2. Si $0\leq a<|d|$, entonces $a=0\cdot d+a$ implica $k=0$ y $r=r_d(a)=a$ pues a cumple la condición que tiene que cumplir el resto (se aplica la unicidad del cociente y el resto).

Algoritmo de división iterativo para calcular (k,r) donde k es el cociente y r es el resto de la división de a por $d\neq 0$.

- Si $a\geq 0$ y $d>0$:
  - Tomar $k=0$, $r=a$.
  - Mientras que $r\geq d$, reemplazar
    - $k\leftarrow k+1$
    - $r\leftarrow r-d$.
  - Dar como respuesta (k,r).
- Si $a\geq 0$ y $d<0$:
  - Aplicar el algoritmo a a y $-d$.
  - Dar como respuesta $(-k,r)$.
- Si $a<0$ y $d>0$:
  - Aplicar el algoritmo a $-k$ y d.
  - Si $r=0$, dar como respuesta $(-k,0)$.
  - Si no, dar como respuesta $(-k-1,d-r)$.
- Si $a<0$ y $d<0$:
  - Aplicar el algoritmo a $-a$ y $-d$.
  - Si $r=0$, dar como respuesta $(-k,0)$.
  - Si no, dar como respuesta $(k+1,-r-d)$.

De hecho el algoritmo para obtener el cociente y el resto tiene una naturaleza intrínsecamente recursiva. Esto es fácil de ver para números no negativos ya que si $a\geq d$ y $a-d=k'd+r'$ con $0\leq r'<d$, entonces $a=(k'+1)d+r'$. Es decir $a=kd+r$ con $0\leq r<d$, donde $k=k'+1$ y $r=r'$.

En Haskell existen funciones preestablecidas que dan el cociente y el resto de la división entera: éstas son las funciones *div* y *mod*: div a d devuelve el cociente k y mod a d devuelve el resto $r_d(a)$ de la división de a por d. En el caso de números no negativos, si uno quisiera describir un algoritmo en Haskell que devuelva el par (div, mod), uno muy ingenuo y muy lento podría ser, módulo posibles errores de sintáxis:

Algoritmo de división recursivo en Haskell para calcular (k,r) donde k es el cociente y r es el resto de la división de a por d para números enteros *no negativos* a y d.

```
division :: Integer → Integer → (Integer,Integer)
division a d | a < d = (0, a)
             | otherwise = (1 + k, r)
               where (k, r) = division(a − d) d
```

La observación siguiente relaciona el algoritmo de división con la divisibilidad. Es inmediata pero esencial:

Observación 4.3.3. (Divisibilidad y resto.)

Sean $a, d \in \mathbb{Z}$, $d \neq 0$. Entonces

$$r_d(a) = 0 \iff d \mid a \iff a \equiv 0 \pmod{d}.$$

Esto observación se extiende inmediatamente:

Proposición 4.3.4. (Congruencia y resto.)

Sea $d \in \mathbb{Z}$, $d \neq 0$. *Entonces*

1. $a \equiv r_d(a) \pmod{d}$, $\forall\, a \in \mathbb{Z}$.
2. $a \equiv r \pmod{d}$ *con* $0 \leq r < |d| \;\Rightarrow\; r = r_d(a)$.
3. $r_1 \equiv r_2 \pmod{d}$ *con* $0 \leq r_1, r_2 < |d| \;\Rightarrow\; r_1 = r_2$.
4. $a \equiv b \pmod{d} \iff r_d(a) = r_d(b)$.

Demostración. 1. Pues $a = k\,d + r_d(a) \;\Rightarrow\; a - r_d(a) = k\,d \;\Rightarrow\; a \equiv r_d(a) \pmod{d}$.

2. $a \equiv r \pmod{d} \;\Rightarrow\; d \mid a - r \;\Rightarrow\; a - r = k\,d$ para algún $k \in \mathbb{Z}$ $\Rightarrow\; a = k\,d + r$.
   Pero la condición $0 \leq r < |d|$ implica entonces que $r = r_d(a)$. (Se usa aquí la unicidad del resto.)

3. $r_1 = 0 \cdot d + r_1$ con $0 \leq r_1 < |d| \;\Rightarrow\; r_1 = r_d(r_1)$.
   Pero por otro lado, $r_1 \equiv r_2 \pmod{d}$ con $0 \leq r_2 < |d| \;\Rightarrow r_2 = r_d(r_1)$ por (2). Se concluye que $r_1 = r_2$ por la unicidad del resto.

4. ($\Rightarrow$) $a \equiv b \pmod{d}$, y $a \equiv r_d(a) \pmod{d}$, $b \equiv r_d(b) \pmod{d}$ por (1). Luego, por transitividad (y simetría) $r_d(a) \equiv r_d(b) \pmod{d}$. Por (3) se obtiene entonces $r_d(a) = r_d(b)$.
   ($\Leftarrow$) $r_d(a) = r_d(b) \;\Rightarrow\; r_d(a) \equiv r_d(b) \pmod{d}$, y juntando por transitividad (y simetría) con $a \equiv r_d(a) \pmod{d}$, $b \equiv r_d(b) \pmod{d}$, resulta $a \equiv b \pmod{d}$.

□

Por lo tanto la relación de equivalencia $\equiv \pmod d$ parte a los números enteros en clases de equivalencia

$$\overline{a} = \{b \in \mathbb{Z} : b \equiv a \pmod d\} = \{b \in \mathbb{Z} : r_d(b) = r_d(a)\},$$

formadas por elementos que tienen todos el mismo resto módulo d. En cada clase podemos elegir el representante más sencillo r con $0 \leq r < |d|$, y hay d clases de equivalencia distintas, $\overline{0}, \ldots, \overline{d-1}$. Se obtiene la partición

$$\mathbb{Z} = \overline{0} \cup \cdots \cup \overline{d-1}.$$

Retomaremos este tema más adelante cuando hablaremos del anillo de restos módulo d.

Además la proposición anterior implica que para calcular el resto de un número módulo d, alcanza con lograr poner a la derecha de la congruencia módulo d un número r con $0 \leq r < |d|$. (Justamente ya mencionamos que en Haskell la instrucción que dados $a, d \in \mathbb{Z}$, $d \neq 0$, calcula el resto $r_d(a)$ de a dividido por d es la instrucción mod $a\, d$. Pero no perdamos de vista que a la derecha de la congruencia podemos poner no sólo el resto $r_d(a)$ sino cualquier número b que tiene el mismo resto que a al dividir por d.

Ejemplos:

- Calcular el resto de dividir por 5 a $166^{1328} \cdot 4878 + 199999$:

  Cada número es congruente a su resto, luego

  $$\begin{cases} 166 \equiv 1 \pmod 5 \\ 4878 \equiv 3 \pmod 5 \\ 199999 \equiv 4 \pmod 5 \end{cases}$$

  Por lo tanto,

  $$\begin{aligned} 166^{1328} \cdot 4878 + 199999 &\equiv 1^{1328} \cdot 3 + 4 \pmod 5 \\ &\equiv 7 \pmod 5 \\ &\equiv 2 \pmod 5 \end{aligned}$$

  Dado que 2 cumple la condición de ser resto módulo 5, se concluye que 2 es el resto.

- Calcular el resto de dividir por 35 a $34^{17771} - 6^{1001}$:

  La congruencia es más fuerte que pensar sólo en el resto. A veces en lugar de reemplazar los números por su resto conviene reemplazarlos por -1 (si se puede) u observar algún comportamiento útil. Aquí por ejemplo se puede usar que $6^2 = 36 \equiv 1 \pmod{35}$ y también que

$34 \equiv -1 \pmod{35}$. Luego:

$$\begin{aligned} 34^{17771} - 6^{1001} &= 34^{17771} - 6^{2\cdot 500+1} \\ &= 34^{17771} + (6^2)^{500} \cdot 6^1 \\ &\equiv (-1)^{17771} - 1^{500} \cdot 6 \pmod{35} \\ &\equiv -1 - 6 \pmod{35} \\ &\equiv -7 \pmod{35} \\ &\equiv 28 \pmod{35}. \end{aligned}$$

Por lo tanto el resto es 28.

Aplicando la Proposición 4.2.7, también se obtiene como consecuencia de la Proposición 4.2.7 el siguiente comportamiento de los restos con respecto a sumas, productos y potencias.

Corolario 4.3.5. (Tablas de Restos.)

Sean $a, b, d \in \mathbb{Z}$, $d \neq 0$. *Entonces*

- $r_d(a+b) = r_d\big(r_d(a) + r_d(b)\big)$.
- $r_d(a \cdot b) = r_d\big(r_d(a) \cdot r_d(b)\big)$.
- $r_d(a^n) = r_d\big(r_d(a)^n\big),\ \forall\, n \in \mathbb{N}$.

Demostración.

$$\begin{cases} a \equiv r_d(a) \pmod{d} \\ b \equiv r_d(b) \pmod{d} \end{cases} \implies \begin{cases} a+b \equiv r_d(a) + r_d(b) \pmod{d} \\ a \cdot b \equiv r_d(a) \cdot r_d(b) \pmod{d} \\ a^n \equiv r_d(a)^n \pmod{d},\ \forall\, n \in \mathbb{N}. \end{cases}$$

Por lo tanto, según la proposición anterior, las expresiones a la izquierda y a la derecha del signo $\equiv$ tienen los mismos restos. □

Ejemplo: Probar que $\forall\ a \in \mathbb{Z}$ tal que $7 \nmid a$, $r_7(a^3) = 1$ o 6. Aplicando las tablas de restos, $r_7(a^3) = r_7\big(r_7(a)^3\big)$ y como $7 \nmid a \Leftrightarrow r_7(a) \neq 0$, alcanza con analizar la tabla

a	1	2	3	4	5	6
a^2	1	4	2	2	4	1
a^3	1	1	6	1	6	6

,

donde la primer fila indica los posibles restos de a módulo 7, la segunda fila los restos correspondientes de a^2 módulo 7 y la tercera fila los restos correspondientes de a^3 módulo 7. O sea por ejemplo si $a \equiv 3 \pmod{7}$, entonces $a^3 \equiv 6 \pmod{7}$, es decir si $r_7(a) = 3$, entonces $r_7(a^3) = 6$.

4.4 Sistemas de numeración.

El sistema de numeración que utilizamos desde que –según parece– Fibonacci lo introdujo en el mundo occidental, es el sistema decimal indo-arábigo, que es un sistema que funciona por posiciones de los dígitos, donde otra importancia del número 0 radica en que indica que hay una posición vacía.

Así, cuando escribimos el número seis mil setescientos nueve, 6709, nos referimos al número compuesto por 6 unidades de 1000 más 7 unidades de 100 más 0 unidades de 10 más 9 unidades (de 1), o sea al número

$$6709 = 6 \cdot 10^3 + 7 \cdot 10^2 + 0 \cdot 10 + 9.$$

El número natural $a = r_n r_{n-1} \dots r_1 r_0$ (donde $0 \leq r_i < 10$ para $0 \leq i \leq n$ y $r_n \neq 0$) simboliza entonces el número

$$r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \cdots + r_1 \cdot 10 + r_0.$$

Las exigencias de un buen sistema de numeración es que cuando vemos un número queremos poder saber en forma bien determinada de qué número estamos hablando, además de requerir que todo número tenga un único desarrollo que le corresponda. Esto se logra con la condición impuesta sobre los dígitos ($0 \leq r_i < 10, 0 \leq i \leq n$): para que un número esté bien determinado, los dígitos tienen que estar entre 0 y 9, ya que el lugar de un dígito en el número determina a qué potencia de 10 corresponde (si uno admitiera por ejemplo el 11 como un dígito, el número 111: ¿correspondería al número $111 = 1 \cdot 10^2 + 1 \cdot 10 + 1$ o al $21 = 1 \cdot 10 + 11 \cdot 1$?, y si uno admitiera el 11 pero con otro símbolo para evitar confusiones como la de arriba, por ejemplo B, el número 11 tendría dos escrituras distintas, una como 11 y la otra como B).

Matemáticamente no hay nada que haga prevalecer el número 10 como elección para la base de numeración: uno puede fijar cualquier número natural $d \geq 2$ como base del sistema de numeración. Para la buena determinación y la unicidad, lo que se tiene que pedir ahora es que los "dígitos", o mejor dicho símbolos, estén entre 0 y $d-1$. Esto se justifica también en la vida real, por ejemplo las computadoras trabajan naturalmente en base 2, o sea con los símbolos, que se llaman *bits*, 0 y 1, ya que esto se corresponde con el paso o no de electricidad.

Teorema 4.4.1. (Desarrollo en base d.)

Sea $d \in \mathbb{N}$ con $d \geq 2$. Todo número $a \in \mathbb{N}_0$ admite *un desarrollo en base d de la forma*

$$a = r_n \cdot d^n + r_{n-1} \cdot d^{n-1} + \cdots + r_1 \cdot d + r_0,$$

con $0 \leq r_i < d$ *para* $0 \leq i \leq n$ *y* $r_n \neq 0$ *si* $a \neq 0$.

Además dicho desarrollo, con las exigencias $0 \leq r_i < d$ *impuestas para los símbolos, es* único.

Se nota $a = (r_n \dots r_0)_d$.

Observación 4.4.2. En el caso de desarrollo en base 10, $(a)_{10}$ se nota simplemente a, en la forma que estamos acostumbrados.

Ejemplo:

$$6709 = (6709)_{10} = (25363)_7 = (1101000110101)_2 = (203314)_5 = (1A35)_{16}$$

(En base 16 los símbolos $10, 11, 12, 13, 14$ y 15 se reemplazan respectivamente por A, B, C, D, E y F para evitar confusiones.) Se obtiene el desarrollo realizando divisiones sucesivas. Por ejemplo para obtener el desarrollo en base 7 de 6709, se hace

$$\begin{aligned} 6709 &= 958 \cdot 7 + 3 \\ &= (136 \cdot 7 + 6) \cdot 7 + 3 \\ &= \big((19 \cdot 7 + 3) \cdot 7 + 6\big) \cdot 7 + 3 \\ &= \Big(\big((2 \cdot 7 + 5) \cdot 7 + 3\big) \cdot 7 + 6\Big) \cdot 7 + 3 \\ &= 2 \cdot 7^4 + 5 \cdot 7^3 + 3 \cdot 7^2 + 6 \cdot 7 + 3, \end{aligned}$$

y así, $6789 = (25363)_7$. Y para obtener sudesarrollo en base 16 se hace

$$\begin{aligned} 6709 &= 419 \cdot 16 + 5 \\ &= (26 \cdot 16 + 3) \cdot 16 + 5 \\ &= \big((1 \cdot 16 + 10) \cdot 16 + 3\big) \cdot 16 + 5 \\ &= 1 \cdot 16^3 + 10 \cdot 16^2 + 3 \cdot 16 + 5, \end{aligned}$$

y así, $6789 = (1A35)_{16}$ ya que el símbolo A representa el 10.

Demostración. Existencia del desarrollo en base d:

La idea intuitiva es ir dividiendo iteradamente el número a y los sucesivos cocientes por d. Para formalizar la prueba se puede hacer por induccción en $a \in \mathbb{N}_0$:

- Para $a = 0$, se tiene $0 = (0)_d$, es decir estamos en el único caso en que todos los dígitos son cero.
- $a \geq 1$:

La hipótesis inductiva es que todo número natural o cero menor que a admite un desarrollo en base d. Queremos probar que entonces a admite también un desarrollo en base d.

Usando el algoritmo de división, dividimos a por d, y obtenemos un cociente k que satisface $0 \leq k < a$ y un resto r_0 que satisface $0 \leq r_0 < d$: Por hipótesis inductiva, al ser $0 \leq k < a$, k admite un desarrollo en base d que notamos por conveniencia en la forma:

$$k = r_n \cdot d^{n-1} + \cdots + r_2 \cdot d + r_1 \quad \text{con } 0 \leq r_n, \ldots, r_1 < d.$$

Entonces

$$\begin{aligned} a &= k \cdot d + r_0 \\ &= (r_n \cdot d^{n-1} + \cdots + r_2 \cdot d + r_1) \cdot d + r_0 \\ &= r_n \cdot d^n + \cdots + r_1 \cdot d + r_0 \end{aligned}$$

donde $0 \leq r_i < d$ para $0 \leq i \leq n$ como se quiere.

Así, todo $a \in \mathbb{N}$ admite un desarrollo en base d.

Unicidad: Es una consecuencia de la unicidad del resto y del cociente en el algoritmo de división: r_0 es el resto de la división de a por d y por lo tanto es único, r_1 es el resto de la división de $(a - r_0)/d$ por d y es único también, etc... Como antes, podemos formalizar esto por inducción en $a \in \mathbb{N}_0$.

- Para $a = 0$, el único desarrollo es claramente $0 = (0)_d$.
- Para $a \geq 1$, supongamos que

  $$a = r_n \cdot d^n + \cdots + r_1 \cdot d + r_0 = s_m \cdot d^m + \cdots + s_1 \cdot d + s_0$$

  con $0 \leq r_i, s_j < d$ para $0 \leq i \leq n, 0 \leq j \leq m$ y $r_n \neq 0$, $s_m \neq 0$. Ahora bien, está claro que $r_d(a) = r_0 = s_0$, y además, el cociente de dividir a por d (que es único) es

  $$k = r_n \cdot d^{n-1} + \cdots + r_1 = s_m \cdot d^{m-1} + \cdots + s_1.$$

  Por hipótesis inductiva, el desarrollo en base d del cociente k es único, luego $n = m$ y $r_i = s_i$, $1 \leq i \leq n$.

Así concluimos que para todo $a \in \mathbb{N}_0$, el desarrollo en base d de a es único. □

Algoritmo iterativo para calcular el desarrollo en base $d > 0$ de un número $a \in \mathbb{N}_0$.

- Si $a = 0$, dar como respuesta $s = (0)_d$.
- Si $a > 0$:
  - Comenzar con $b = a$, $s = (\ )_d$.
  - Mientras que $b \neq 0$:
    - Calcular el cociente k y el resto r de la división de b por d.
    - Agregar r como la cifra de más a la izquierda en s.
    - Reemplazar $b \leftarrow k$.
  - Dar como respuesta s.

Nuevamente este procedimiento tiene un carácter intrínsecamente recursivo, ya que si se tiene $a = k \cdot d + r$ con $0 \leq r < d$ y se obtiene el desarrollo en base d de k: $k = (r_n \dots r_0)_d$, entonces el desarrollo en base d de a es

$$a = (r_n \dots r_0\, r)_d.$$

Un posible algoritmo para calcular el desarrollo en base d de a podría ser entonces (salvo errores de sintáxis):

Algoritmo recursivo en Haskell para calcular el desarrollo en base $d > 0$ de un número $a \in \mathbb{N}_0$.

```
des :: Integer → Integer → [Integer]
des 0 d = [0]
des a d = des (div a d) d ++ [mod a d]
```

Observación 4.4.3.

- ¿Cómo se escribe el número d^n en base d? La respuesta es

$$d^n = (1\ \underbrace{0 \dots 0}_{n})_d,$$

pues $d^n = 1 \cdot d^n + 0 \cdot d^{n-1} + \dots + 0 \cdot d^1 + 0 \cdot d^0$. Notar que d^n ocupa $n+1$ símbolos en base d, o sea tiene *tamaño* $n+1$ en base d, y es el número más chico que se puede escribir en base d usando $n+1$ símbolos (o sea de tamaño $n+1$).

- ¿Y cuál es el número más grande de tamaño n en base d, y cuál es su desarrollo? Claramente es el número $d^n - 1$ ya que d^n es el número

más chico de tamaño $n+1$ en base d. También se puede pensar que tiene que ser el número

$$\sum_{k=0}^{n-1}(d-1)\cdot d^k$$

pues se pone el máximo posible, $d-1$, para cada símbolo (y ese número coincide con d^n-1 por la serie geométrica...), o sea

$$d^n-1=(\underbrace{d-1\ \dots\ d-1}_{n})_d.$$

- ¿Cuántos números se pueden escribir usando a lo sumo n símbolos en base d? Son todos los números a con $0\le a\le d^n-1$, y por lo tanto son d^n. Todos se escriben en la forma

$$a=(\underbrace{r_{n-1}\ \dots\ r_0}_{n})_d \quad \text{para } 0\le r_i\le d-1.$$

- ¿Cuál es el tamaño en base d de un número $a\in\mathbb{N}$? (Es decir ¿cuántos símbolos son necesarios para escribir $a=(r_n\dots r_0)_d$ en base d?)

  La respuesta es $[\log_d(a)]+1$, donde $[\ ]$ nota la *parte entera*, o sea para un número real positivo, el número natural (o cero) más grande que es menor o igual que el número, pues por los incisos anteriores, si a requiere exactamente n símbolos, es que

$$d^{n-1}\le a<d^n,$$

  es decir $n-1\le\log_d(a)<n$, lo que implica que $[\log_d(a)]=n-1$, y por lo tanto $n=[\log_d(a)]+1$.

<u>Notas:</u>

- En Computación se utiliza, además del sistema binario, el sistema hexadecimal, o en base 16, que permite expresar cualquier número natural a partir de los símbolos siguientes

$$\{0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F\}.$$

  En esa base, como explicamos más arriba, el símbolo A representa el número 10 en base diez, es decir $10=(A)_{16}$. Análogamente, $11=(B)_{16}$, $12=(C)_{16}$, $13=(D)_{16}$, $14=(E)_{16}$ y $15=(F)_{16}$. Para escribir el 16 en base 16, necesitamos dos símbolos: $16=(10)_{16}$. Pero por lo visto arriba, usando solamente dos símbolos se pueden escribir $16^2=2^8$ números en base 16, lo cual es muy económico

en términos computacionales. A raíz de eso, se suele utilizar el *byte*, correspondiente a 8 bits, o sea en almacenamiento a 2 símbolos en base hexadecimal, como unidad de memoria. Por ejemplo $(11111111)_2 = (FF)_{16}$.

- Cuando introdujimos las torres de Hanoi nos preguntamos si era más económico para calcular el término a_n conocer la sucesión $(a_n)_{n\in\mathbb{N}}$ como $a_1 = 1,\ a_{n+1} = 2a_n + 1,\ \forall\, n \in \mathbb{N}$, o como $a_n = 2^n - 1,\ \forall\, n \in \mathbb{N}$.

  Esto es un caso particular del problema de cuántas operaciones son necesarias para calcular a^k, con $k \in \mathbb{N}$. Usando el algoritmo que se conoce como "dividir y conquistar", la respuesta está en calcular el desarrollo binario del exponente $k = (r_{n-1} \dots r_0)_2$.

  Por ejemplo si se quiere calcular a^{16} es más rápido hacer el cálculo

  $$a \to a \cdot a = a^2 \to a^2 \cdot a^2 = a^{2^2} = a^4 \to a^4 \cdot a^4 = a^{2^2 \cdot 2} = a^{2^3} = a^8$$
  $$\to a^8 \cdot a^8 = a^{2^3 \cdot 2} = a^{2^4} = a^{16}$$

  que requiere hacer $4 = \log_2(16)$ productos que hacer ingenuamente

  $$a \to a \cdot a = a^2 \to a \cdot a^2 = a^3 \to a \cdot a^3 = a^4 \to \cdots \to a \cdot a^{15} = a^{16}$$

  que requiere 15 productos. Ahora si se quiere calcular a^{22} el algoritmo "ingenuo" requeriría 21 productos mientras que como arriba, haciendo solo 4 productos, se calcula toda la secuencia

  $$a,\ a^2,\ a^{2^2},\ a^{2^3},\ a^{2^4}$$

  y ahora como $22 = (10110)_2$, es decir $22 = 2^4 + 2^2 + 2^1$, se obtiene

  $$a^{22} = a^{2^4 + 2^2 + 2^1} = a^{2^4} \cdot a^{2^2} \cdot a^{2^1},$$

  o sea se necesitan realizar 2 productos más para obtener a^{22}.

  Este argumento se puede repetir en general: si $k = r_{n-1}2^{n-1} + \cdots + r_0 2^0$ (donde n es la longitud de k en base 2, o sea del orden de $\log_2(k)$), entonces

  $$\begin{aligned} a^k &= a^{r_{n-1}2^{n-1} + r_{n-2}2^{n-2} + \cdots + r_1 2^1 + r_0 2^0} \\ &= a^{2^{n-1} r_{n-1}} \cdot a^{2^{n-2} r_{n-2}} \cdots a^{2^1 r_1} \cdot a^{2^0 r_0}, \end{aligned}$$

  donde observemos que cada r_i es o bien 1 o bien 0. Luego para obtener a^k se puede calcular recursivamente la secuencia de potencias

  $$a \to a^{2^1} \to a^{2^2} \to \cdots \to a^{2^{n-1}}$$

  haciendo $n-1$ productos, y luego multiplicar entre sí todas aquellas potencias a^{2^i} que satifacen que $r_i = 1$, que son a lo sumo n (este segundo paso involucra por lo tanto hacer $\leq n-1$ productos). En total hay que hacer $\leq 2(n-1)$ cuentas, o sea del orden de $2\log_2 k$ cuentas, mucho mejor que hacer $k-1$ cuentas si se multiplica recursivamente $a, a^2 = a \cdot a, a^3 = a^2 \cdot a$, etc.

4.4.1 Criterios de divisibilidad.

¡No son magia! Cada criterio de divisibilidad tiene su explicación. Lo ejemplificamos acá con dos de ellos.

Sea $a = \pm\, r_n r_{n-1} \cdots r_1 r_0$ el desarrollo decimal de a.

- Probemos el conocido criterio de divisibilidad por 3:

$$3 \mid a \iff 3 \mid r_n + r_{n-1} + \cdots + r_1 + r_0.$$

Como $10 \equiv 1 \pmod 3$ entonces $10^i \equiv 1 \pmod 3$, para todo $i \in \mathbb{N}_0$. Luego

$$a = r_n{\cdot}10^n + r_{n-1}{\cdot}10^{n-1} + \cdots + r_1{\cdot}10 + r_0 \equiv r_n + r_{n-1} + \cdots + r_1 + r_0 \pmod 3.$$

En particular

$$\begin{aligned} 3 \mid a &\iff a \equiv 0 \pmod 3 \\ &\iff r_n + r_{n-1} + \cdots + r_1 + r_0 \equiv 0 \pmod 3 \\ &\iff 3 \mid r_n + r_{n-1} + \cdots + r_1 + r_0. \end{aligned}$$

- Criterio de divisibilidad por 11:

$$11 \mid a \iff 11 \mid (-1)^n r_n + (-1)^{n-1} r_{n-1} + \cdots - r_1 + r_0.$$

Observemos que $r_{11}(10) = 10 \;\Rightarrow\; 10 \equiv 10 \pmod{11}$: esto no ayuda mucho en principio. Pero como ya utilizamos más arriba, también vale $10 \equiv -1 \pmod{11}$, y así,

$$10^i \equiv (-1)^i \pmod{11}$$

Luego,

$$\begin{aligned} a &= r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \cdots + r_1 \cdot 10 + r_0 \\ &\equiv (-1)^n r_n + (-1)^{n-1} r_{n-1} + \cdots - r_1 + r_0 \pmod{11}. \end{aligned}$$

En particular

$$\begin{aligned} 11 \mid a &\iff a \equiv 0 \pmod{11} \\ &\iff (-1)^n r_n + (-1)^{n-1} r_{n-1} + \cdots - r_1 + r_0 \pmod{11} \\ &\iff 11 \mid (-1)^n r_n + (-1)^{n-1} r_{n-1} + \cdots - r_1 + r_0. \end{aligned}$$

4.5 Máximo común divisor.

Definición 4.5.1. (Máximo común divisor.)

Sean $a, b \in \mathbb{Z}$, no ambos nulos. El *máximo común divisor* entre a y b, que se nota $(a : b)$, es el mayor de los divisores comunes de a y b. Es decir:

$$(a : b) \mid a,\ (a : b) \mid b \quad \text{y si} \quad d \mid a \text{ y } d \mid b, \text{ entonces } \ d \leq (a : b).$$

Claramente ese número *existe*, ya que la lista de divisores comunes es no vacía (1 es un divisor común) y finita (por ser al menos uno entre a y b no nulo), y es *único* (por ser el mayor de todos). Además es *positivo* por la misma razón.

Notaremos en lo que sigue con $\mathrm{DivCom}(\{a, b\})$ el conjunto de los divisores comunes de a y b y con $\mathrm{DivCom}_+(\{a, b\})$ el conjunto de los divisores comunes positivos, es decir:

$$\mathrm{DivCom}(\{a, b\}) = \{\, d \in \mathbb{Z} : d \mid a \text{ y } d \mid b \,\} \ = \ \mathrm{Div}(a) \cap \mathrm{Div}(b)$$
$$\mathrm{DivCom}_+(\{a, b\}) = \{\, d \in \mathbb{N} : d \mid a \text{ y } d \mid b \,\} \ = \ \mathrm{Div}_+(a) \cap \mathrm{Div}_+(b).$$

Luego, el máximo común divisor es el elemento más grande de cualquiera de esos dos conjuntos.

Ejemplos:

- $(12 : 18) = 6$, pues $\mathrm{Div}_+(12) = \{1, 2, 3, 4, 6, 12\}$, $\mathrm{Div}_+(18) = \{1, 2, 3, 6, 9, 18\}$, y por lo tanto $\mathrm{DivCom}_+(\{12, 18\}) = \{1, 2, 3, 6\}$.
- $(12 : -35) = 1$ ya que $\mathrm{Div}_+(-35) = \{1, 5, 7, 35\}$, y por lo tanto $\mathrm{DivCom}_+(\{12, -35\}) = \{1\}$.
- $(a : b) = (b : a)$, $\forall\, a, b \in \mathbb{Z}$ no ambos nulos.
- $(a : b) = (-a : b) = (a : -b) = (-a : -b) = (|a| : |b|)$, $\forall\, a, b \in \mathbb{Z}$ no ambos nulos.
- $(a : 1) = 1$, $\forall\, a \in \mathbb{Z}$.
- $(a : 0) = |a|$, $\forall\, a \in \mathbb{Z} - \{0\}$.
- Para todo $a, b \in \mathbb{Z}$ con $b \neq 0$, se tiene: $b \mid a \Rightarrow (a : b) = |b|$.
- Probar que los únicos valores posibles para $(a^2 + 8 : a + 1)$, $\forall\, a \in \mathbb{Z}$, son 1, 3 o 9, y mostrar con ejemplos que se realizan todos.

Para ello miramos quiénes son los posibles divisores comunes de a^2+8 y $a+1$:

$$\left\{\begin{array}{l} d \mid a^2+8 \\ d \mid a+1 \end{array}\right. \implies \left\{\begin{array}{l} d \mid a^2+8 \\ d \mid (a-1)(a+1) = a^2-1 \end{array}\right. \implies d \mid 9,$$

restando. Por lo tanto en principio los posibles valores para el máximo común divisor son únicamente los divisores positivos de 9: 1, 3 o 9. Efectivamente, para $a = 0$ se consigue $(a^2+8 : a+1) = (8:1) = 1$, para $a = 2$ se consigue $(a^2+8 : a+1) = (12:3) = 3$ y para $a = -1$ se consigue $(a^2+8 : a+1) = (9:0) = 9$.

4.5.1 Algoritmo de Euclides.

Existe un algoritmo para calcular el máximo común divisor entre dos números, que no depende de calcular sus divisores. Este algoritmo fue introducido o recopilado por Euclides ($\sim$325–$\sim$265 AC) en "Los Elementos", y se lo llama directamente *Algoritmo de Euclides.*

Proposición 4.5.2. *Sean $a, b \in \mathbb{Z}$ no ambos nulos, y sea $k \in \mathbb{Z}$, entonces:*

$$\begin{aligned} &\mathrm{DivCom}(\{a,b\}) = \mathrm{DivCom}(\{b, a-k\cdot b\}), \text{ y} \\ &\mathrm{DivCom}_+(\{a,b\}) = \mathrm{DivCom}_+(\{b, a-k\cdot b\}). \end{aligned}$$

En particular, para todo $k \in \mathbb{Z}$, $\quad (a:b) = (b : a-k\cdot b)$,
y dados $a, b, c \in \mathbb{Z}$ con $b \neq 0$,

$$a \equiv c \pmod{b} \quad \implies \quad (a:b) = (b:c).$$

Aplicando esto a $a \equiv r_b(a) \pmod{b}$, se obtiene que $(a:b) = (b : r_b(a))$.

Demostración. Para probar que $(a:b) = (b : a-k\cdot b)$, alcanza con probar la primera igualdad, la de los conjuntos DivCom, pues entonces el máximo de los divisores comunes será el mismo.

Sabemos que $d \mid a$, $d \mid b \Rightarrow d \mid a-k\cdot b$, y también $d \mid b$, $d \mid a-k\cdot b \Rightarrow d \mid a$. Por lo tanto

$$\begin{aligned} d \in \mathrm{DivCom}(\{a,b\}) &\iff d \mid a \text{ y } d \mid b \\ &\iff d \mid a-k\cdot b \text{ y } d \mid b \\ &\iff d \in \mathrm{DivCom}(\{b, a-k\cdot b\}). \end{aligned}$$

Ahora bien,

$$a \equiv c \pmod{b} \Leftrightarrow b \mid a-c \Leftrightarrow \exists\, k \in \mathbb{Z} : a-c = k\cdot b \Leftrightarrow \exists\, k \in \mathbb{Z} : c = a-k\cdot b$$

y por lo tanto, $(a:b) = (b : a-k\cdot b) = (b:c)$ como se quería probar. $\square$

Vamos a ejemplificar primero el funcionamiento del algoritmo de Euclides en un caso particular.

Ejemplo: Cálculo de $(120 : -84)$:

Como $(120 : -84) = (120 : 84)$, calculamos este último para simplificar las divisiones (esto no es esencial para el algoritmo). Se tiene

$$\begin{array}{rcl@{\quad}c@{\quad}rcl} 120 & = & 1 \cdot 84 + 36 & \Longrightarrow & (120 : 84) & = & (84 : 36) \\ 84 & = & 2 \cdot 36 + 12 & \Longrightarrow & (84 : 36) & = & (36 : 12) \\ 36 & = & 3 \cdot 12 + \ 0 & \Longrightarrow & (36 : 12) & = & (12 : 0). \end{array}$$

Pero $(12 : 0) = 12$, luego $(120 : -84) = 12$ ya que

$$(120 : -84) = (120 : 84) = (84 : 36) = (36 : 12) = (12 : 0) = 12.$$

Enunciamos y demostramos ahora el *Algoritmo de Euclides* "en palabras".

Teorema 4.5.3. (Algoritmo de Euclides.)

Sean $a, b \in \mathbb{Z}$ no nulos. Existe $\ell \in \mathbb{N}_0$ tal que en una sucesión finita de $\ell + 1$ divisiones

$$\begin{array}{lcll} a & = & k_1 \cdot b + r_1 & con \quad 0 \leq r_1 < |b| \\ b & = & k_2 \cdot r_1 + r_2 & con \quad 0 \leq r_2 < r_1 \\ r_1 & = & k_3 \cdot r_2 + r_3 & con \quad 0 \leq r_3 < r_2 \\ \vdots & & & \\ r_{\ell-2} & = & k_\ell \cdot r_{\ell-1} + r_\ell & con \quad 0 \leq r_\ell < r_{\ell-1} \\ r_{\ell-1} & = & k_{\ell+1} \cdot r_\ell + r_{\ell+1} & con \quad 0 \leq r_{\ell+1} \leq r_\ell, \end{array}$$

se llega por primera vez al resto nulo $r_{\ell+1} = 0$. Entonces $(a : b) = r_\ell$, el último resto no nulo.

La sucesión de divisiones hasta llegar al último resto no nulo se suele llamar el *Esquema de Euclides extendido.*

Demostración. Siempre se llega en un número finito de pasos (acotado a simple vista por $|b|$) a un resto nulo ya que

$$|b| > r_1 > r_2 > r_3 > \cdots \geq 0,$$

y esta sucesión estrictamente decreciente de restos ≥ 0 no puede ser infinita. Cuando en el procedimiento se llega a un resto nulo, $r_{\ell+1} = 0$, se tiene

$$(a : b) = (b : r_1) = (r_1 : r_2) = \cdots = (r_{\ell-1} : r_\ell) = (r_\ell : 0) = r_\ell.$$

□

Observación 4.5.4. Si $a, b \in \mathbb{Z}$ son tales que $a = 0$ y $b \neq 0$, ya sabemos que $(a : b) = |b|$ (o si $a \neq 0$ y $b = 0$, entonces $(a : b) = |a|$). Por lo tanto el Algoritmo de Euclides permite calcular el máximo común divisor de cualquier par de números enteros no ambos nulos.

Algoritmo de Euclides iterativo para calcular el máximo común divisor entre dos enteros no nulos a y b.

- Comenzar con $r_1 = a$, $r_2 = b$.
- Mientras que $r_2 \neq 0$:
  - Calcular el resto r de la división de r_1 por r_2.
  - Reemplazar
    - $r_1 \leftarrow r_2$
    - $r_2 \leftarrow r$
- Dar como respuesta r_1.

Pero el Algoritmo de Euclides tiene un naturaleza intrínsecamente recursiva, ya que si $a = k \cdot b + r$ entonces $(a : b) = (b : r)$, así que es otro ejemplo perfecto para Haskell!

Algoritmo de Euclides recursivo en Haskell.

```
mcd :: Integer → Integer → Integer
mcd a b | abs b > abs a = mcd b a
mcd a 0 = abs a
mcd a b = mcd b (mod a b)
```

Mencionamos antes que este algoritmo es el más eficiente para calcular el máximo común divisor entre dos números. Para ser más precisos, entre números grandes, o sea con suficientes dígitos para que calcular su escritura como potencias de primos sea difícil (como detallaremos más adelante): Calcular el máximo común divisor nunca requiere más divisiones que cinco veces la cantidad de dígitos que tienen los números.

No dejen de hacer ejemplos en el taller para los cuales se note la diferencia entre los tiempos de cálculo aplicando los dos algoritmos: factorización en primos y el algoritmo de Euclides.

Una aplicación no trivial del Algoritmo de Euclides:

Sean $a \in \mathbb{N}$, $a \neq 1$, y $m, n \in \mathbb{N}$. Entonces

$$(a^m - 1 : a^n - 1) = a^{(m:n)} - 1.$$

Demostración. Vamos a probar que en efecto $a^{(m:n)}-1$ es el último resto no nulo al realizar el algoritmo de Euclides para calcular el máximo común divisor.

Recordemos que vimos en los primeros ejemplos de divisibilidad la afirmación

$$n \mid m \;\Rightarrow\; a^n-1 \mid a^m-1.$$

En el caso general, si $m = k\,n + r$ con $0 \le r < n$, entonces

$$a^m-1 = a^{k\,n+r}-1 = a^r(a^{k\,n}-1)+(a^r-1) = k'(a^n-1)+(a^r-1),$$

dado que $n \mid k\,n \;\Rightarrow\; a^n-1 \mid a^{k\,n}-1$. Además, como $0 \le a^r-1 < a^n-1$ por ser $0 \le r < n$ y $a \in \mathbb{N}$, $a \neq 0$, se tiene que a^r-1 es el resto de dividir a a^m-1 por a^n-1. Por lo tanto, aplicando la Proposición 4.5.2, se obtiene

$$(a^m-1 : a^n-1) = (a^n-1 : a^{r_n(m)}-1).$$

Así, si se tiene el siguiente esquema de Euclides extendido para m y n,

$$\begin{cases} m = k_1 \cdot n + r_1 \quad \text{con} \quad r_1 \neq 0 \\ n = k_2 \cdot r_1 + r_2 \quad \text{con} \quad r_2 \neq 0 \\ r_1 = k_3 \cdot r_2 + r_3 \quad \text{con} \quad r_3 \neq 0 \\ \vdots \\ r_{\ell-2} = k_\ell \cdot r_{\ell-1} + r_\ell \quad \text{con} \quad r_\ell \neq 0 \\ r_{\ell-1} = k_{\ell+1} \cdot r_\ell + r_{\ell+1} \quad \text{con} \quad r_{\ell+1} = 0 \end{cases},$$

se deduce que

$$\begin{cases} a^m-1 = k'_1 \cdot (a^n-1) + (a^{r_1}-1) \\ a^n-1 = k'_2 \cdot (a^{r_1}-1) + (a^{r_2}-1) \\ a^{r_1}-1 = k'_3 \cdot (a^{r_2}-1) + (a^{r_3}-1) \\ \vdots \\ a^{r_{\ell-2}}-1 = k'_\ell \cdot (a^{r_{\ell-1}}-1) + (a^{r_\ell}-1) \\ a^{r_{\ell-1}}-1 = k'_{\ell+1} \cdot (a^{r_\ell}-1) + (a^{r_{\ell+1}}-1) \end{cases}$$

donde como $r_i \neq 0$ para $1 \le i \le \ell$, entonces $a^{r_i}-1 \neq 0$ pues $a \in \mathbb{N}$, $a \neq 1$, y $a^{r_{\ell+1}}-1 = a^0-1 = 0$. Así el último resto no nulo es $a^{r_\ell}-1 = a^{(m:n)}-1$, ya que $r_\ell = (m:n)$, por el Algoritmo de Euclides. □

Una consecuencia crucial del Algoritmo de Euclides para la teoría de los números enteros es que el máximo común divisor entre dos números siempre se puede escibir como una *combinación entera de esos dos números* (y de hecho es el número positivo más chico con esa propiedad). Este hecho que veremos ahora tiene consecuencias importantísimas y sorprendentes que iremos viendo a lo largo de este capítulo.

Teorema 4.5.5. (Mcd y combinación entera.)

Sean $a, b \in \mathbb{Z}$, *no ambos nulos. Entonces existen* $s, t \in \mathbb{Z}$ *tales que*

$$(a : b) = s \cdot a + t \cdot b.$$

Este resultado se demuesta con el *Esquema de Euclides extendido*, mirandolo de atrás para adelante. Miremos cómo se pueden obtener en forma sistemática coeficientes enteros s y t, en el caso particular del ejemplo que calculamos antes:

Ejemplo: $(120 : -84) = 12$:

Mirando las dos divisiones que permitieron obtener a 12 como último resto no nulo, pero al revés, se tiene

$$\begin{array}{rclcrcl} 84 &=& 2 \cdot 36 + 12 & \Longrightarrow & 12 &=& 84 - 2 \cdot 36 \\ 120 &=& 1 \cdot 84 + 36 & \Longrightarrow & 12 &=& 84 - 2 \cdot (120 - 1 \cdot 84) \\ & & & & &=& 3 \cdot 84 - 2 \cdot 120. \end{array}$$

Por lo tanto, $12 = -2 \cdot 120 + 3 \cdot 84 = -2 \cdot 120 + (-3) \cdot (-84)$. Aquí, $s = -2$ y $t = -3$ sirven.

Demostración. Se miran de atrás para adelante las sucesivas divisiones hasta la que da al máximo común divisor como último resto no nulo, y, poniendo en factor común los sucesivos divisores y restos y reagrupando, se obtiene una escritura entera de $(a : b)$ como combinación entera de a y b. (Luego, si habíamos —para simplificar las divisiones— cambiado los signos de los a y b originales, se modifican los signos para escribir $(a : b)$ como combinación entera de los a y b originales.) Si $r_\ell = (a : b)$,

$$\begin{array}{rclcrcl} r_{\ell-2} &=& k_\ell r_{\ell-1} + r_\ell & \Longrightarrow & r_\ell &=& r_{\ell-2} - k_\ell r_{\ell-1} \\ r_{\ell-3} &=& k_{\ell-1} r_{\ell-2} + r_{\ell-1} & \Longrightarrow & r_\ell &=& r_{\ell-2} - k_\ell (r_{\ell-3} - k_{\ell-1} r_{\ell-2}) \\ & & & & &=& (1 + k_\ell k_{\ell-2}) r_{\ell-2} - k_\ell r_{\ell-3} \\ \vdots & & & & & & \\ r_1 &=& k_3 r_2 + r_3 & \Longrightarrow & r_\ell &=& *\, r_1 + *'\, r_2 \\ b &=& k_2 r_1 + r_2 & \Longrightarrow & r_\ell &=& *\, r_1 + *'\, (b - k_2 r_1) \\ & & & & &=& (*\, - k_2\, *')\, r_1 + *'\, b \\ a &=& k_1 b + r_1 & \Longrightarrow & r_\ell &=& (*\, - k_2\, *')(a - k_1 b) + *'\, b \\ & & & & &=& s\, a + t\, b, \end{array}$$

donde las estrellitas simbolizan los números que se obtuvieron como coeficientes al llegar a ese paso. Así, $(a : b) = r_\ell = s\, a + t\, b$ donde claramente $s, t \in \mathbb{Z}$ ya que son obtenidos sumando y multiplicando enteros. □

Observemos para escribir el algoritmo que si definimos $r_{-1} = a$, $r_0 = b$, y si en general $r_{i-2} = k_i\, r_{i-1} + r_i$, y logramos escribir $r_{i-2} = s_{i-2} a + t_{i-2} b$ y

$r_{i-1} = s_{i-1}a + t_{i-1}b$ comenzando desde $r_{-1} = 1 \cdot a + 0 \cdot b$, o sea $s_{-1} = 1$, $t_{-1} = 0$, y $r_0 = 0 \cdot a + 1 \cdot b$, o sea $s_0 = 0$, $t_0 = 1$, entonces tenemos la recurrencia

$$\begin{aligned} r_i &= r_{i-2} - k_i\, r_{i-1} = s_{i-2}a + t_{i-2}b - k_i(s_{i-1}a + t_{i-1}b) \\ &= (s_{i-2} - k_i\, s_{i-1})a + (t_{i-2} - k_i\, t_{i-1})b. \end{aligned}$$

Es decir $r_i = s_i\, a + t_i\, b$ donde

$$s_i = s_{i-2} - k_i\, s_{i-1} \quad \text{y} \quad t_i = t_{i-2} - k_i\, t_{i-1}.$$

Se recupera la escritura de $(a : b) = r_\ell = s_\ell\, a + t_\ell\, b$ donde r_ℓ es el último resto no nulo.

Esquema extendido de Euclides iterativo para escribir el máximo común divisor $(a : b)$ como combinación entera de a y b.

- Comenzar con $r_1 = a$, $r_2 = b$, $s_1 = 1$, $t_1 = 0$, $s_2 = 0$, $t_2 = 1$.
- Mientras que $r_2 \neq 0$:
  - Calcular el cociente k y el resto r de la división de r_1 por r_2.
  - Calcular $s = s_1 - k * s_2$ y $t = t_1 - k * t_2$
  - Reemplazar
    - $r_1 \leftarrow r_2$
    - $r_2 \leftarrow r$
    - $s_1 \leftarrow s_2$, $t_1 \leftarrow t_2$
    - $s_2 \leftarrow s$, $t_2 \leftarrow t$
- Dar como respuesta r_1, s_1, t_1 (que satisfacen $(a : b) = r_1 = s_1\, a + t_1\, b$).

Este algoritmo también es intrínsecamente recursivo, ya que si $a = k \cdot b + r$ y $(b : r) = s \cdot b + t \cdot r$, entonces,

$$(a : b) = (b : r) = s \cdot b + t \cdot r = s \cdot b + t \cdot (a - k \cdot b) = t \cdot a + (s - t \cdot k) \cdot b.$$

Así:

Esquema extendido de Euclides recursivo en Haskell: Dados a y b no negativos y no ambos nulos, devuelve (d', s', t') tales que $d' = (a : b) =$

$s' \cdot a + t' \cdot b$.

```
mcdExt :: Integer → Integer → (Integer , Integer , Integer)
mcdExt a b | b > a = mcdExt b a
mcdExt a 0 = (a, 1, 0)
mcdExt a b = (d, t, s − t ∗ k)
        where (k, r) = (div a b, mod a b)
              (d, s, t) = mcdExt b r
```

En realidad, se pueden caracterizar fácilmente todos los números enteros que son combinación entera de a y b:

Observación 4.5.6. (Combinaciones enteras de a y b.)

Sean $a, b \in \mathbb{Z}$ no ambos nulos, y $c \in \mathbb{Z}$.

$$c = s' \cdot a + t' \cdot b \text{ para } s', t' \in \mathbb{Z} \iff (a : b) \mid c.$$

Demostración.

- ($\Rightarrow$) Dado que $(a : b) \mid a$ y $(a : b) \mid b$, se tiene $(a : b) \mid s'a + t'b$, luego $(a : b) \mid c$.
- ($\Leftarrow$) Si $(a : b) \mid c$, entonces $c = k \cdot (a : b)$. Como sabemos que existen $s, t \in \mathbb{Z}$ tales que $(a : b) = s \cdot a + t \cdot b$, se tiene

$$c = k \cdot (a : b) = k(s \cdot a + t \cdot b) = (k \cdot s)a + (k \cdot t)b.$$

Luego $s' = k \cdot s$ y $t' = k \cdot t$.

□

La observación anterior nos dice que el máximo común divisor $(a : b)$ es el número *natural más chico* que se puede escribir como combinación entera de a y b y que todas las demás combinaciones enteras de a y b son divisibles por él.

El Teorema 4.5.5 tiene otra consecuencia importantísima que no es obvia a primera vista: el máximo común divisor no solo es el más grande de los divisores comunes sino que también es divisible por todos los divisores comunes.

Proposición 4.5.7. (Mcd y divisores comunes.)

Sean $a, b \in \mathbb{Z}$, no ambos nulos y sea $d \in \mathbb{Z}$, con $d \neq 0$. Entonces

$$d \mid a \text{ y } d \mid b \iff d \mid (a : b).$$

Demostración.

- ($\Rightarrow$): Esta es la implicación interesante y no trivial:

  Recordemos que existen $s, t \in \mathbb{Z}$ tales que $(a : b) = s \cdot a + t \cdot b$. Ahora, dado que por hipotesis, $c \mid a$ y $c \mid b$, se tiene que $c \mid s \cdot a + t \cdot b = (a : b)$.

- ($\Leftarrow$): Esta implicación es obvia por la transitividad de la divisibilidad.

□

Otra consecuencia útil del Teorema 4.5.5, de la Observación 4.5.6 y de la Proposición 4.5.7 es la siguiente:

Proposición 4.5.8. (Mcd de múltiplo común de dos números.)

Sean $a, b \in \mathbb{Z}$, *no ambos nulos, y sea* $k \in \mathbb{Z}$ *con* $k \neq 0$. *Entonces*

$$(k\,a : k\,b) = |k| \cdot (a : b).$$

Demostración. Sin pérdida de generalidad, podemos suponer $k > 0$.

Por un lado, aplicando la Proposición 4.5.7, se tiene

$$(a : b) \mid a \text{ y } (a : b) \mid b \implies k\,(a : b) \mid k\,a \text{ y } k\,(a : b) \mid k\,b \implies k\,(a : b) \mid (k\,a : k\,b).$$

Por otro lado, por el Teorema 4.5.5 y la Observación 4.5.6, se tiene

$$(a : b) = s\,a + t\,b \implies k\,(a : b) = s\,(k\,a) + t\,(k\,b) \implies (k\,a : k\,b) \mid k\,(a : b).$$

Como ambos términos son positivos, se concluye que son iguales. □

En realidad, los resultados que se obtuvieron permiten tres caracterizaciones equivalentes del máximo común divisor, que se enuncian a continuación. La primera corresponde a la Definición 4.5.1 del mcd y es la caracterización intuitiva, la segunda corresponde principalmente al Teorema 4.5.5 y la tercera a la Proposición 4.5.7. La segunda y la tercera son las operativas. Se deja la prueba a cargo del lector, mencionando simplemente que alcanza con probar (*1* $\Rightarrow$ *2*), (*2* $\Rightarrow$ *3*) y (*3* $\Rightarrow$ *1*), ya que por ejemplo para probar que (*2* $\Rightarrow$ *1*) se usa (*2* $\Rightarrow$ *3* $\Rightarrow$ *1*).

Teorema 4.5.9. (Equivalencias del mcd.)

Sean $a, b \in \mathbb{Z}$, *no ambos nulos, y sea* $d \in \mathbb{N}$. *Son equivalentes:*

1. $d \mid a,\ d \mid b$ *y si* $c \mid a$ *y* $c \mid b$, *entonces* $c \leq d$.
2. $d \mid a,\ d \mid b$ *y existen* $s, t \in \mathbb{Z}$ *tales que* $d = sa + tb$.
3. $d \mid a,\ d \mid b$ *y si* $c \mid a$ *y* $c \mid b$, *entonces* $c \mid d$.

Un número $d \in \mathbb{N}$ *que cumple cualquiera de esas 3 propiedades es el máximo común divisor* $(a : b)$.

4.5.2 Números coprimos.

Una atención especial merecen los pares de números cuyo máximo común divisor es igual a 1. Juegan un papel central en lo que sigue.

Definición 4.5.10. (Números coprimos.)

Se dice que $a, b \in \mathbb{Z}$ no ambos nulos son *coprimos* si y solo si $(a : b) = 1$, es decir si y solo si los únicos divisores comunes de a y b son ± 1.

En este texto, adoptamos la notación introducida por el matemático e informático Donald Knuth (quién de hecho es el creador del TeX (y LATeX), procesadores con los que escribimos textos matemáticos que lucen tan bonitos, en particular este texto), y escribimos $a \perp b$. O sea:

$$a \perp b \iff (a : b) = 1$$

Ejemplos:

- $103 \perp 98$ pero $12202 \not\perp 43554$.
- $a \perp 0 \Leftrightarrow a = \pm 1$
- Para todo $b \in \mathbb{Z}$, $\pm 1 \perp b$.
- Para $a, b \in \mathbb{Z}$ coprimos, los distintos valores que puede tomar $(2a+b : 3a-2b)$ son exactamente el 1 y el 7:
  - Investiguemos algunos valores de $(2a + b : 3a - 2b)$ con $a \perp b$: $a = 1, b = 0 : (2 : 3) = 1$; $a = 1, b = 1 : (3 : 1) = 1$; $a = 3, b = 1 : (7 : 7) = 7$.
    Luego, efectivamente los dos valores, 1 y 7, se obtienen. Probemos que son los únicos dos posibles.
  - Sea d un divisor común entre $2a + b$ y $3a - 2b$,

$$\begin{cases} d \mid 2a+b \\ d \mid 3a-2b \end{cases} \implies \begin{cases} d \mid 3(2a+b) \\ d \mid 2(3a-2b) \end{cases}$$
$$\implies \begin{cases} d \mid 6a+3b \\ d \mid 6a-4b \end{cases} \implies d \mid 7b.$$

    De la misma manera:

$$\begin{cases} d \mid 2a+b \\ d \mid 3a-2b \end{cases} \implies \begin{cases} d \mid 2(2a+b) \\ d \mid 3a-2b \end{cases}$$
$$\implies \begin{cases} d \mid 4a+2b \\ d \mid 3a-2b \end{cases} \implies d \mid 7a.$$

Luego $d \mid 7a$ y $d \mid 7b$. Aplicando las Proposiciones 4.5.7 y 4.5.8 y el hecho que $a \perp b$, se tiene

$$d \mid (7a : 7b) = 7(a : b) = 7 \implies d \mid 7.$$

Se concluye que el máximo común divisor, que es el mayor de estos d posibles, es o bien 1 o 7 como se quería probar (además efectivamente ya mostramos que había casos en que es 1 y casos en que es 7).

Recordemos que el máximo común divisor se puede escribir como combinación entera. Luego

Observación 4.5.11. (Coprimos y combinación entera.)

Sean $a, b \in \mathbb{Z}$ no ambos nulos. Entonces

$$a \perp b \iff \exists\, s, t \in \mathbb{Z} \;:\; 1 = s\,a + t\,b.$$

Demostración.

- $(\Rightarrow)$ es el hecho que el mcd 1 es combinación entera de los números.
- $(\Leftarrow)$ es por la Observación 4.5.6: $(a : b) \mid 1 \;\Rightarrow\; (a : b) = 1$.

□

La proposición que sigue trata de propiedades esenciales de divisibilidad cuando hay números coprimos de por medio. No se podrían demostrar estas propiedades si no se tuviera la Observación 4.5.11.

Proposición 4.5.12. (Propiedades esenciales de divisibilidad con coprimalidad.)

Sean $a, b, c, d \in \mathbb{Z}$ con $c \neq 0$ y $d \neq 0$. Entonces

1. $c \mid a,\ d \mid a$ *y* $c \perp d \implies c\,d \mid a$.
2. $d \mid a\,b$ *y* $d \perp a \implies d \mid b$.

Observemos que estas afirmaciones no son ciertas si no se piden las propiedades de coprimalidad. Por ejemplo $6 \mid 12$ y $4 \mid 12$ pero $24 \nmid 12$, y $6 \mid 2 \cdot 3 \not\Rightarrow 6 \mid 2$ o $6 \mid 3$. Por otro lado, las recíprocas siempre valen: $c\,d \mid a \;\Rightarrow\; c \mid a$ y $d \mid a$, y $d \mid b \;\Rightarrow\; d \mid a\,b$. Luego podemos reformular la Proposición 4.5.12 de la manera siguiente:

1. Sea $c \perp d$. Entonces $c \mid a, d \mid a \Leftrightarrow c\,d \mid a$.

2. Sea $d \perp a$. Entonces $d \mid a\,b \Leftrightarrow d \mid b$.

Demostración. 1. $c \perp d \;\Rightarrow\; 1 = s\,c + t\,d \;\Rightarrow\; a = s\,(c\,a) + t\,(d\,a)$, pero $d \mid a \;\Rightarrow\; c\,d \mid c\,a$ y $c \mid a \;\Rightarrow\; c\,d \mid d\,a$, luego $c\,d \mid s\,(c\,a) + t\,(d\,a) = a$.

2. $d \perp a \;\Rightarrow\; 1 = s\,d + t\,a$, luego $b = (s\,b)\,d + t\,(a\,b)$, pero $d \mid a\,b$, y $d \mid d$. Por lo tanto, $d \mid (s\,b)\,d + t\,(a\,b) = b$.

□

<u>*Ejemplo:*</u> Cálculo de los $a, b \in \mathbb{Z}$ coprimos tales que $\dfrac{2}{a} + \dfrac{a}{b}$ es entero.

$$\frac{2}{a} + \frac{a}{b} = \frac{2b + a^2}{ab} \in \mathbb{Z} \iff ab \mid 2b + a^2.$$

Pero al ser $a \perp b$, $ab \mid 2b + a^2 \Leftrightarrow a \mid 2b + a^2$ y $b \mid 2b + a^2$.

Pero, dado que $a \mid a^2$, $a \mid 2b + a^2 \Leftrightarrow a \mid 2b$, y, dado que $a \perp b$, $a \mid 2b \Leftrightarrow a \mid 2$. Es decir, $a \in \{\pm 1, \pm 2\}$.

De la misma forma, dado que $b \mid 2b$, $b \mid 2b + a^2 \Leftrightarrow b \mid a^2$, y, dado que $b \perp a^2$ (pues $a \perp b$), $b \mid a^2 \cdot 1 \Leftrightarrow b \mid 1$, o sea $b \in \{\pm 1\}$.

Se obtienen luego los 8 pares $a = \pm 1, b = \pm 1$ y $a = \pm 2, b = \pm 1$.

Otra consecuencia muy útil de la Proposición 4.5.11, ya que se trata siempre de reducirse a pares coprimos para poder aplicar proposiciones como la anterior, es la siguiente:

Proposición 4.5.13. ("Coprimizando")

Sean $a, b \in \mathbb{Z}$, no ambos nulos. Entonces

$$\frac{a}{(a : b)} \perp \frac{b}{(a : b)}.$$

Por lo tanto

$$a = (a : b)\,a' \quad y \quad b = (a : b)\,b'$$

donde los números enteros $a' = \dfrac{a}{(a : b)}$ y $b' = \dfrac{b}{(a : b)}$ son coprimos.

Demostración. Se sabe que $(a : b) = s\,a + t\,b$. Luego, dividiendo por $(a : b)$, se obtiene $1 = s\dfrac{a}{(a : b)} + t\dfrac{b}{(a : b)}$, es decir $\dfrac{a}{(a : b)}$ y $\dfrac{b}{(a : b)}$ son coprimos.

□

Ejemplos:

- Sean $a, b \in \mathbb{Z}$ no ambos nulos tales que $(a : b) = 6$. ¿Cuáles son los posibles valores de $(6a + 12b : 6\,a - 6\,b)$?

  Coprimizando, se tiene $a = 6\,a'$, $b = 6\,b'$ con $a' \perp b'$, luego

  $$\begin{aligned}(6a + 12b : 6a - 6b) &= (36a' + 72b : 36a' - 36b') \\ &= (36'(a' + 2b') : 36(a' - b')) \\ &= 36(a' + 2b : a' - b').\end{aligned}$$

  Para concluir falta averiguar quiénes son los posibles valores de $(a' + 2b' : a' - b')$ si $a' \perp b'$.

  Sea entonces d un divisor común:

  $$\begin{cases} d \mid a' + 2b' \\ d \mid a' - b' \end{cases} \implies d \mid 3b',$$

  $$\begin{cases} d \mid a' + 2b' \\ d \mid a' - b' \end{cases} \implies \begin{cases} d \mid a' + 2b' \\ d \mid 2a' - 2b' \end{cases} \implies d \mid 3a'.$$

  Obtuvimos $d \mid 3a'$ y $d \mid 3b'$. Luego $d \mid (3a' : 3b') = 3(a' : b') = 3$.

  Por lo tanto, los posibles valores de $(a' + 2b' : a' - b')$ si $a' \perp b'$ son en principio 1 y 3. Efectivamente si por ejemplo $a' = 1$ y $b' = 0$, $(a' + 2b' : a' - b') = 1$ mientras que si $a' = b' = 1$, $(a' + 2b' : a' - b') = (3 : 0) = 3$.

  Por lo tanto hemos probado que si $(a : b) = 6$, los valores que puede tomar

  $$(6a + 12b : 6\,a - 6\,b) = 36(a' + 2b : a' - b')$$

  son $36 \cdot 1 = 36$ o $36 \cdot 3 = 108$.

- Sea $a \in \mathbb{Z}$ tal que $(a : 8) = 4$. ¿Cuáles son los posibles valores de $(a^2 + a + 32 : 16)$?

  La condición $(a : 8) = 4$ implica en particular que $4 \mid a$, o sea $a = 4\,a'$. Por lo tanto,

  $$4 = (a : 8) = (4a' : 4 \cdot 2) = 4(a' : 2) \implies 1 = (a' : 2),$$

  o sea a' impar. Luego,

  $$\begin{aligned}(a^2 + a + 32 : 16) &= (16\,a'^2 + 4\,a' + 32 : 16) = \big(4\,(4\,a'^2 + a' + 8) : 4 \cdot 4\big) \\ &= 4\,(4a'^2 + a' + 8 : 4),\end{aligned}$$

  donde a' es impar. Ahora bien, $(4a'^2 + a' + 8 : 4) \in \{1, 2, 4\}$ pues tiene que ser un divisor positivo de 4. Como claramente $2 \nmid 4a'^2 + a' + 8$ pues a' es impar, 2 no es un divisor común (no divide al mcd). Luego $(4a'^2 + 4a' + 8 : 4) = 1$, y por lo tanto $(a^2 + a + 32 : 16) = 4 \cdot 1 = 4$.

De hecho la Proposición 4.5.13 permite presentar otra caracterización del máximo común divisor, como las propuestas en el Teorema 4.5.9:

Observación 4.5.14. Sean $a, b \in \mathbb{Z}$, no ambos nulos. Sea $d \in \mathbb{N}$ un número que satisface que

$$d \mid a,\ d \mid b \quad \text{y} \quad \frac{a}{d} \perp \frac{b}{d}.$$

Entonces $d = (a : b)$.

(Esto vale por ejemplo porque $\frac{a}{d} \perp \frac{b}{d} \Leftrightarrow \exists\, s, t \in \mathbb{Z}$ con $1 = s\frac{a}{d} + t\frac{b}{d}$, lo que implica que $d = sa + tb$, la caracterización (2) del Teorema 4.5.9.)

4.6 Primos y factorización.

Recordemos que un número $p \in \mathbb{Z}$ es *primo* si y solo si es $\neq 0, \pm 1$ y tiene únicamente 4 divisores, o, lo que es lo mismo, si y solo si tiene únicamente 2 divisores positivos. También, que un número $a \in \mathbb{Z}$ es *compuesto* si y solo si es $\neq 0, \pm 1$ y existe $d \in \mathbb{Z}$ con $1 < d < |a|$ tal que $d \mid a$.
Los números primos juegan un papel fundamental en el conjunto de los números enteros, y su estudio es la base de la Teoría de Números o Aritmética.

Una de las propiedades esenciales que distingue a los números primos de los números compuestos es que "todo número es divisible por algún número primo":

Proposición 4.6.1. (Todo número entero $\neq 0, \pm 1$ es divisible por algún primo.)

Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$. Entonces existe un número primo (positivo) p tal que $p \mid a$.

Demostración. La demostración intuitiva de "si a es primo, ya está pues es divisible por él mismo, y si no, es compuesto, entonces es divisible por algún b más chico, si ese b es primo, ya está, si no es divisible por algún c más chico, etc..." se formaliza por inducción en a.

Claramente alcanza probar la proposición para a positivo, es decir para $a \geq 2$ (pues $a \neq 0, \pm 1$) pues sabemos que $p \mid a \Leftrightarrow p \mid |a|$.

$$p(a): \quad \exists\, p \text{ primo positivo } :\ p \mid a.$$

- Caso base: ¿$p(2)$ V? Sí, pues $p := 2 \mid 2$.
- Paso inductivo: Dado $a > 2$, ¿$p(2), \ldots, p(a-1)$ Verdaderas $\Rightarrow$ $p(a)$ Verdadera?

- HI: $\forall\, d,\ 1 < d < a$, existe un primo (positivo) p tal que $p \mid d$.
- Qpq existe un primo (positivo) p tal que $p \mid a$.

Se tiene:

- Si a es primo, $p(a)$ es verdadera pues $p := a \mid a$.
- Si a no es primo, entonces es compuesto, y por lo tanto existe $d \in \mathbb{Z}$ con $1 < d < a$ tal que $d \mid a$. Por hipótesis inductiva, como $1 < d < a$, existe un primo positivo p tal que $p \mid d$. Se concluye que $p \mid a$ por transitividad de la divisibilidad.

Es decir hemos probado tanto el caso base como el paso inductivo. Se concluye que $p(a)$ es Verdadero, $\forall\, a \geq 2$. Así, todo número distinto de $0, \pm 1$ es divisible por algún primo positivo.

Notemos que éste es un perfecto ejemplo de inducción completa ya que en el caso en que a es compuesto, no se sabe exactamente quién es el divisor d de a a quién se le aplica la hipótesis inductiva: sólo se sabe que es alguno entre 1 y a. □

Una consecuencia de este hecho es que hay infinitos primos distintos. (El hecho que haya infinitos números naturales no garantiza de por sí que haya infinitos primos ya que los infinitos números podrían obtenerse multiplicando de distintas formas y a distintas potencias finitos primos.) La demostración que damos a continuación fue hecha por Euclides alrededor el año 300 AC. Hay muchas otras demostraciones de este hecho (por ejemplo otra conocida se basa en que la serie armónica diverge).

Corolario 4.6.2. (Cantidad de primos.)

Existen infinitos primos (positivos) distintos.

Demostración. Supongamos que no es así y que hay sólo un número finito N de primos positivos. O sea que el conjunto $\mathcal{P}$ de primos positivos es $\mathcal{P} = \{\, p_1, \ldots, p_N \,\}$. Consideremos entonces el siguiente número natural M:

$$M := p_1 \cdot p_2 \cdots p_N + 1.$$

Dado que $M \geq 2$ pues $2 \in \mathcal{P}$, existe por la proposición anterior un primo positivo $p_i \in \mathcal{P}$ que divide a M. Pero

$$p_i \mid M \quad \text{y} \quad p_i \mid p_1 \cdot p_2 \cdots p_N \quad \Longrightarrow \quad p_i \mid 1,$$

contradicción que proviene de suponer que hay sólo finitos primos. □

Otra consecuencia de que todo número $\neq 0, \pm 1$ es divisible por algún primo es la famosa Criba de Eratóstenes de Cirene ($\sim$276–$\sim$194 AC), que construye recursivamente la lista de todos los primos hasta un número dado. Por ejemplo aquí la lista de primos hasta 57:

Criba de Eratóstenes (hasta 57)

- Se escribe la lista de todos los números del 2 al 57:

  $2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, , 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57.$

- Se tachan los múltiplos estrictos del primero de la lista, el 2, que sabemos que es primo:

  $\boxed{2}, 3, \not{4}, 5, \not{6}, 7, \not{8}, 9, \not{10}, 11, \not{12}, 13, \not{14}, 15, \not{16}, 17, \not{18}, 19, \not{20}, 21, \not{22}, 23, \not{24}, 25, \not{26}, 27, \not{28}, 29, \not{30}, 31, \not{32}, 33, \not{34}, 35, \not{36}, 37, \not{38}, 39, \not{40}, 41, \not{42}, 43, \not{44}, 45, \not{46}, 47, \not{48}, 49, \not{50}, 51, \not{52}, 53, \not{54}, 55, \not{56}, 57.$

  El primero que sobrevivió, en este caso el 3, es claramente primo, ya que sino tendría que ser divisible por un primo más chico que él.

- Se tachan los múltiplos estrictos (no tachados en la lista) del 3:

  $\boxed{2}, \boxed{3}, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \not{21}, \not{22}, 23, \not{24}, 25, \not{26}, \not{27}, \not{28}, 29, \not{30}, 31, \not{32}, \not{33}, \not{34}, 35, \not{36}, 37, \not{38}, \not{39}, \not{40}, 41, \not{42}, 43, \not{44}, \not{45}, \not{46}, 47, \not{48}, 49, \not{50}, \not{51}, \not{52}, 53, \not{54}, 55, \not{56}, \not{57}.$

  El primero que sobrevivió, en este caso el 5, es claramente primo, ya que sino tendría que ser divisible por un primo más chico que él.

- Se repite el procedimiento con el 5:

  $\boxed{2}, \boxed{3}, \not{4}, \boxed{5}, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \not{21}, \not{22}, 23, \not{24}, \not{25}, \not{26}, \not{27}, \not{28}, 29, \not{30}, 31, \not{32}, \not{33}, \not{34}, \not{35}, \not{36}, 37, \not{38}, \not{39}, \not{40}, 41, \not{42}, 43, \not{44}, \not{45}, \not{46}, 47, \not{48}, 49, \not{50}, \not{51}, \not{52}, 53, \not{54}, \not{55}, \not{56}, \not{57}.$

- Se repite el procedimiento con el 7:

  $\boxed{2}, \boxed{3}, \not{4}, \boxed{5}, \not{6}, \boxed{7}, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \not{21}, \not{22}, 23, \not{24}, \not{25}, \not{26}, \not{27}, \not{28}, 29, \not{30}, 31, \not{32}, \not{33}, \not{34}, \not{35}, \not{36}, 37, \not{38}, \not{39}, \not{40}, 41, \not{42}, 43, \not{44}, \not{45}, \not{46}, 47, \not{48}, \not{49}, \not{50}, \not{51}, \not{52}, 53, \not{54}, \not{55}, \not{56}, \not{57}.$

- Se puede probar que alcanza hacer esto hasta que se alcanzó el último primo $p \leq \sqrt{57}$, es decir hasta el primo $p = 7$, pues todo número compuesto n es divisible por algún primo menor o igual que su raíz cuadrada (probarlo). Luego la lista que quedó de números no tachados son todos los primos menores o iguales que 57, es decir:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53.$$

Legendre

Gauss

V. Poussin

Hadamard

Agrawal

Kayal

Saxena

Digresión sobre Complejidad (1) Dado un número a, hay un algoritmo muy natural para establecer si a es primo o no: simplemente se divide a a por todos los números d menores que él (o por todos los primos menores que él, produciéndolos por ejemplo con la criba, o en realidad alcanza con dividirlo por todos los primos menores que $\sqrt{a}$, como se comentó arriba). Si nunca da resto 0, es que a es primo. Pero este algoritmo no es muy satisfactorio ya que la cantidad de candidatos a divisores d se asemeja a $\sqrt{a}$ (más precisamente a $\sqrt{a/\ln(a)}$ como consecuencia del teorema de distribución de primos conjeturado por Adrien-Marie Legendre en 1798, refinado posteriormente por Carl-Fiedrich Gauss, y demostrado independientemente por Jacques Hadamard y Charles-Jean de la Vallée Poussin en 1896).

Es comúnmente aceptado que para que un algoritmo sea eficiente, la cantidad de cuentas que realiza tiene que ser lineal en el tamaño de la entrada, o sea la cantidad de espacio de memoria que ocupa el número en una computadora: en este caso $\log_2(a)$, o a lo sumo acotado por una potencia fija de ese tamaño (esto es lo que se llama un algoritmo polinomial, o que pertenece a la clase P).
Hasta muy recientemente, el mejor algoritmo para decidir si un número a es primo realizaba $\log_2(a)^{c \log\log\log(a)}$ para una constante fija c, o sea era "casi" polinomial.

En el año 2002, el informático indio, Manindra Agrawal, y dos de sus alumnos que estaban haciendo su tesis de maestría bajo su dirección, Neeraj Kayal y Nitin Saxena, mostraron que "Primos está en P", es decir que se puede establecer si un número entero a es primo (o no) haciendo una cantidad de cuentas acotada por una potencia fija de $\log_2(a)$.

Este test de primalidad (denominado test de primalidad AKS) no es en realidad eficiente en la práctica: para ello se siguen usando tests "probabilistas" que dan una evidencia seria de primalidad cuando no pueden probar que un

número es compuesto, y son suficientes a efectos prácticos. Sin embargo, el resultado de Agrawal, Kayal y Saxena es fantástico, no sólo por lograr finalmente un objetivo teórico de clasificación buscado por mucha gente durante mucho tiempo, sino por la simplicidad y elegancia de sus métodos. Así fue reconocido por la comunidad matemática: fue publicado en el año 2004 en la revista Annals of Mathematics (considerada la mejor revista matemática del mundo) y le valió a sus autores numerosos premios (y a los dos jóvenes excelentes trabajos).
Para terminar esta digresión, el número primo más grande conocido hoy (hoy es 27 de Marzo de 2019, puede cambiar mañana!) es el "primo de Mersenne" $2^{82\,589\,933}-1$, que tiene $24\,862\,048$ dígitos, según lo que nos dice internet.

Los primos de Mersenne son números primos de la forma 2^p-1 con p primo (se puede comprobar que si un número de la forma 2^n-1 es primo, entonces el exponente n tiene que ser primo, pero no vale la recíproca: $2^{11}-1$ no es primo), y se llaman así en honor al monje y matemático francés Marin Mersenne, 1588-1648, que los estudió.

Es un problema abierto determinar si hay infinitos primos de Mersenne.

Digresión sobre Complejidad (2) Un problema de otra índole, y cuya resolución haría muy famoso a cualquiera, es el problema de, dado un número a compuesto, encontrarle eficientemente un factor d no trivial (o sea $\neq 1, a$). No existe ningún algoritmo a la fecha que realiza una cantidad de cuentas polinomial en $\log_2(a)$, y el número más grande que se logró factorizar (anunciado en el 2010), usando cientos de computadoras que trabajaron durante más de 2 años, tiene 232 dígitos. Se sabe que este problema está en NP, lo que hablando sin precisión, significa que si un "oráculo" me provee de un candidato a factor d, se puede verificar haciendo una cantidad polinomial (en $\log(a)$) de cuentas, si d es efectivamente un factor o no de a. Se cree que este problema es dificil, o sea que no pertenece a la clase P. De hecho la mayoría de los protocolos criptográficos (para transmisión de datos en forma segura y secreta) que se utilizan hoy en día están basados en la dificultad de factorizar números compuestos grandes (o de problemas relacionados)¡así que mejor que así sea!

4.6.1 La propiedad fundamental de los números primos.

Si p es un número primo (positivo), y $a \in \mathbb{Z}$ es cualquiera, entonces $\mathrm{Div}_+(p) = \{1, p\}$ y por lo tanto $\mathrm{DivCom}_+(\{p, a\}) \subset \{1, p\}$: es igual a $\{1, p\}$ cuando $p \mid a$ y es igual a $\{1\}$ cuando $p \nmid a$. Por lo tanto el máximo común divisor entre p y a, es igual a p cuando $p \mid a$ y es igual a 1 cuando

$p \nmid a$:

$$(p : a) = \begin{cases} p & \text{si} \quad p \mid a \\ 1 & \text{si} \quad p \nmid a \end{cases}, \qquad \text{y por lo tanto} \qquad p \perp a \;\Leftrightarrow\; p \nmid a.$$

(En particular, observemos que si p y q son primos positivos distintos, entonces $p \perp q$.)

Volvamos a la Proposición 4.5.12,(2) para p y a. En este caso, ella dice:

Teorema 4.6.3. (Propiedad fundamental de los números primos.)

Sea p un primo y sean $a, b \in \mathbb{Z}$. Entonces

$$p \mid a \cdot b \implies p \mid a \quad o \quad p \mid b.$$

Demostración. La Proposición 4.5.12 (2) dice que si $p \mid a \cdot b$ y $p \perp a$ entonces $p \mid b$. Por lo visto arriba, la condición $p \perp a$ es equivalente a $p \nmid a$. Luego la Proposición 4.5.12 (2) dice que si $p \mid a \cdot b$ y $p \nmid a$ entonces $p \mid b$. Esto es claramente lo mismo que decir que si $p \mid a \cdot b$ entonces $p \mid a$ o $p \mid b$, pues si $p \mid a \cdot b$, hay dos posibilidades: Si $p \mid a$, ya está. Y si $p \nmid a$, entonces $p \mid b$. □

Esta es la propiedad más importante que cumplen los números primos (comparar con el último inciso de las Propiedades 4.2.4). Más aún, esta propiedad caracteriza los números primos:

p es primo si y solo si cada vez que p divide a un producto divide a alguno de los factores.

Esta es de hecho la definición de elemento primo en un dominio íntegro arbitrario, como verán más adelante los que estudian matemática. En el caso de los números enteros $\mathbb{Z}$, se puede probar que para $p \neq 0, \pm 1$, son equivalentes las propiedades

- p tiene únicamente 2 divisores positivos.
- $\forall\, a, b,\ p \mid a \cdot b \;\Rightarrow\; p \mid a$ o $p \mid b$.

(Pues acabamos de probar que si p tiene únicamente 2 divisores positivos, entonces $p \mid a \cdot b \;\Rightarrow\; p \mid a$ o $p \mid b$. Para probar que la condición $\forall\, a, b$, $p \mid a \cdot b \;\Rightarrow\; p \mid a$ o $p \mid b$ implica que p tiene únicamente 2 divisores positivos, probaremos la contrarecíproca: Si $p \neq 0, \pm 1$ tuviera más que 2 divisores positivos, o sea fuera compuesto, entonces $p = c \cdot d$ con $1 < c, d < p$. Luego se tendría $p \mid c \cdot d$ pero $p \nmid c$ y $p \nmid d$.)

Esta equivalencia justifica la definición histórica de primo que usamos aquí.

El Teorema 4.6.3 se generaliza inmediatamente a

Proposición 4.6.4. *Sea p un número primo y sean $a_1, \ldots, a_n \in \mathbb{Z}$, con $n \geq 2$. Entonces*

$$p \mid a_1 \cdots a_n \implies p \mid a_i \text{ para algún } i,\ 1 \leq i \leq n.$$

En particular, dado $a \in \mathbb{Z}$, si $p \mid a^n$ entonces $p \mid a$.

Demostración. Por inducción en n, empezando en $n = 2$.

$p(n)$: $\forall\, a_1, \ldots, a_n \in \mathbb{Z},\ p \mid a_1 \cdots a_n \implies p \mid a_i$ para algún $i,\ 1 \leq i \leq n$.

- Caso base: ¿$p(2)$ V? Sí, por el Teorema 4.6.3: si $p \mid a_1 \cdot a_2$ entonces $p \mid a_1$ o $p \mid a_2$.
- Paso inductivo: Dado $h \geq 2$, ¿$p(h)$ Verdadera $\Rightarrow$ $p(h{+}1)$ Verdadera?
  - HI: $\forall\, a_1, \ldots, a_h \in \mathbb{Z},\ p \mid a_1 \cdots a_h \Rightarrow p \mid a_i$ para algún $i,\ 1 \leq i \leq h$.
  - Qpq $\forall\, a_1, \ldots, a_{h+1} \in \mathbb{Z},\ p \mid a_1 \cdots a_{h+1} \Rightarrow p \mid a_i$ para algún $i,\ 1 \leq i \leq h+1$.

  Llamemos $b = a_1 \cdots a_h$. Entonces $p \mid a_1 \cdots a_{h+1} \Leftrightarrow p \mid b \cdot a_{h+1}$. Luego por el Teorema 4.6.3 (el caso n=2) aplicado a b y a_{h+1}, $p \mid b \cdot a_{h+1} \Rightarrow p \mid b$ o $p \mid a_{h+1}$.

  Si $p \mid a_{h+1}$, ya está. Y si $p \mid b = a_1 \cdots a_h$, por HI, $p \mid a_i$ para algún i, $1 \leq i \leq h$. O sea que también está.

Es decir hemos probado tanto el caso base como el paso inductivo. Se concluye que $p(n)$ es Verdadero, $\forall\, n \geq 2$. □

4.6.2 El Teorema fundamental de la aritmética.

Estamos ahora en condiciones de demostrar completamente el famoso *Teorema fundamental de la aritmética*, piedra angular de toda la teoría de números, acerca de la factorización única de los números como producto de primos.

Este teorema parece ser que fue enunciado y demostrado por primera vez por Gauss en el S. XVIII-XIX, y es el que explica cómo son los números. En particular justifica el interés de los matemáticos por conocer mejor el comportamiento de los primos: cómo se distribuyen, cómo conseguirlos, etc.

Teorema 4.6.5. (Teorema fundamental de la aritmética.)

Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$. Entonces a se escribe en forma única como producto de primos (positivos)*, (o se factoriza en forma única como producto de primos (positivos),) es decir:*

- $\forall\, a \in \mathbb{Z},\ a \neq 0, \pm 1$, *existe* $r \in \mathbb{N}$ *y* existen *primos positivos* $p_1, \ldots, p_r$ *distintos y* $m_1, \ldots, m_r \in \mathbb{N}$ *tales que*

$$a = \pm\, p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}.$$

- *Esta escritura es* única *salvo permutación de los primos.*

Demostración.

Existencia: Nuevamente, alcanza con probar el teorema para a positivo, y se formaliza por inducción en a, $a \geq 2$:

$p(a)$: a admite una factorización como producto de primos.

- Caso base: $p(2)$ es Verdadera pues $2 = +\,2^1$.
- Paso inductivo:
  - Si a es un primo p, $p(a)$ es verdadera pues $a = p = +\,p^1$.
  - Si a no es primo, entonces por la Proposición 4.6.1, a es divisible por algún primo positivo p más chico que él, y por lo tanto el cociente $k = a/p$ satisface $2 \leq k \leq a-1$. Por hipotesis inductiva, k admite una factorización como producto de primos, en la forma $k = p_1^{m_1} \cdots p_r^{m_r}$. Por lo tanto a admite la factorización

$$a = p \cdot p_1^{m_1} \cdots p_r^{m_r}.$$

Así, todo número distinto de $0, \pm 1$ admite una factorización como producto de primos.

Unicidad: Supongamos que $a = \pm\, p_1^{m_1} \cdots p_r^{m_r} = \pm\, q_1^{n_1} \cdots q_s^{n_s}$ en las condiciones del enunciado. Queremos probar que entonces los signos, los primos y los exponentes coinciden.

Claramente los signos coinciden, así que podemos suponer a positivo.

En la expresión $p_1^{m_1} \cdots p_r^{m_r} = q_1^{n_1} \cdots q_s^{n_s}$, simplifiquemos todos los primos comunes (que aparecen de los dos lados) a la menor potencia a la que aparecen.

Si al hacer eso no sobra nada, o sea obtenemos $1 = 1$, es que todos los primos y las potencias coincidían.

Si no pasa eso y sobra algo de algún lado al menos, obtenemos una expresión del mismo tipo, pero donde $p_i \neq q_j$ (pues son todos los que sobraron). Podemos suponer sin pérdida de generalidad que del lado izquierdo sobró un p_i. Entonces tenemos que p_i divide a lo que sobró del lado derecho o al 1 si no sobró nada. O sea $p_i \mid 1$ (lo que es absurdo) o $p_i \mid q_1^{n_1} \cdots q_s^{n_s}$. En

este último caso, por la Proposición 4.6.4, existe j tal que $p_i \mid q_j$ pero p_i y q_j son primos distintos. Contradicción, que proviene de suponer que sobró un primo de algún lado. □

Cuando uno conoce la factorización en primos de un número, conoce todo del número, como se verá en lo que sigue.

Ejemplo: Sean $a = 84 = 2^2 \cdot 3 \cdot 7$ y $b = 188650 = 2 \cdot 5^2 \cdot 7^3 \cdot 11$. Entonces

$$a \cdot b = 2^3 \cdot 3 \cdot 5^2 \cdot 7^4 \cdot 11 \quad \text{y} \quad a^9 = 2^{18} \cdot 3^9 \cdot 7^9$$

son las factorizaciones en primos de $a \cdot b$ y a^9 (simplemente se suman (o multiplican) los exponentes). Esto vale siempre. Para formular fácilmente este resultado, si $a, b \in \mathbb{Z}$ son dos números no nulos, convenimos en escribirlos como potencias de los mismos primos (positivos) distintos $p_1, \ldots, p_r$, permitiendo poner potencia 0 cuando el primo no aparece. Por ejemplo, para $a = 84 = 2^2 \cdot 3 \cdot 7$ y $b = 188650 = 2 \cdot 5^2 \cdot 7^3 \cdot 11$, escribimos

$$a = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^0 \quad \text{y} \quad b = 2^1 \cdot 3^0 \cdot 5^2 \cdot 7^3 \cdot 11^1.$$

Observación 4.6.6. (Primos de productos y potencias.)

Sean $a, b \in \mathbb{Z}$ no nulos de la forma

$$a = \pm p_1^{m_1} \cdots p_r^{m_r} \quad \text{con} \quad m_1, \ldots, m_r \in \mathbb{N}_0,$$
$$b = \pm p_1^{n_1} \cdots p_r^{n_r} \quad \text{con} \quad n_1, \ldots, n_r \in \mathbb{N}_0.$$

Entonces

- $a \cdot b = \left(\pm p_1^{m_1} \cdots p_r^{m_r} \right) \cdot \left(\pm p_1^{n_1} \cdots p_r^{n_r} \right) = \pm p_1^{m_1+n_1} \cdots p_r^{m_r+n_r}$.

  Es decir $a \cdot b$ tiene exactamente los primos de a y de b en su factorización y los exponentes se suman.

- $a^n = \left(\pm p_1^{m_1} \cdots p_r^{m_r} \right)^n = (\pm 1)^n \, p_1^{m_1 n} \cdots p_r^{m_r n}$ es la factorización en primos de a^n, para todo $n \in \mathbb{N}$.

  Es decir a^n tiene exactamente los mismos primos que a en su factorización, y los exponentes van multiplicados por n.

Nota: Otro hecho que se desprende de este (y que de hecho aparece en la demostración de la unicidad de la factorización) es que $p \mid a$ si y solo si p aparece en la factorización en primos de a.

Ejemplos:

- El Teorema fundamental de la Aritmética permite por ejemplo probar que $\sqrt{2}$ no es un número racional. Pues si fuera $\sqrt{2} = \dfrac{a}{b}$ con $a, b \in \mathbb{N}$

tendríamos $\sqrt{2}\,b = a$, o sea $2\,b^2 = a^2$, donde $a = p_1^{m_1}\cdots p_r^{m_r}$ con $m_1,\ldots,m_r \in \mathbb{N}_0$, $b = p_1^{n_1}\cdots p_r^{n_r}$ con $n_1,\ldots,n_r \in \mathbb{N}_0$. Luego

$$2\,p_1^{2n_1}\cdots p_r^{2n_r} = p_1^{2m_1}\cdots p_r^{2m_r}$$

lo que es claramente imposible por la unicidad de la factorización en primos, porque a la izquierda el primo 2 aparece un número impar de veces, mientras que a la derecha aparece un número par de veces.

- Sea $d \mid 2^3\cdot 5^4$. ¿Cómo puede ser d?

  Está claro que si $k\cdot d = 2^3\cdot 5^4$, entonces en k y en d no pueden aparecer más que los primos 2 y 5 (por la unicidad de la factorización). Además si $d = 2^i\cdot 5^j$ con $0 \le i,j$ para que $d\in\mathbb{Z}$, y $k = 2^{i'}\cdot 5^{j'}$ con $0 \le i',j'$ para que $k\in\mathbb{Z}$, tiene que satisfacerse

  $$2^3\cdot 5^4 = k\cdot d = 2^{i'}\cdot 5^{j'}\cdot 2^i\cdot 5^j = 2^{i'+i}\cdot 5^{j'+j}.$$

  Así, $i'+i=3$ y $j'+j=4$. Esto implica, dado que $i'\ge 0$ y $j'\ge 0$, que $0\le i\le 3$ y $0\le j\le 4$.

  Así, si $d \mid 2^3\cdot 5^4$, la factorización en primos de d es

  $$d = 2^i\cdot 5^j, \quad \text{con } 0\le i\le 3,\ 0\le j\le 4.$$

  Luego $\mathrm{Div}(2^35^4) = \{\pm 2^i5^j,\ 0\le i\le 3, 0\le j\le 4\}$.

  Por lo tanto, 2^35^4 tiene $(3{+}1)(4{+}1) = 20$ divisores positivos distintos, y $2\cdot 20 = 40$ divisores enteros, positivos y negativos.

Proposición 4.6.7. (Divisores de un número y cantidad.)

Sea $a\in\mathbb{Z}$, $a\neq 0,\pm 1$, y sea $a = \pm\,p_1^{m_1}\cdots p_r^{m_r}$ la factorización en primos de a. Entonces

1. $d \mid a \iff d = \pm\,p_1^{n_1}\cdots p_r^{n_r}$ *con* $0\le n_1\le m_1,\ldots,0\le n_r\le m_r$.
2. $\#\mathrm{Div}_+(a) = (m_1{+}1)\cdots(m_r{+}1)$ *y* $\#\mathrm{Div}(a) = 2(m_1{+}1)\cdots(m_r{+}1)$.

Demostración. Es claro que alcanza con probar la proposición para $a = p_1^{m_1}\cdots p_r^{m_r}$ positivo.

1. ($\Rightarrow$) $d\mid a \Leftrightarrow \exists\, k\in\mathbb{Z}$ tq $a = k\cdot d$. Luego la factorización en primos de $k\cdot d$ tiene que ser igual a la de a:

   $$k\cdot d = p_1^{m_1}\cdots p_r^{m_r}.$$

   Esto implica por la Observación 4.6.6 que la factorización en primos de d debe ser de la forma $d = \pm\,p_1^{n_1}\cdots p_r^{n_r}$ para $n_1,\ldots,n_r$ que satisfacen $0\le n_1\le m_1,\ldots,0\le n_r\le m_r$.

($\Leftarrow$) Si $d = \pm p_1^{n_1} \cdots p_r^{n_r}$ con $0 \leq n_1 \leq m_1, \ldots, 0 \leq n_r \leq m_r$, entonces podemos tomar

$$k = \pm p_1^{m_1 - n_1} \cdots p_r^{m_r - n_r}$$

(todos los exponentes son ≥ 0 y por lo tanto $k \in \mathbb{Z}$), y es luego claro que

$$k \cdot d = (p_1^{m_1 - n_1} \cdots p_r^{m_r - n_r}) \cdot (p_1^{n_1} \cdots p_r^{n_r}) = p_1^{m_1} \cdots p_r^{m_r} = a.$$

2. Ahora solo se trata de contar:

   $$\mathrm{Div}_+(p_1^{m_1} \cdots p_r^{m_r}) = \{p_1^{n_1} \cdots p_r^{n_r} \text{ con } 0 \leq n_1 \leq m_1, \ldots, 0 \leq n_r \leq m_r\},$$

   y luego hay $(m_1 + 1)$ elecciones para n_1 (de 0 a m_1), $(m_2 + 1)$ elecciones para n_2 (de 0 a m_2), etc.

   O sea $\#\mathrm{Div}_+(a) = (m_1 + 1) \cdots (m_r + 1)$, y hay el doble de divisores totales (positivos y negativos).

□

Ejemplos:

- Calcular la suma de los divisores positivos de 10^{10}: Se tiene

  $$\mathrm{Div}_+(10^{10}) = \mathrm{Div}_+(2^{10} \cdot 5^{10}) = \{2^i 5^j,\ 0 \leq i \leq 10, 0 \leq j \leq 10\}.$$

  Por lo tanto

  $$\sum_{d>0, d|10^{10}} d = \sum_{0 \leq i,j \leq 10} 2^i 5^j = \sum_{i=0}^{10} (\sum_{j=0}^{10} 2^i 5^j) = \sum_{i=0}^{10} (2^i \sum_{j=0}^{10} 5^j)$$
  $$= (\sum_{j=0}^{10} 5^j)(\sum_{i=0}^{10} 2^i) = \frac{5^{11} - 1}{5 - 1} \cdot \frac{2^{11} - 1}{2 - 1} = (2^{11} - 1)\frac{5^{11} - 1}{4}.$$

- ¿Cuál es el menor número natural n con 12 divisores positivos?

  $a = 1$ tiene únicamente 1 divisor positivo. O sea $a \geq 2$. Sea $a = p_1^{m_1} \cdots p_r^{m_r}$ con $m_1, \ldots, m_r \in \mathbb{N}$ la factorización en primos de a. Sabemos que entonces la cantidad de divisores positivos de a es $(m_1 + 1) \cdots (m_r + 1)$. Observemos que como $m_i \geq 1$, entonces $m_i + 1 \geq 2$, $\forall\, i$. Luego, la condición $12 = (m_1 + 1) \cdots (m_r + 1)$ implica $12 \geq 2^r$, o sea $r \leq 3$: a tiene a lo sumo 3 primos distintos. Por lo tanto a es de una de las siguientes formas:

  $$a = p^m \quad \text{o} \quad a = p_1^{m_1} \cdot p_2^{m_2} \quad \text{o} \quad a = p_1^{m_1} \cdot p_2^{m_2} \cdot p_3^{m_3}.$$

- Caso $a = p^m$: En ese caso a tiene $m+1$ divisores positivos. Si se quiere que sean 12, entonces $m+1 = 12$ implica $m = 11$: $a = p^{11}$, y el más chico de ellos es claramente $a = 2^{11} = 2048$.
- Caso $a = p_1^{m_1} \cdot p_2^{m_2}$: En ese caso a tiene $(m_1+1)(m_2+1)$ divisores positivos. Si se quiere que sean 12, entonces $(m_1+1)(m_2+1) = 12 = 6 \cdot 2 = 4 \cdot 3$ implica $m_1+1 = 6, m_2+1 = 2$ o $m_1+1 = 4, m_2+1 = 3$ (o cambiando el rol de m_1 y m_2). Así se obtiene $m_1 = 5, m_2 = 1$ o $m_1 = 3, m_2 = 2$. Luego $a = p_1^5 \cdot p_2$ o $a = p_1^3 \cdot p_2^2$. Claramente los más chicos de éstos son $a = 2^5 \cdot 3 = 96$ y $a = 2^3 \cdot 3^2 = 72$.
- Caso $a = p_1^{m_1} \cdot p_2^{m_2} \cdot p_3^{m_3}$: En ese caso a tiene $(m_1+1)(m_2+1)(m_3+1)$ divisores positivos. Si se quiere que sean 12, entonces $(m_1+1)(m_2+1)(m_3+1) = 12 = 3 \cdot 2 \cdot 2$ implica $m_1+1 = 3, m_2+1 = 2$ y $m_3+1 = 2$ (o cambiando el rol de m_1, m_2 y m_3). Así se obtiene $m_1 = 2, m_2 = 1, m_3 = 1$. Luego $a = p_1^2 \cdot p_2 \cdot p_3$. Claramente el más chico de éstos es $a = 2^2 \cdot 3 \cdot 5 = 60$.

Por lo tanto en menor número natural con 12 divisores positivos es $a = 60$.

Habíamos visto en la Proposición 4.2.4 que si $d \mid a$ entonces $d^n \mid a^n$ para todo $n \in \mathbb{N}$, y mencionado que vale la recíproca pero aún no teníamos a ese nivel las herramientas para probarlo. Ahora sí...

Proposición 4.6.8. (Divisores y potencias.)

Sean $a, d \in \mathbb{Z}$ con $d \neq 0$, y sea $n \in \mathbb{N}$. Entonces

$$d \mid a \iff d^n \mid a^n.$$

Ojo que en la Proposición, tiene que ser el mismo exponente n de los dos lados del signo $\mid$. Si no, no es cierto. Por ejemplo $2 \mid 4$ pero $2^{10} \nmid 4^2$, y $8^2 \mid 4^3$ pero $8 \nmid 4$.

Demostración. Solo falta probar $(\Leftarrow)$, que si $d^n \mid a^n$ entonces $d \mid a$.

- Para $a = 0$ no hay nada que probar porque $d \mid 0$, $\forall\, d \neq 0$.
- Para $a = \pm 1$, casi tampoco, ya que si $d^n \mid (\pm 1)^n$, entonces $d^n = \pm 1$, luego $d = \pm 1$, que divide a $a = \pm 1$.
- El caso $a \neq 0, \pm 1$ es el interesante. Si $a = \pm p_1^{m_1} \cdots p_r^{m_r}$, entonces

$$a^n = (\pm p_1^{m_1} \cdots p_r^{m_r})^n = \pm p_1^{n \cdot m_1} \cdots p_r^{n \cdot m_r}.$$

Ahora bien, la condición $d^n \mid a^n$ implica que $d \mid a^n$. Por lo tanto $d = \pm p_1^{n_1} \cdots p_r^{n_r}$ no tiene más primos en su factorización que los de a. Pero entonces

$$d^n = \pm p_1^{n \cdot n_1} \cdots p_r^{n \cdot n_r} \mid a^n$$

implica por la Proposición 4.6.7 que $0 \leq n \cdot n_1 \leq n \cdot m_1, \ldots, 0 \leq n \cdot n_r \leq n \cdot m_r$, es decir, simplificando el n, que

$$0 \leq n_1 \leq m_1, \ldots, 0 \leq n_r \leq m_r.$$

Esto prueba, nuevamente por la Proposición 4.6.7, que $d \mid a$.

□

Podemos ahora dar la caracterización del *máximo común divisor* y del *mínimo común múltiplo* de dos números no nulos que se suele dar en el colegio, o las fórmulas para calcularlos cuando se conoce la factorización de los números. Por ejemplo, para $a = 588 = 2^2 \cdot 3 \cdot 7^2$ y $b = 188650 = 2 \cdot 5^2 \cdot 7^3 \cdot 11$, "sabemos" que el máximo común divisor $(a : b)$ es el producto de los primos comunes a a y b a la menor potencia a la que aparecen, o sea $(a : b) = 2 \cdot 7^2 = 98$.

Proposición 4.6.9. (Máximo común divisor y factorización.)

Sean $a, b \in \mathbb{Z}$ no nulos de la forma

$$a = \pm p_1^{m_1} \cdots p_r^{m_r} \quad \textit{con} \quad m_1, \ldots, m_r \in \mathbb{N}_0,$$
$$b = \pm p_1^{n_1} \cdots p_r^{n_r} \quad \textit{con} \quad n_1, \ldots, n_r \in \mathbb{N}_0.$$

Entonces

$$(a : b) = p_1^{\min\{m_1, n_1\}} \cdots p_r^{\min\{m_r, n_r\}}.$$

Demostración. Hay que probar que $p_1^{\min\{m_1,n_1\}} \cdots p_r^{\min\{m_r,n_r\}}$ es el mayor de los divisores comunes de a y b. Investiguemos los divisores comunes (positivos) de a y b:

$$d \mid a \iff d = p_1^{k_1} \cdots p_r^{k_r} \quad \text{con} \quad 0 \leq k_1 \leq m_1, \ldots, 0 \leq k_r \leq m_r,$$
$$d \mid b \iff d = p_1^{k_1} \cdots p_r^{k_r} \quad \text{con} \quad 0 \leq k_1 \leq n_1, \ldots, 0 \leq k_r \leq n_r.$$

Por lo tanto $d \mid a$ y $d \mid b$ si y solo si

$$d = p_1^{k_1} \cdots p_r^{k_r} \quad \text{con} \quad 0 \leq k_1 \leq \min\{m_1, n_1\}, \ldots, 0 \leq k_r \leq \min\{m_r, n_r\}.$$

De esa forma el mayor de los divisores comunes es

$$(a : b) = p_1^{\min\{m_1,n_1\}} \cdots p_r^{\min\{m_r,n_r\}}$$

como se quería probar. □

Corolario 4.6.10. (Mcd de potencias.)

Sean $a, b \in \mathbb{Z}$ *no nulos.*

1. *Sean* $a, b \neq 0, \pm 1$ *con factorización en primos* $a = \pm p_1^{m_1} \cdots p_r^{m_r}$, $m_1, \ldots, m_r \in \mathbb{N}$, *y* $b = \pm q_1^{n_1} \cdots q_s^{n_s}$, $n_1, \ldots, n_s \in \mathbb{N}$. *Entonces*

$$(a : b) = 1 \iff p_i \neq q_j, \ \forall\, i, j.$$

2. $(a : b) = 1$ *y* $(a : c) = 1 \iff (a : bc) = 1$.

3. $(a : b) = 1 \iff (a^m : b^n) = 1, \ \forall\, m, n \in \mathbb{N}$.

4. $(a^n : b^n) = (a : b)^n, \ \forall\, n \in \mathbb{N}$.

   ¡Ojo que para esta 4ta propiedad tiene que ser la misma potencia n *!*

Demostración. 1. Sabemos por la Proposición anterior que $(a : b)$ es igual al producto de los primos comunes a a y b con la mínima potencia a la que aparecen. Esto da $(a : b) = 1$ si y solo si no hay primos en común.

2. ($\Rightarrow$) Si $(a : b) = 1$, a no tiene primos en común con b, y si $(a : c) = 1$, a no tienen primos en común con c. Por lo tanto a no tiene primos en común ni con b ni con c, luego no tiene primos en común con bc, ya que los primos de bc son los de b y los de c. Por lo tanto $(a : bc) = 1$.

   ($\Leftarrow$) Recíprocamente, si a no tiene primos en común con bc, no tiene primos en común ni con b ni con c, luego es coprimo con b y con c.

3. a y b no tienen primos en común si y solo si a^m y b^n no tienen primos en común, ya que sabemos que los primos de a^m son exactamente los mismos que los de a, y los primos de b^n exactamente los mismos primos que los de b.

4. Sea $d := (a : b)$. Coprimizando, se tiene que $a = d\,a'$ y $b = d\,b'$ con $a' \perp b'$. Luego,

$$(a^n : b^n) = \big((d\,a')^n : (d\,b')^n\big) = (d^n a'^n : d^n b'^n) = d^n (a'^n : b'^n) = d^n.$$

   O sea $(a^n : b^n) = (a : b)^n$, ya que $a'^n \perp b'^n$ al ser $a' \perp b'$.

□

Ejemplos:

- Calcular $(2^n + 3^n : 2^n - 2 \cdot 3^n)$, para todo $n \in \mathbb{N}$.

Sea d un posible divisor común:

$$\left\{\begin{array}{l} d \mid 2^n + 3^n \\ d \mid 2^n - 2\cdot 3^n \end{array}\right. \implies d \mid 3^n + 2\cdot 3^n \implies d \mid 3\cdot 3^n.$$

De la misma manera:

$$\left\{\begin{array}{l} d \mid 2^n + 3^n \\ d \mid 2^n - 2\cdot 3^n \end{array}\right. \implies \left\{\begin{array}{l} d \mid 2\cdot 2^n + 2\cdot 3^n \\ d \mid 2^n - 2\cdot 3^n \end{array}\right. \implies d \mid 2\cdot 2^n + 2^n \implies d \mid 3\cdot 2^n.$$

Pero

$$d \mid 3\cdot 3^n \text{ y } d \mid 3\cdot 2^n \implies d \mid (3\cdot 3^n : 3\cdot 2^n) = 3\,(3^n : 2^n) = 3\cdot 1 = 3.$$

Por lo tanto, $(2^n + 3^n : 2^n - 2\cdot 3^n) = 1$ o 3.

Pero se ve claramente que 3 no puede ser un divisor común ya que $3 \nmid 2^n + 3^n$ (pues si lo dividiera, se tendría que $3 \mid 2^n$, absurdo!). Por lo tanto el 3 queda descartado como posible mcd, y se concluye que $(2^n + 3^n : 2^n - 2\cdot 3^n) = 1$, $\forall\, n \in \mathbb{N}$.

- Sean $a, b \in \mathbb{Z}$ no ambos nulos tales que $(a : b) = 6$.
  Calcular $(a\,b : 6\,a - 6\,b)$.

  "Coprimizando", se tiene $a = 6\,a'$, $b = 6\,b'$ con $a' \perp b'$, luego

  $$\begin{aligned}(a\,b : 6\,a - 6\,b) &= (36\,a'b' : 36a' - 36b') = (36\,a'b' : 36(a' - b')) \\ &= 36(a'b' : a' - b').\end{aligned}$$

  Para concluir falta calcular los posibles valores de $(a'b' : a' - b')$ cuando $a' \perp b'$:

  Sea d un divisor común:

  $$\left\{\begin{array}{l} d \mid a'b' \\ d \mid a' - b' \end{array}\right. \implies \left\{\begin{array}{l} d \mid a'b' \\ d \mid a'(a' - b') \end{array}\right. \implies \left\{\begin{array}{l} d \mid a'b' \\ d \mid a'^2 - a'b' \end{array}\right. \implies d \mid a'^2$$

  De la misma manera:

  $$\left\{\begin{array}{l} d \mid a'b' \\ d \mid a' - b' \end{array}\right. \implies \left\{\begin{array}{l} d \mid a'b' \\ d \mid b'(a' - b') \end{array}\right. \implies \left\{\begin{array}{l} d \mid a'b' \\ d \mid a'b' - b'^2 \end{array}\right. \implies d \mid b'^2$$

  Obtuvimos $d \mid a'^2$ y $d \mid b'^2$. Luego $d \mid (a'^2 : b'^2)$. Pero, como vimos arriba, $a' \perp b' \Rightarrow a'^2 \perp b'^2$, es decir $(a'^2 : b'^2) = 1$. O sea $d \mid 1$. Así se prueba que los únicos divisores comunes de $a'b'$ y $a' - b'$ son ± 1, luego $a'b' \perp a' - b'$, y se concluye

  $$(a\,b : 6\,a - 6\,b) = 36(a'b' : a' - b') = 36.$$

4.6.3 Mínimo común múltiplo.

Definición 4.6.11. (Mínimo común múltiplo.)

Sean $a, b \in \mathbb{Z}$, no nulos. El *mínimo común múltiplo* entre a y b, que se nota $[a : b]$, es el menor número natural que es un múltiplo común de a y b.

Ejemplo: Como todos ya "saben", para $a = 588 = 2^2 \cdot 3 \cdot 7^2$ y $b = 188650 = 2 \cdot 5^2 \cdot 7^3 \cdot 11$, el mínimo común múltiplo $[a : b]$ es el producto de todos los primos que aparecen en a y en b a la máxima potencia a la que aparecen, o sea $[a : b] = 2^2 \cdot 3 \cdot 5^2 \cdot 7^3 \cdot 11$. Probemos este hecho en general.

Proposición 4.6.12. (Mínimo común múltiplo y factorización.)

Sean $a, b \in \mathbb{Z}$ no nulos de la forma

$$\begin{aligned} a &= \pm\, p_1^{m_1} \cdots p_r^{m_r} \quad \textit{con} \quad m_1, \ldots, m_r \in \mathbb{N}_0, \\ b &= \pm\, p_1^{n_1} \cdots p_r^{n_r} \quad \textit{con} \quad n_1, \ldots, n_r \in \mathbb{N}_0. \end{aligned}$$

Entonces

$$[a : b] = p_1^{\max\{m_1,n_1\}} \cdots p_r^{\max\{m_r,n_r\}}.$$

Demostración. Hay que probar que $p_1^{\max\{m_1,n_1\}} \cdots p_r^{\max\{m_r,n_r\}}$ es el menor de los múltiplos comunes de a y b. Investiguemos luego los múltiplos comunes $m > 0$ de a y b:

$$\begin{aligned} a \mid m &\iff m = p_1^{m_1} \cdots p_r^{m_r} \cdot k_1 \qquad \text{para algún } k_1 \in \mathbb{N}, \\ b \mid m &\iff m = p_1^{n_1} \cdots p_r^{n_r} \cdot k_2 \qquad \text{para algún } k_2 \in \mathbb{N}. \end{aligned}$$

Por lo tanto

$$a \mid m \text{ y } b \mid m \iff m = p_1^{\max\{m_1,n_1\}} \cdots p_r^{\max\{m_r,n_r\}} \cdot k \text{ para algún } k \in \mathbb{N}.$$

De esa forma el menor de los múltiples comunes positivos es con $k = 1$ y da $[a : b] = p_1^{\max\{m_1,n_1\}} \cdots p_r^{\max\{m_r,n_r\}}$ como se quería probar. □

De la demostración de la proposición anterior se deduce inmediatamente el resultado siguiente:

Corolario 4.6.13. (Mcm y múltiplos comunes.)

Sean $a, b \in \mathbb{Z}$, no ambos nulos y sea $m \in \mathbb{Z}$, con $m \neq 0$. Entonces

$$a \mid m \quad y \quad b \mid m \iff [a : b] \mid m.$$

Ejemplo: Observemos que para $a = 2^2 \cdot 3^1 \cdot 7^2$ y $b = 2^1 \cdot 5^2 \cdot 7^3 \cdot 11^1$, teníamos $(a : b) = 2^1 \cdot 7^2$ y $[a : b] = 2^2 \cdot 3^1 \cdot 5^2 \cdot 7^3 \cdot 11^1$. Luego

$$\begin{aligned}(a : b) \cdot [a : b] &= (2^1 \cdot 7^2) \cdot (2^2 \cdot 3^1 \cdot 5^2 \cdot 7^3 \cdot 11^1) \\ &= 2^{1+2} \cdot 3^{0+1} \cdot 5^{0+2} \cdot 7^{2+3} \cdot 11^{0+1} \\ &= 2^{2+1} \cdot 3^{1+0} \cdot 5^{0+2} \cdot 7^{2+3} \cdot 11^{0+1} \\ &= (2^2 \cdot 3^1 \cdot 7^2) \cdot (2^1 \cdot 5^2 \cdot 7^3 \cdot 11^1) \;=\; a \cdot b.\end{aligned}$$

Es inmediato probar que este resultado vale en general.

Proposición 4.6.14. (Producto mcd y mcm.)

Sean $a, b \in \mathbb{Z}$, no nulos, entonces $|a \cdot b| = (a : b) \cdot [a : b]$.

En particular, si $a \perp b$, entonces $[a : b] = |a \cdot b|$.

Esto da una alternativa para calcular el mínimo común múltiplo cuando uno no conoce la factorización de los números. De hecho esta forma de calcular el mínimo común múltiplo es para números grandes más veloz que factorizar los números para luego aplicar la Proposición 4.6.14, ya que calcular el máximo común divisor por el algoritmo de Euclides es para números grandes más veloz que factorizar.

Ejemplo: Determinar todos los pares de números $a, b \in \mathbb{N}$ que satisfacen que

$$(a : b) = 2^2 \cdot 3 \cdot 17 \quad \text{y} \quad [a : b] = 2^5 \cdot 3 \cdot 5^2 \cdot 17^2.$$

¡Nunca olvidar que "coprimizar" en general ayuda!

Sabemos que $a = (a : b)\, a'$ y $b = (a : b)\, b'$ con $a' \perp b'$. Luego

$$(a : b)[a : b] = a\, b = (a : b)^2 a'\, b'.$$

Es decir

$$a'b' = \frac{[a : b]}{(a : b)} = \frac{2^5 \cdot 3 \cdot 5^2 \cdot 17^2}{2^2 \cdot 3 \cdot 17} = 2^3 \cdot 5^2 \cdot 17, \text{ con } a' \perp b'.$$

Al ser $a' \perp b'$ no puede aparecer un mismo primo simultáneamente en a' y b', y por lo tanto las posibilidades son (eligiendo cuáles son los primos que aparecen en a' y luego los restantes estarán en b'):

$$\begin{array}{ll} a' = 1,\ b' = 2^3 \cdot 5^2 \cdot 17 & a' = 2^3,\ b' = 5^2 \cdot 17 \\ a' = 5^2,\ b' = 2^3 \cdot 17 & a' = 17,\ b' = 2^3 \cdot 5^2 \\ a' = 2^3 \cdot 5^2,\ b' = 17 & a' = 2^3 \cdot 17,\ b' = 5^2 \\ a' = 5^2 \cdot 17,\ b' = 2^3 & a' = 2^3 \cdot 5^2 \cdot 17,\ b' = 1. \end{array}$$

Multiplicando estos números por $(a : b) = 2^2 \cdot 3 \cdot 17$ se obtienen todos los pares (a, b).

Terminemos este capítulo mencionando una famosa y clásica conjetura sobre primos, la *conjetura de los primos gemelos*, y los recientes avances sobre el tema. Se dice que dos números primos son gemelos si difieren en 2, como por ejemplo 41 y 43. La conjetura, aún no resuelta, afirma que existen infinitos pares de primos gemelos.

En Abril 2013, el matemático chino-americano Yitang Zhang anunció el resultado cercano más relacionado en algún sentido con esta conjetura, ya que también se trata de diferencias entre primos: Zhang anunció que existen infinitos pares de primos, no gemelos, pero que difieren en menos de 70 millones.

A partir del resultado de Zhang, se ha promovido una carrera para reducir esa diferencia: en Abril 2014 la brecha llegó a 246. Es decir hoy en día se sabe que existen infinitos pares de primos que difieren en menos de 246. Más aún, asumiendo como verdaderas ciertas conjeturas, se puede probar que la brecha se reduce a 6. Los avances aparecen en la página
http://michaelnielsen.org/polymath1/index.php?title=Bounded_gaps_between_primes

Pero la conjetura de los primos gemelos sigue abierta...

4.7 Apéndice

La construcción del conjunto de números enteros $\mathbb{Z}$ se puede formalizar definiéndolo como el conjunto de clases de equivalencia de la relación de equivalencia $\sim$ en $\mathbb{N}\times\mathbb{N}$ dada por:

$$(a,b)\sim(c,d) \iff a+d=b+c,\ \forall\,(a,b),(c,d)\in\mathbb{N}\times\mathbb{N}.$$

Es fácil verificar que ésta es una relación de equivalencia en $\mathbb{N}\times\mathbb{N}$.

La motivación de que las clases de equivalencia de esta relación dan el conjunto que conocemos como el conjunto de números enteros $\mathbb{Z}$ proviene de que $a+d=b+c$ es lo mismo que decir (en $\mathbb{Z}$) que $a-b=c-d$, y por ejemplo se puede pensar en el $-2=4-6$ como el par $(4,6)\in\mathbb{N}\times\mathbb{N}$, pero también como el par $(5,7)$, ya que $-2=5-7$ también, o como cualquier par $(n,n+2)$ con $n\in\mathbb{N}$. Del mismo modo el número entero $0=n-n$ se corresponde con cualquier par (n,n), $n\in\mathbb{Z}$. Así, se tiene

- $\overline{(1,1)}=\{(n,n),\ n\in\mathbb{N}\}\underset{\text{def}}{=}0\in\mathbb{Z}$
- $\overline{(m+1,1)}=\{(m+n+1,n+1),\ n\in\mathbb{N}\}\underset{\text{def}}{=}m\in\mathbb{Z},\ \forall\, m\in\mathbb{N}$
- $\overline{(1,m+1)}=\{(n+1,m+n+1),\ n\in\mathbb{N}\}\underset{\text{def}}{=}-m\in\mathbb{Z},\ \forall\, m\in\mathbb{N}.$

Con esta definición se puede probar que en $\mathbb{Z}$ valen las propiedades para la suma mencionadas al principio del capítulo.

4.8 Ejercicios.

Divisibilidad

1. Decidir cuáles de las siguientes afirmaciones son verdaderas $\forall\, a, b, c \in \mathbb{Z}$

   i) $a \cdot b \mid c \;\Rightarrow\; a \mid c$ y $b \mid c$
   ii) $4 \mid a^2 \;\Rightarrow\; 2 \mid a$
   iii) $2 \mid a \cdot b \;\Rightarrow\; 2 \mid a$ ó $2 \mid b$
   iv) $9 \mid a \cdot b \;\Rightarrow\; 9 \mid a$ ó $9 \mid b$
   v) $a \mid b + c \;\Rightarrow\; a \mid b$ ó $a \mid c$
   vi) $a \mid c$ y $b \mid c \;\Rightarrow\; a \cdot b \mid c$
   vii) $a \mid b \;\Rightarrow\; a \leq b$
   viii) $a \mid b \;\Rightarrow\; |a| \leq |b|$
   ix) $a \mid b + a^2 \;\Rightarrow\; a \mid b$
   x) $a \mid b \;\Rightarrow\; a^n \mid b^n$, $\forall\, n \in \mathbb{N}$

2. Hallar todos los $n \in \mathbb{N}$ tales que

   i) $3n - 1 \mid n + 7$
   ii) $3n - 2 \mid 5n - 8$
   iii) $2n + 1 \mid n^2 + 5$
   iv) $n - 2 \mid n^3 - 8$

3. Sean $a, b \in \mathbb{Z}$.

   i) Probar que $a - b \mid a^n - b^n$ para todo $n \in \mathbb{N}$ y $a \neq b \in \mathbb{Z}$.
   ii) Probar que si n es un número natural par y $a \neq -b$, entonces $a + b \mid a^n - b^n$.
   iii) Probar que si n es un número natural impar y $a \neq -b$, entonces $a + b \mid a^n + b^n$.

4. Sea a un entero impar. Probar que $2^{n+2} \mid a^{2^n} - 1$ para todo $n \in \mathbb{N}$.

5. Sea $n \in \mathbb{N}$.

   i) Probar que si n es compuesto, entonces $2^n - 1$ es compuesto.
   (Los primos de la forma $2^p - 1$ para p primo se llaman *primos de Mersenne*, por Marin Mersenne, monje y filósofo francés, 1588-1648. Se conjetura que existen infinitos primos de Mersenne, pero aún no se sabe. Se conocen a la fecha 51 primos de Mersenne (Enero 2021). El más grande producido hasta ahora es $2^{82.589.933} - 1$, que tiene 24.862.048 dígitos, y es el número primo más grande conocido a la fecha.)
   ii) Probar que si $2^n + 1$ es primo, entonces n es una potencia de 2.
   (Los números de la forma $\mathcal{F}_n = 2^{2^n} + 1$ se llaman *números de Fermat*, por Pierre de Fermat, juez y matemático francés, 1601-1665. Fermat conjeturó que cualquiera sea $n \in \mathbb{N}_0$, $\mathcal{F}_n$

era primo, pero esto resultó falso: los primeros $\mathcal{F}_0 = 3$, $\mathcal{F}_1 = 5$, $\mathcal{F}_2 = 17$, $\mathcal{F}_3 = 257$, $\mathcal{F}_4 = 65537$, son todos primos, pero $\mathcal{F}_5 = 4294967297 = 641 \times 6700417$. Hasta ahora no se conocen más primos de Fermat que los 5 primeros mencionados.)

6. i) Probar que el producto de n números naturales consecutivos es divisible por $n!$.

   ii) Probar que $\binom{2n}{n}$ es divisible por 2.

7. Probar que las siguientes afirmaciones son verdaderas para todo $n \in \mathbb{N}$

   i) $99 \mid 10^{2n} + 197$

   ii) $9 \mid 7 \cdot 5^{2n} + 2^{4n+1}$

   iii) $56 \mid 13^{2n} + 28n^2 - 84n - 1$

   iv) $256 \mid 7^{2n} + 208n - 1$

Algoritmo de División

8. Calcular el cociente y el resto de la división de a por b en los casos

   i) $a = 133\,,\ b = -14$

   ii) $a = 13\,,\ b = 111$

   iii) $a = 3b + 7\,,\ b \neq 0$

   iv) $a = b^2 - 6\,,\ b \neq 0$

   v) $a = n^2 + 5\,,\ b = n + 2\,,\ n \in \mathbb{N}$

   vi) $a = n + 3\,,\ b = n^2 + 1\,,\ n \in \mathbb{N}$

9. Sabiendo que el resto de la división de un entero a por 18 es 5, calcular el resto de la división de

   i) la división de $a^2 - 3a + 11$ por 18.

   ii) la división de a por 3.

   iii) la división de $4a + 1$ por 9.

   iv) la división de $7a^2 + 12$ por 28

10. i) Si $a \equiv 22\ (14)$, hallar el resto de dividir a a por 14, por 2 y por 7.

    ii) Si $a \equiv 13\ (5)$, hallar el resto de dividir a $33a^3 + 3a^2 - 197a + 2$ por 5.

    iii) Hallar, para cada $n \in \mathbb{N}$, el resto de la división de $\sum_{i=1}^{n} (-1)^i \cdot i!$ por 12.

11. i) Probar que $a^2 \equiv -1\ (5) \Leftrightarrow a \equiv 2\ (5)$ ó $a \equiv 3\ (5)$.

    ii) Probar que no existe ningún entero a tal que $a^3 \equiv -3\ (7)$.

iii) Probar que $a^7 \equiv a\ (7)$ para todo $a \in \mathbb{Z}$.

iv) Probar que $7 \mid a^2 + b^2 \Leftrightarrow 7 \mid a$ y $7 \mid b$.

v) Probar que $5 \mid a^2+b^2+1 \Rightarrow 5 \mid a$ ó $5 \mid b$. ¿Vale la implicación recíproca?

12. i) Probar que $2^{5k} \equiv 1\ (31)$ para todo $k \in \mathbb{N}$.

ii) Hallar el resto de la división de 2^{51833} por 31.

iii) Sea $k \in \mathbb{N}$. Sabiendo que $2^k \equiv 39\ (31)$, hallar el resto de la división de k por 5.

iv) Hallar el resto de la división de $43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999}$ por 31.

13. Se define por recurrencia la sucesión $(a_n)_{n\in\mathbb{N}}$:

$a_1 = 3,\ a_2 = -5$ y $a_{n+2} = a_{n+1} - 6^{2n} \cdot a_n + 21^n \cdot n^{21}$ para todo $n \in \mathbb{N}$.

Probar que $a_n \equiv 3^n (\text{mod } 7)$ para todo $n \in \mathbb{N}$.

Sistemas de numeración

14. (a) Hallar el desarrollo en base 2 de

i) 1365

ii) 2800

iii) $3 \cdot 2^{13}$

iv) $13 \cdot 2^n + 5 \cdot 2^{n-1}$

(b) Hallar el desarrollo en base 16 de 2800.

15. Sea $a = (a_d a_{d-1} \dots a_1 a_0)_2$ un número escrito en base 2 (o sea escrito en bits). Determinar simplemente cómo son las escrituras en base 2 del número $2a$ y del número $a/2$ cuando a es par, o sea las operaciones "multiplicar por 2" y "dividir por 2" cuando se puede. Esas operaciones se llaman *shift* en inglés, o sea corrimiento, y son operaciones que una computadora hace en forma sencilla.

16. Enunciar y demostrar criterios de divisibilidad por 8 y por 9.

17. i) Sea $k \in \mathbb{N}$, $k = (aaaa)_7$. Probar que $8 \mid k$.

ii) Sea $k \in \mathbb{N}$, $k = (\underbrace{a \dots a}_{d})_7$. Determinar para qué valores de $d \in \mathbb{N}$ se tiene que $8 \mid k$.

Máximo común divisor

18. En cada uno de los siguientes casos calcular el máximo común divisor entre a y b y escribirlo como combinación lineal entera de a y b:

i) $a = 2532\,,\ b = 63$
ii) $a = 131\,,\ b = 23$
iii) $a = n^4 - 3\,,\ b = n^2 + 2\ ,\ n \in \mathbb{N}\,.$

19. Sean $a, b \in \mathbb{Z}$. Sabiendo que el resto de dividir a a por b es 27 y que el resto de dividir b por 27 es 21, calcular $(a : b)$.

20. Sea $a \in \mathbb{Z}$.

    i) Probar que $(5a+8 : 7a+3) = 1$ o 41. Exhibir un valor de a para el cual da 1, y verificar que efectivamente para $a = 23$ da 41.

    ii) Probar que $(2a^2 + 3a - 1 : 5a + 6) = 1$ o 43. Exhibir un valor de a para el cual da 1, y verificar que efectivamente para $a = 16$ da 41.

    iii) Probar que $(a^2 - 3a + 2 : 3a^3 - 5a^2) = 2$ ó 4, y exhibir un valor de a para cada caso.
    (Para este ítem es **indispensable** mostrar que el máximo común divisor nunca puede ser 1).

21. Sean $a, b \in \mathbb{Z}$ coprimos. Probar que $7a - 3b$ y $2a - b$ son coprimos.

22. Sean $a, b \in \mathbb{Z}$ con $(a : b) = 2$. Probar que los valores posibles para $(7a + 3b : 4a - 5b)$ son 2 y 94. Exhibir valores de a y b para los cuales da 2 y para los cuales da 94.

23. i) Determinar todos los $a, b \in \mathbb{Z}$ coprimos tales que $\dfrac{b+4}{a} + \dfrac{5}{b} \in \mathbb{Z}$.

    ii) Determinar todos los $a, b \in \mathbb{Z}$ coprimos tales que $\dfrac{9a}{b} + \dfrac{7a^2}{b^2} \in \mathbb{Z}$.

    iii) Determinar todos los $a \in \mathbb{Z}$ tales que $\dfrac{2a+3}{a+1} + \dfrac{a+2}{4} \in \mathbb{Z}$.

Primos y factorización

24. Probar que existen infinitos primos congruentes a 3 módulo 4.
Sugerencia: probar primero que si $a \neq \pm 1$ satisface $a \equiv 3 \pmod 4$, entonces existe p primo, $p \equiv 3 \pmod 4$ tal que $p \,|\, a$. Luego probar que si existieran sólo finitos primos congruentes a 3 módulo 4, digamos $p_1, p_2, \ldots, p_n$, entonces $a = -1 + 4\prod_{i=1}^{n} p_i$ sería un entero distinto de 1 y -1 que no es divisible por ningún primo congruente a 3 módulo 4.

25. Sea p primo positivo.

    i) Probar que si $0 < k < p$, entonces $p \mid \binom{p}{k}$.

    ii) Probar que si $a, b \in \mathbb{Z}$, entonces $(a+b)^p \equiv a^p + b^p \pmod{p}$.

26. Decidir si existen enteros a y b no nulos que satisfagan

    i) $a^2 = 3b^3$ ii) $7a^2 = 8b^2$.

27. Sea $n \in \mathbb{N}$, $n \geq 2$. Probar que si p es un primo positivo entonces $\sqrt[n]{p} \notin \mathbb{Q}$.

28. Sean p y q primos positivos distintos y sea $n \in \mathbb{N}$. Probar que si $pq \mid a^n$ entonces $pq \mid a$.

29. Determinar cuántos divisores positivos tienen 9000, $15^4 \cdot 42^3 \cdot 56^5$ y $10^n \cdot 11^{n+1}$. ¿ Y cuántos divisores en total ?

30. Hallar la suma de los divisores positivos de $2^4 \cdot 5^{123}$ y de $10^n \cdot 11^{n+1}$.

31. Hallar el menor número natural n tal que $6552\,n$ sea un cuadrado (es decir que exista $k \in \mathbb{N}$ tal que $6552\,n = k^2$).

32. Sean $a, b \in \mathbb{Z}$, $a, b \geq 2$. Probar que si ab es un cuadrado en $\mathbb{Z}$ y $(a : b) = 1$, entonces tanto a como b son cuadrados en $\mathbb{Z}$.

33. Hallar todos los $n \in \mathbb{N}$ tales que

    i) $(n : 945) = 63$, $(n : 1176) = 84$ y $n \leq 2800$

    ii) $(n : 1260) = 70$ y n tiene 30 divisores positivos.

34. Hallar el menor número natural n tal que $(n : 3150) = 45$ y n tenga exactamente 12 divisores positivos.

35. i) Sea $k \in \mathbb{N}$. Probar que $(2^k + 7^k : 2^k - 7^k) = 1$,

    ii) Sea $k \in \mathbb{N}$. Probar que $(2^k + 5^{k+1} : 2^{k+1} + 5^k) = 3$ ó 9, y dar un ejemplo para cada caso.

    iii) Caracterizar para cada $k \in \mathbb{N}$ el valor que toma $(12^k - 1 : 12^k + 1286$.

36. Sean $a, b \in \mathbb{Z}$. Probar que si $(a : b) = 1$ entonces $(a^2 \cdot b^3 : a + b) = 1$.

37. Sean $a, b \in \mathbb{Z}$ tales que $(a : b) = 5$.

    i) Calcular los posibles valores de $(ab : 5a - 10b)$ y dar un ejemplo para cada uno de ellos.

ii) Para cada $k \in \mathbb{N}$, calcular $(a^{k-1}b : a^k + b^k)$.

38. i) Sean $a, b \in \mathbb{Z}$ tales que $(a : b) = 3$. Calcular los posibles valores de $(a^2 + 15b + 57 : 4050)$ y dar un ejemplo para cada caso.

ii) Sean $a, b \in \mathbb{Z}$. Sabiendo que $b \equiv 6 \pmod{24}$ y que $(a : b) = 13$, calcular $(5a^2 + 11b + 117 : 624)$.

39. Hallar todos los $n \in \mathbb{N}$ tales que

i) $[n : 130] = 260$.

ii) $[n : 420] = 7560$.

40. Hallar todos los $a, b \in \mathbb{Z}$ tales que

i) $(a : b) = 10$ y $[a : b] = 1500$

ii) $3 \mid a$, $(a : b) = 20$ y $[a : b] = 9000$

Capítulo 5

Enteros – Segunda parte.

5.1 Ecuaciones lineales diofánticas.

Vamos a aplicar ahora la teoría del máximo común divisor que vimos a la resolución de ciertas ecuaciones en enteros, que se llaman *Ecuaciones lineales diofánticas*. Las ecuaciones diofánticas son las ecuaciones con coeficientes enteros de las cuales se buscan las soluciones enteras.

El nombre se puso por *Diofanto de Alejandría*, $\sim$200–284, quién fue quién desarrolló ese tipo de ecuaciones en su obra *La Aritmética*.

Las ecuaciones diofánticas más sencillas son las ecuaciones lineales de la forma $a \cdot X + b \cdot Y = c$ con $a, b, c \in \mathbb{Z}$, donde a y b no son ambos nulos, de las cuales se buscan los pares de soluciones *enteras*. Observemos que una ecuación de este tipo es la ecuación de una recta en $\mathbb{R}^2$, que sabemos resolver en $\mathbb{R}^2$, y que nos estamos preguntando por qué puntos de coordenadas ambas enteras pasa esa recta.

El problema es entonces el siguiente: encontrar todos los pares $(x, y) \in \mathbb{Z}^2$ que son solución de la ecuación

$$a \cdot X + b \cdot Y = c,$$

donde a, b, c son enteros dados, a, b no ambos nulos.

Como primer paso queremos decidir si existe al menos una solución entera $(x_0, y_0) \in \mathbb{Z}^2$.

Observación 5.1.1. Si $a = 0$ o $b = 0$ (pongamos $b = 0$), el problema se vuelve un problema de divisibilidad: $a \cdot X + 0 \cdot Y = c$ tiene solución entera si y solo si $a \mid c$, y en ese caso las soluciones son todos los pares $(c/a, j)$, $j \in \mathbb{Z}$. Luego en lo que sigue podemos suponer que a y b son ambos no nulos.

Ejemplos:

- $5\,X + 9\,Y = 1$ tiene por ejemplo como solución entera $x_0 = 2\,,\ y_0 = -1\,.$
- $5\,X + 9\,Y = 10$ tiene como solución entera $x_0 = 2\,,\ y_0 = 0$ pero también tiene como solución entera, usando el ejemplo anterior, $x_0 = 10 \cdot 2 = 20\,,\ y_0 = -1 \cdot 10 = -10\,.$
- $4\,X + 6\,Y = 7$ no tiene solución entera porque el resultado de lo de la izquierda es claramente siempre par. De hecho recordamos que si un número se escribe como combinación entera de a y b, entonces tiene que ser un múltiplo de $(a : b)\,.$
- $4\,X + 6\,Y = 2$ tiene solución ya que $2 = (4 : 6)$ y sabemos que el mcd es combinación entera de los números. Se puede elegir aquí $x_0 = -1,\ y_0 = 1\,.$
- $18\,X - 12\,Y = 2$ no tiene solución entera pues $(18 : 12) = 6$ y $6 \nmid 2\,.$
- $18\,X - 12\,Y = 60$ tiene solución pues $(18 : 12) \mid 60$: por ejemplo escribimos $6 = 18{\cdot}1 - 12{\cdot}1$ y así obtenemos $60 = 10{\cdot}6 = 18{\cdot}10 - 12{\cdot}10\,,$ es decir $x_0 = 10,\ y_0 = 10\,.$

Deducimos la siguiente afirmación:

Proposición 5.1.2. (Ecuación diofántica y máximo común divisor.)

Sean $a, b, c \in \mathbb{Z}$ con a, b no nulos. La ecuación diofántica

$$a\,X + b\,Y = c$$

admite soluciones enteras si y solo si $(a : b) \mid c\,.$ Es decir:

$$\exists\ (x_0, y_0) \in \mathbb{Z}^2 :\ a\,x_0 + b\,y_0 = c \iff (a : b) \mid c.$$

Demostración.

- $(\Rightarrow)$ Sea $(x_0, y_0) \in \mathbb{Z}^2$ una solución entera, entonces, como siempre, dado que $(a : b) \mid a$ y $(a : b) \mid b\,,$ se concluye que $(a : b) \mid a\,x_0 + b\,y_0 = c\,,$ es decir, $(a : b) \mid c\,.$
- $(\Leftarrow)$ Sabemos que existen $s, t \in \mathbb{Z}$ tales que $(a : b) = s\,a + t\,b\,.$ Luego, dado que $(a : b) \mid c\,,$ existe $k \in \mathbb{Z}$ tal que $c = k\,(a : b)\,,$ y por lo tanto se tiene que $c = a\,(k\,s) + b\,(k\,t)\,.$ Podemos tomar $x_0 := k\,s,\ y_0 := k\,t\,.$

□

Como $1 \mid c\,,\ \forall\, c \in \mathbb{Z}\,,$ se obtiene inmediatamente el corolario siguiente.

Corolario 5.1.3. (Ecuación diofántica con a y b coprimos.)

Sean $a, b \in \mathbb{Z}$ *no nulos y* coprimos. *Entonces la ecuación diofántica*

$$a\,X + b\,Y = c$$

tiene soluciones enteras, para todo $c \in \mathbb{Z}$.

La Proposición 5.1.2 da además una forma de conseguir una solución (x_0, y_0) particular (si existe): cuando no se consigue a ojo o fácilmente, podemos aplicar el algoritmo de Euclides para escribir el mcd como combinación entera. Y luego de allí obtener la combinación entera que da c como en la demostración anterior. Pero siempre es más fácil trabajar directamente con la ecuación *"coprimizada"*, como veremos en lo que sigue.

Antes introducimos la definición-notación siguiente que adoptamos en estas notas:

Definición-Notación 5.1.4. (Ecuaciones diofánticas equivalentes.)

Sean $a \cdot X + b \cdot Y = c$ y $a' \cdot X + b' \cdot Y = c'$ dos ecuaciones diofánticas. Decimos que son *equivalentes* si tienen exactamente las mismas soluciones $(x, y) \in \mathbb{Z}^2$. En ese caso adoptamos la notación

$$a \cdot X + b \cdot Y = c \;\leftrightsquigarrow\; a' \cdot X + b' \cdot Y = c'.$$

Observación 5.1.5. (Ecuación diofántica y ecuación "coprimizada".)

Sean $a, b, c \in \mathbb{Z}$ con a, b no nulos tales que $(a : b) \mid c$.
Definamos $a' = \dfrac{a}{(a : b)}$, $b' = \dfrac{b}{(a : b)}$ y $c' = \dfrac{c}{(a : b)}$. Entonces,

$$a \cdot X + b \cdot Y = c \;\leftrightsquigarrow\; a' \cdot X + b' \cdot Y = c'.$$

Demostración. Cuando $(a : b) \mid c$, es claro que $\forall\,(x, y) \in \mathbb{Z}^2$, $ax + by = c \Leftrightarrow a'x + b'y = c'$. Luego las dos ecuaciones tiene exactamente las mismas soluciones. □

Siempre resulta más simple hacer este proceso de "coprimización" de entrada para encontrar una solución particular: se escribe el 1 como combinación entera de a' y b': $1 = sa' + tb'$ y luego haciendo $c' = c'sa' + c'tb'$ se obtiene por ejemplo $x_0 = c's$ e $y_0 = c't$.

El paso siguiente es encontrar todas las soluciones enteras de una ecuación diofántica que admite al menos una solución entera.

Vamos a tratar primero en detalle un caso particular, el caso $c = 0$, es decir el caso de una ecuación diofántica de tipo

$$a \cdot X + b \cdot Y = 0$$

que siempre tiene solución pues $(a : b) \mid 0$ independientemente de quién es $(a : b)$. Miramos primero un ejemplo.

Ejemplo: Soluciones enteras de $18\,X + 27\,Y = 0$:

La solución más simple es $x_0 = 0, y_0 = 0$. O también se tiene $x_1 = 27, y_1 = -18$. Así que la solución no es única. También por ejemplo $x_2 = -27, y_2 = 18$ o $x_3 = 3, y_3 = -2$ sirven. Vamos a probar que son infinitas. ¿ Cómo se consiguen todas ?

Por lo mencionado arriba, la ecuación original es equivalente a la ecuación "coprimizada":

$$18\,X + 27\,Y = 0 \quad \leftrightsquigarrow \quad 2\,X + 3\,Y = 0.$$

Ahora bien, sea $(x, y) \in \mathbb{Z}^2$ solución:

$$\begin{aligned} 2\,x + 3\,y = 0 \quad &\iff \quad 2\,x = -3\,y \\ &\implies \quad 2 \mid 3\,y \ \text{ y } \ 3 \mid 2\,x \\ &\implies \quad 2 \mid y \ \ (\text{pues } 2 \perp 3) \ \text{ y } \ 3 \mid x \ (\text{pues } 3 \perp 2) \\ &\implies \quad y = 2\,j \ \text{ y } \ x = 3\,k. \end{aligned}$$

Volviendo al primer renglón, resulta:

$$2\,(3\,k) = -3\,(2\,j) \implies j = -k.$$

Es decir: $x = 3\,k$ e $y = -2\,k$ para algún $k \in \mathbb{Z}$.

Hemos probado: (x, y) solución entera $\implies$ existe $k \in \mathbb{Z}$ tal que $x = 3\,k$ e $y = -2\,k$.

Verifiquemos la recíproca: Si $x = 3\,k$ e $y = -2\,k$ para el mismo $k \in \mathbb{Z}$, entonces (x, y) es solución de la ecuación. Efectivamente, se tiene $2\,x + 3\,y = 2\,(3\,k) + 3\,(-2\,k) = 0$.

Luego, hemos probado que el conjunto de soluciones enteras de esta ecuación es el conjunto:

$$\mathcal{S}_0 = \{\ (x, y) : x = 3\,k,\ y = -2\,k;\ k \in \mathbb{Z}\ \}.$$

(Observemos que si nos olvidamos de coprimizar la ecuación y nos quedamos, usando la misma estructura, con las soluciones de tipo $x = 27\,k$, $y = -18\,k$, $k \in \mathbb{Z}$, perdemos soluciones ya que se nos escapa por ejemplo la solución de antes $x_3 = 3$, $y_3 = -2$.)

Este procedimiento se puede generalizar sin problemas:

Proposición 5.1.6. (La ecuación diofántica $a \cdot X + b \cdot Y = 0$.)

Sean $a, b \in \mathbb{Z}$, no nulos.

El conjunto $\mathcal{S}_0$ de soluciones enteras de la ecuación diofántica $a \cdot X + b \cdot Y = 0$ es

$$\mathcal{S}_0 = \{ (x, y) : x = b'k,\ y = -a'k,\ k \in \mathbb{Z} \},\ \textit{donde}\ a' := \frac{a}{(a : b)}\ \textit{y}\ b' := \frac{b'}{(a : b)}.$$

Demostración. Se tiene

$$a\,X + b\,Y = 0 \quad \leftrightsquigarrow \quad a'X + b'Y = 0,$$

donde $a' = a/(a : b)$ y $b' = b/(a : b)$ son coprimos.

Ahora bien, sea $(x, y) \in \mathbb{Z}^2$ solución:

$$\begin{aligned} a'\,x + b'\,y = 0 \quad &\iff \quad a'\,x = -b'\,y \\ &\implies \quad a' \mid b'\,y \quad \text{y} \quad b' \mid a'\,x \\ &\underset{a' \perp b'}{\implies} \quad a' \mid y \quad \text{y} \quad b' \mid x \\ &\implies \quad \exists\, j, k \in \mathbb{Z} :\ y = j\,a' \ \text{ y } \ x = k\,b'. \end{aligned}$$

Volviendo al primer renglón, resulta:

$$a'\,(k\,b') = -b'\,(j\,a') \implies j = -k.$$

Es decir: $x = b'\,k$ e $y = -a'\,k$ para algún $k \in \mathbb{Z}$.

Hemos probado: (x, y) solución entera $\implies$ existe $k \in \mathbb{Z}$ tal que $x = b'\,k$ e $y = -a'\,k$.

Verifiquemos la recíproca: Si $x = b'\,k$ e $y = -a'\,k$ para el mismo $k \in \mathbb{Z}$, entonces (x, y) es solución de la ecuación. Efectivamente, se tiene $a'\,x + b'\,y = a'\,(b'\,k) + b'\,(-a'\,k) = 0$. □

La resolución completa de este caso particular nos sirve para resolver completamente una ecuación lineal diofántica arbitraria.

Teorema 5.1.7. (La ecuación diofántica $a \cdot X + b \cdot Y = c$.)

Sean $a, b, c \in \mathbb{Z}$, con a, b no nulos.

El conjunto $\mathcal{S}$ de soluciones enteras de la ecuación diofántica $a \cdot X + b \cdot Y = c$ es:

- $\mathcal{S} = \emptyset$ *cuando* $(a : b) \nmid c$.

- $\mathcal{S} = \{\ (x,y) : x = x_0 + b'k,\ y = y_0 - a'k;\ k \in \mathbb{Z}\ \}$, *donde* (x_0, y_0) *es una solución particular cualquiera de la ecuación y* $a' := \dfrac{a}{(a:b)}$, $b' := \dfrac{b}{(a:b)}$ *cuando* $(a:b) \mid c$.

Demostración. Sabemos que si $(a:b) \nmid c$, la ecuación no admite solución, luego $\mathcal{S} = \emptyset$ en ese caso. Cuando $(a:b) \mid c$, tenemos al menos una solución particular $(x_0, y_0) \in \mathbb{Z}^2$ de la ecuación, es decir $a\,x_0 + b\,y_0 = c$. Sea ahora $(x,y) \in \mathbb{Z}^2$ una solución cualquiera. Se tiene

$$a\,x + b\,y = c \iff a\,x + b\,y = a\,x_0 + b\,y_0 \iff a\,(x - x_0) + b\,(y - y_0) = 0.$$

Es decir (x,y) es solución de $a\,X + b\,Y = c$ si y solo si $(x - x_0, y - y_0)$ es solución de $a\,X + b\,Y = 0$, es decir, por la Proposición 5.1.6, si y solo si existe $k \in \mathbb{Z}$ tal que

$$x - x_0 = b'\,k,\ y - y_0 = -a'\,k, \quad \text{o sea} \quad x = x_0 + b'\,k,\ y = y_0 - a'\,k.$$

□

Resumimos el algoritmo que se obtiene a partir del Teorema 5.1.7 en el cuadro siguiente:

Resolución completa de la ecuación diofántica $a\,X + b\,Y = c$

1. ¿ Tiene solución la ecuación ?
   (a) **no** cuando $(a:b) \nmid c$. En ese caso $\mathcal{S} = \emptyset$.
   (b) **sí** cuando $(a:b) \mid c$. En ese caso:
2. "Coprimizo" la ecuación:
$$a'\,X + b'\,Y = c', \ \text{ con } a' := \frac{a}{(a:b)},\ b' := \frac{b}{(a:b)} \ \text{ y } \ c' := \frac{c}{(a:b)}.$$
3. Busco una solución particular $(x_0, y_0) \in \mathbb{Z}^2$ (a ojo o aplicando el algoritmo de Euclides).
4. Todas las soluciones son:
$$\mathcal{S} = \{\ (x,y) : x = x_0 + b'k,\ y = y_0 - a'k;\ k \in \mathbb{Z}\ \}.$$

Ejemplos:

- Soluciones enteras de $18\,X + 27\,Y = -90$:
  Hay soluciones pues $(18 : 27) = 9 \mid -90$.
  "Coprimizo": $2\,X + 3\,Y = -10$.
  Solución particular: $(x_0, y_0) := (-5, 0)$.
  Entonces $\mathcal{S} = \{\,(x, y) :\ x = -5 + 3k,\ y = -2k,\ k \in \mathbb{Z}\,\}$.

- Soluciones *naturales* de $175\,X + 275\,Y = 3000$:
  Hay soluciones enteras pues $(175 : 275) = 25 \mid 3000$.
  "Coprimizo": $\dfrac{175}{25}\,X + \dfrac{275}{25}\,Y = \dfrac{3000}{25}$, i.e. $7\,X + 11\,Y = 120$.
  Solución particular?

$$
\begin{aligned}
& 11 = 1 \cdot 7 + 4,\ 7 = 1 \cdot 4 + 3,\ 4 = 1 \cdot 3 + 1 \\
\Rightarrow\ & 1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2 \cdot (11 - 7) - 7 = 2 \cdot 11 - 3 \cdot 7 \\
\Rightarrow\ & 1 = 7 \cdot (-3) + 11 \cdot 2 \\
\Rightarrow\ & 120 = 7 \cdot (-3 \cdot 120) + 11 \cdot (2 \cdot 120) \ =\ 7 \cdot (-360) + 11 \cdot 240 \\
\Rightarrow\ & (x_0, y_0) = (-360, 240).
\end{aligned}
$$

  Soluciones enteras: $x = -360 + 11\,k,\ y = 240 - 7\,k,\ k \in \mathbb{Z}$.
  Soluciones naturales:

$$
\begin{aligned}
x > 0 \ \text{ e } \ y > 0 \ &\Longleftrightarrow\ -360 + 11\,k > 0 \ \text{ y } \ 240 - 7\,k > 0 \\
&\Longleftrightarrow\ 11\,k > 360 \ \text{ y } \ 240 > 7\,k \\
&\Longleftrightarrow\ k > (360/11) = 32,7... \ \text{ y } \ k < (240/7) = 34,2...
\end{aligned}
$$

  Por lo tanto $k \in \{33, 34\}$: hay dos pares de soluciones naturales, $x_1 := -360 + 11 \cdot 33 = 3$, $y_1 := 240 - 7 \cdot 33 = 9$ y $x_2 := -360 + 11 \cdot 34 = 14$, $y_2 := 240 - 7 \cdot 34 = 2$.
  Entonces $\mathcal{S}_{\mathbb{N}} = \{\,(3, 9),\ (14, 2)\,\}$.

5.2 Ecuaciones lineales de congruencia.

El analisis realizado para las ecuaciones diofánticas se aplica directamente a ciertas *ecuaciones lineales de congruencia*. Más especificamente, dado $m \in \mathbb{N}$, a las ecuaciones de la forma

$$a\,X \equiv c \pmod{m},$$

para $a, c \in \mathbb{Z}$.

Como en el caso de las ecuaciones diofánticas, vamos a adoptar en estas notas una definición-notación de ecuaciones lineales de congruencia equivalentes.

Definición-Notación 5.2.1. (Ecuaciones de congruencia equivalentes.)

Sean $a\,X \equiv c \pmod{m}$ y $a'\,X \equiv c' \pmod{m'}$ dos ecuaciones de congruencia. Decimos que son *equivalentes* si tienen exactamente las mismas soluciones $x \in \mathbb{Z}$. En ese caso adoptamos la notación

$$a\,X \equiv c \pmod{m} \iff a'\,X \equiv c' \pmod{m'}.$$

Veremos ahora que la ecuación de congruencia $a\,X \equiv c \pmod{m}$ tiene al menos una solución $x_0 \in \mathbb{Z}$ si y solo si la ecuación diofántica $a\,X - m\,Y = c$ admite al menos una solución $(x_0, y_0) \in \mathbb{Z}^2$, y por lo visto en el Teorema 5.1.7, esto es si y solo si $(a : -m) = (a : m) \mid c$.

Proposición 5.2.2. (Ecuación de congruencia, mcd y ecuación "coprimizada".)

Sea $m \in \mathbb{N}$. Dados $a, c \in \mathbb{Z}$, la ecuación de congruencia $a\,X \equiv c \pmod{m}$ tiene soluciones enteras si y solo si $(a : m) \mid c$.

Si ese es el caso, sean $a' := \dfrac{a}{(a : m)}$, $c' := \dfrac{c}{(a : m)}$ y $m' := \dfrac{m}{(a : m)}$. Entonces

$$\boldsymbol{a}\,X \equiv c \pmod{m} \iff a'X \equiv c' \pmod{m'}.$$

Para probar la segunda afirmación, es útil aislar la propiedad siguiente, que es inmediata y cuya demostración se deja a cargo del lector:

Observación 5.2.3. (Simplificando factores comunes en ecuación de congruencia-I.)

Sean $m' \in \mathbb{N}$ y $a', c', d \in \mathbb{Z}$ no nulos. Entonces,

$$\forall\, x \in \mathbb{Z}, \quad (d\,a')\,x \equiv d\,c' \ \big(\bmod (d\,m')\big) \iff a'\,x \equiv c' \pmod{m'}.$$

Demostración. (de la Proposición 5.2.2.)

Si $(a : m) \mid c$, entonces la ecuación diofántica $aX - mY = c$ admite al menos una solución particular $(x_0, y_0) \in \mathbb{Z}^2$. Es decir, $ax_0 - my_0 = c$, o equivalentemente $ax_0 - c = my_0$. Por lo tanto $m | ax_0 - c$, o lo que es lo mismo, $ax_0 \equiv c \pmod{m}$. Luego $x_0 \in \mathbb{Z}$ es una solución particular de la ecuación de congruencia $a\,X \equiv c \pmod{m}$.

Recíprocamente, si $x_0 \in \mathbb{Z}$ es una solución particular de la ecuación de congruencia $a\,X \equiv c \pmod{m}$, entonces existe $y_0 \in \mathbb{Z}$ tal que $ax_0 - c = my_0$, por lo cual la ecuación diofántica $aX - mY = c$ admite la solución particular $(x_0, y_0) \in \mathbb{Z}^2$. Por lo visto en la sección anterior, esta ecuación diofántica tiene solución si y sólo si $(a : -m) = (a : m) \mid c$.

Finalmente, cuando $(a : m) \mid c$, se aplica la Proposición 5.2.3 para para $d = (a : m)$, $a = da'$, $c = dc'$ y $m = dm'$: luego

$$\forall\, x \in \mathbb{Z}, \quad a\,x \equiv c \pmod{m} \iff a'\,x \equiv c' \pmod{m'}.$$

Es decir las dos ecuaciones de congruencia tienen exactamente las mismas soluciones. □

En particular, dado que si $(a : m) = 1$, entonces $(a : m) \mid c$, $\forall\, c \in \mathbb{Z}$, se obtiene:

Corolario 5.2.4. (Ecuación de congruencia con a y m coprimos.)

Sean $m \in \mathbb{N}$ y $a \in \mathbb{Z}$ tal que a y m son coprimos. *Entonces, la ecuación de congruencia $a\,X \equiv c \pmod{m}$ tiene soluciones enteras, cualquiera sea $c \in \mathbb{Z}$.*

El teorema siguiente describe todas las soluciones de una ecuación de congruencia.

Teorema 5.2.5. (La ecuación de congruencia $a\,X \equiv c \pmod{m}$.)

Sea $m \in \mathbb{N}$ y sean $a, c \in \mathbb{Z}$ con $a \neq 0$.

El conjunto $\mathcal{S}$ de soluciones enteras de la ecuación de congruencia

$$a\,X \equiv c \pmod{m}$$

es

- $\mathcal{S} = \emptyset$, *cuando* $(a : m) \nmid c$.
- $\mathcal{S} = \{x \in \mathbb{Z} : \ x \equiv x_0 \pmod{m'}\}$ *donde $x_0 \in \mathbb{Z}$ es una solución particular cualquiera de la ecuación $a\,X \equiv c \pmod{m}$ o de la ecuación equivalente $a'\,X \equiv c' \pmod{m'}$ donde $a' = \dfrac{a}{(a : m)}$, $c' = \dfrac{c}{(a : m)}$ y $m' = \dfrac{m}{(a : m)}$, cuando $(a : m) \mid c$, ya que*

  $$a\,X \equiv c \pmod{m} \quad \rightsquigarrow \quad X \equiv x_0 \pmod{m'}.$$

  Más aún, existe una única solución $x_0 \in \mathbb{Z}$ que satisface $0 \leq x_0 < m'$.

Demostración. Sabemos por la Proposición 5.2.2 que si $(a : m) \nmid c$, no hay solución, luego $\mathcal{S} = \emptyset$ en ese caso. Sea entonces el caso $(a : m) \mid c$. Tenemos que probar que

$$a\,X \equiv c \pmod{m} \quad \rightsquigarrow \quad X \equiv x_0 \pmod{m'}.$$

Pero ya sabemos que en ese caso,

$$a\,X \equiv c \pmod{m} \quad \leftrightsquigarrow \quad a'\,X \equiv c' \pmod{m'}.$$

Por lo tanto alcanza con probar que

$$a'\,X \equiv c' \pmod{m'} \quad \leftrightsquigarrow \quad X \equiv x_0 \pmod{m'},$$

o sea tienen las mismas soluciones enteras.

• Verifiquemos primero que si $x \in \mathbb{Z}$ es solución de la ecuación $X \equiv x_0 \pmod{m'}$, es decir satisface $x \equiv x_0 \pmod{m'}$, entonces es también solución de la ecuación $a'\,X \equiv c' \pmod{m'}$:

Se tiene que $x \equiv x_0 \pmod{m'}$ implica $a'\,x \equiv a'\,x_0 \pmod{m'}$. Como $x_0 \in \mathbb{Z}$ es una solución particular de la ecuación $a'\,X \equiv c' \pmod{m'}$, o sea vale $a'\,x_0 \equiv c' \pmod{m'}$, por transitividad se cumple $a'\,x \equiv c' \pmod{m'}$.

• Verifiquemos ahora que una solución x cualquiera de la ecuación $a'\,X \equiv c' \pmod{m'}$ es también solución de la ecuación $X \equiv x_0 \pmod{m'}$:

Si $x \in \mathbb{Z}$ es una solución cualquiera de la ecuación de congruencia $a'\,x \equiv c' \pmod{m'}$, entonces existe $y \in \mathbb{Z}$ tal que (x, y) es solución de la ecuación diofántica $a'\,X - m'\,Y = c'$. Por el Teorema 5.1.7, $x = x_0 + (-m')k$ e $y = y_0 - a'k$ donde (x_0, y_0) es una solución particular cualquiera de la ecuación diofántica y $k \in \mathbb{Z}$. En particular $m' \mid x - x_0$, es decir $x \equiv x_0 \pmod{m'}$ como se quería probar.

Para terminar, mostremos que hay una única solución x_0 con $0 \leq x_0 < m'$. Que existe es obvio pues si la solución encontrada x_0 no está en esas condiciones, se toma $r_{m'}(x_0)$ que satisface la misma ecuación de congruencia ya que $x_0 \equiv r_{m'}(x_0) \pmod{m'}$. Cualquier otra solución x satisface $x \equiv r_{m'}(x_0) \pmod{m'}$, y por lo tanto no puede haber otra solución $x \neq r_{m'}(x_0)$ con $0 \leq x < m'$. □

Antes de resumir el algoritmo que se obtiene a partir del Teorema 5.2.5, hagamos algunos ejemplos.

Ejemplos:

- La ecuación $9\,X \equiv 2 \pmod{15}$ no tiene solución pues $(9 : 15) \nmid 2$.
- La ecuación $9\,X \equiv 6 \pmod{15}$ tiene solución pues $(9 : 15) = 3 \mid 6$:

  $$9\,X \equiv 6 \pmod{15} \quad \leftrightsquigarrow \quad 3\,X \equiv 2 \pmod{5} \quad \leftrightsquigarrow \quad X \equiv 4 \pmod{5}.$$

  (Aquí, $x_0 := 4$ es una solución particular, pues $3{\cdot}4 = 12 \equiv 2 \pmod{5}$.)
  O sea $\mathcal{S} = \{\, x \in \mathbb{Z} :\ x \equiv 4 \pmod{5} \}$.

Si lo que buscamos es expresar todas las soluciones módulo 15 (el módulo correspondiente al planteo original) tenemos que fijarnos todos los números x_0 con $0 \leq x_0 < 15$ que satisfacen $x_0 \equiv 4 \pmod 5$, es decir $x_0 = 4 + 5\,k$ con $k \in \mathbb{Z}$ tales que $0 \leq x_0 < 15$. Estos son $4 = 4 + 0 \cdot 5$, $9 = 4 + 1 \cdot 5$ y $14 = 4 + 2 \cdot 5$. Así,

$$\begin{aligned}\mathcal{S} &= \{\, x \in \mathbb{Z} :\ x \equiv 4 \pmod 5\} \\ &= \{\, x \in \mathbb{Z} :\ x \equiv 4 \pmod{15} \ \text{ o } \ x \equiv 9 \pmod{15} \ \text{ o } x \equiv 14 \pmod{15}\}.\end{aligned}$$

- La ecuación $3\,X \equiv 2 \pmod 4$ tiene solución pues 3 y 4 son coprimos:

$$3\,X \equiv 2 \pmod 4 \quad \leftrightsquigarrow \quad X \equiv 2 \pmod 4.$$

  O sea $\mathcal{S} = \{\, x \in \mathbb{Z} :\ x \equiv 2 \pmod 4\}$.

- La ecuación $12\,X \equiv 6 \pmod{10}$ tiene solución pues $(12 : 10) = 2 \mid 6$. Pero es aún más fácil simplificar todo lo que se puede en la ecuación antes, como $12 \equiv 2 \pmod{10}$, se tiene:

$$12\,X \equiv 6 \pmod{10} \quad \leftrightsquigarrow \quad 2\,X \equiv 6 \pmod{10} \quad \leftrightsquigarrow \quad X \equiv 3 \pmod 5.$$

  O sea $\mathcal{S} = \{\, x \in \mathbb{Z} :\ x \equiv 3 \pmod 5\}$,

  o también, $\mathcal{S} = \{\, x \in \mathbb{Z} :\ x \equiv 3 \pmod{10} \ \text{ o } \ x \equiv 8 \pmod{10}\}$

- La ecuación $120\,X \equiv 60 \pmod{250}$ tiene solución pues $(120 : 250) = 10 \mid 60$.

$$120\,X \equiv 60 \pmod{250} \ \leftrightsquigarrow \ 12\,X \equiv 6 \pmod{25}.$$

  Pero, $\forall\, x \in \mathbb{Z}$,

$$6\,(2\,x) \equiv 6 \cdot 1 \pmod{25} \ \underset{6 \perp 25}{\iff} \ 2\,x \equiv 1 \pmod{25},$$

  pues, como $6 \perp 25$, se tiene $25 \mid 6 \cdot (2\,x - 1) \ \Leftrightarrow \ 25 \mid 2x - 1$.

  Por lo tanto,

$$12\,X \equiv 6 \pmod{25} \ \leftrightsquigarrow \ 2\,X \equiv 1 \pmod{25} \ \leftrightsquigarrow \ X \equiv 13 \pmod{25}.$$

  O sea $\mathcal{S} = \{\, x \in \mathbb{Z} :\ x \equiv 13 \pmod{25}\}$. Si queremos expresar las soluciones módulo 250, tendremos 10 soluciones distintas: ¿Cuáles son?

El argumento usado en el último ejemplo vale en general:

Observación 5.2.6. (Simplificando factores comunes en ecuación de congruencia-II.)

Sean $m \in \mathbb{N}$ y $a, c, d \in \mathbb{Z}$, con a, d no nulos.

Si d y m son *coprimos*, entonces se tiene la siguiente equivalencia de ecuaciones de congruencia:

$$(d\,a)\,X \equiv d\,c \pmod{m} \quad \leftrightsquigarrow \quad a\,X \equiv c \pmod{m}.$$

Demostración. Hay que probar que las dos ecuaciones de congruencia tienen las mismas soluciones $x \in \mathbb{Z}$:

($\Rightarrow$): Esto es porque $m \mid d\,(a\,x - c)$ y $m \perp d$ implica $m \mid a\,x - c$.

($\Leftarrow$): Vale siempre. □

Resolución completa de la ecuación de congruencia $a\,X \equiv c \pmod{m}$

1. Antes que nada reemplazo, si es necesario, a por $r_m(a)$ y c por $r_m(c)$ sin cambiar las soluciones, ya que $a \equiv r_m(a) \pmod{m}$ y $c \equiv r_m(c) \pmod{m}$, o por algún otro número conveniente que sea congruente, por ejemplo -1. Así, de entrada se tiene que los coeficientes de la ecuación de congruencia son los más simples posibles.

2. ¿ Tiene solución la ecuación ?

   (a) **no** si $(a : m) \nmid c$.

   (b) **sí** si $(a : m) \mid c$. En ese caso:

3. "Coprimizo" la ecuación:

   $$a'\,X \equiv c' \pmod{m'}, \text{ con } a' := \frac{a}{(a : m)},\ c' := \frac{c}{(a : m)} \text{ y } m' := \frac{m}{(a : m)}.$$

4. Si es necesario, ahora que $a' \perp m'$, simplifico todos los factores comunes entre a' y c' aplicando la Observación 5.2.6. Esto me simplifica la búsqueda de la solución particular.

5. Busco una solución particular $x_0 \in \mathbb{Z}$ que satisface que $a'x_0 \equiv c' \pmod{m'}$ (a ojo o encontrando una solución particular de la ecuación diofántica $a'X - m'Y = c'$ asociada).

6. Se concluye que

   $$a\,X \equiv c \pmod{m} \quad \leftrightsquigarrow \quad X \equiv x_0 \pmod{m'}.$$

O sea, el conjunto de soluciones de la ecuación de congruencia es el conjunto

$$\mathcal{S} = \{\, x \in \mathbb{Z} :\ x \equiv x_0 \pmod{m'} \,\}.$$

5.3 Teorema chino del resto (TCR).

La primera versión conocida de este teorema, sobre la resolución simultánea de varias congruencias, se encontró en un tratado escrito por el matemático chino *Sun Tzu*, que vivió entre los Siglos III y V. Dicen que le servía al emperador chino para contar su numeroso ejército sin contar los hombres uno por uno...

En la Sección 5.2 aprendimos a resolver ecuaciones de congruencia: para cada ecuación de la forma $aX \equiv c \pmod{m}$ sabemos producir la ecuación equivalente (es decir con las mismas soluciones) más simple posible, que es de la forma $X \equiv x_0 \pmod{m'}$. Ahora se trata de resolver *sistemas* de ecuaciones lineales de congruencia de la forma

$$\left\{ \begin{array}{rcll} X & \equiv & c_1 & \pmod{m_1} \\ X & \equiv & c_2 & \pmod{m_2} \\ & \vdots & & \\ X & \equiv & c_n & \pmod{m_n} \end{array} \right. \tag{5.1}$$

donde $m_1, \ldots, m_n \in \mathbb{N}$ y $c_1, \ldots, c_n \in \mathbb{Z}$. Aquí resolver significa obtener una descripción equivalente via una sola ecuación de congruencia simple (que tenga las mismas soluciones) de la forma

$$X \equiv x_0 \pmod{m},$$

o lo que es lo mismo, describir el conjunto de soluciones como

$$\mathcal{S} = \{x \in \mathbb{Z} :\ x \equiv x_0 \pmod{m}\},$$

para algún $m \in \mathbb{N}$ adecuado y algún x_0, $0 \leq x_0 < m$.

Adoptamos como en la Sección 5.2 la notación $\leftrightsquigarrow$ para sistemas de ecuaciones de congruencia equivalentes, o sea con las mismas soluciones.

Analizaremos ahora unos ejemplos sencillos que nos ayudarán a formular propiedades que garantizan la equivalencia y/o incompatibilidad de ciertos sistemas de ecuaciones de congruencias.

<u>*Ejemplos:*</u>

- $$\left\{ \begin{array}{rcl} X & \equiv & 3 \pmod{5} \\ X & \equiv & 3 \pmod{12} \end{array} \right. \quad \leftrightsquigarrow \quad X \equiv 3 \pmod{60},$$

pues $5 \mid X-3$ y $12 \mid X-3$ es equivalente a $60 = 5 \cdot 12 \mid X-3$ dado que $5 \perp 12$.

- $$\begin{cases} X & \equiv & 3 \pmod 5 \\ X & \equiv & 2 \pmod{10} \end{cases}$$

  es incompatible dado que $X \equiv 2 \pmod{10}$ implica $X \equiv 2 \pmod d$ para todo d divisor de 10 (pues $10 \mid X-2 \;\Rightarrow\; d \mid X-2$ si $d \mid 10$). En particular, para $d = 5$, no puede ser a la vez $X \equiv 2 \pmod 5$ y $X \equiv 3 \pmod 5$.

- $$\begin{cases} X & \equiv & 3 \pmod 5 \\ X & \equiv & 3 \pmod{10} \end{cases} \quad \leftrightsquigarrow \quad X \equiv 3 \pmod{10},$$

  pues $X \equiv 3 \pmod{10}$ automáticamente implica que se cumple también $X \equiv 3 \pmod d$ para todo d divisor de 10 (¿Por qué?), y en particular automáticamente se cumple $X \equiv 3 \pmod 5$.

- $$\begin{cases} X & \equiv & 3 \pmod 5 \\ X & \equiv & 8 \pmod{10} \end{cases} \quad \leftrightsquigarrow \quad X \equiv 8 \pmod{10},$$

  pues $X \equiv 8 \pmod{10}$ automáticamente implica que se cumple también $X \equiv 8 \pmod d$ para todo d divisor de 10, y en particular automáticamente se cumple $X \equiv 8 \pmod 5$, pero dado que $8 \equiv 3 \pmod 5$, automáticamente se cumple $X \equiv 3 \pmod 5$.

Estos ejemplos se generalizan a las propiedades siguientes, que se aplicarán sistemáticamente en lo que sigue.

Proposición 5.3.1. (Sistemas equivalentes.)

1. *Sean* $m_1, \ldots, m_n \in \mathbb{N}$ coprimos dos a dos, *es decir* $m_i \perp m_j$ *para* $i \neq j$. *Entonces,* $\forall\, c \in \mathbb{Z}$,

$$\begin{cases} X & \equiv & c \pmod{m_1} \\ X & \equiv & c \pmod{m_2} \\ & \vdots & \\ X & \equiv & c \pmod{m_n} \end{cases} \quad \leftrightsquigarrow \quad X \equiv c \pmod{m_1 \cdot m_2 \cdots m_n}.$$

2. *Sean* $m, m' \in \mathbb{N}$ *tales que* $m' \mid m$. *Entonces,* $\forall\, c, c' \in \mathbb{Z}$,

   - *Si* $c \not\equiv c' \pmod{m'}$, $\begin{cases} X & \equiv & c' \pmod{m'} \\ X & \equiv & c \pmod m \end{cases}$ *es incompatible,*

   - *Si* $c \equiv c' \pmod{m'}$, $\begin{cases} X & \equiv & c' \pmod{m'} \\ X & \equiv & c \pmod m \end{cases} \leftrightsquigarrow X \equiv c \pmod m.$

Demostración. 1. Hay que probar que el sistema del lado izquierdo tiene exactamente las mismas soluciones $x \in \mathbb{Z}$ que la ecuación del lado derecho.

($\Leftarrow$) Si $x \in \mathbb{Z}$ satisface $x \equiv c \pmod{m_1 \cdot m_2 \cdots m_n}$, es decir $m_1 \cdot m_2 \cdots m_n \mid x - c$, entonces claramente $m_i \mid x - c$, $\forall\, i$, es decir $x \equiv c \pmod{m_i}$, $\forall\, i$.

($\Rightarrow$) Por inducción en la cantidad de factores n.

- Para $n = 1$, no hay nada que probar.
- $n \Rightarrow n+1$: Queremos probar que si $m_1, \ldots, m_{n+1}$ son coprimos dos a dos, entonces $\forall\, c \in \mathbb{Z}$, $\forall\, x \in \mathbb{Z}$

$$\begin{cases} x \equiv c \pmod{m_1} \\ \quad \vdots \\ x \equiv c \pmod{m_n} \\ x \equiv c \pmod{m_{n+1}} \end{cases} \implies x \equiv c \pmod{m_1 \cdots m_n \cdot m_{n+1}}$$

Por H.I., como $m_1, \ldots, m_n$ son coprimos dos a dos,

$$\begin{cases} x \equiv c \pmod{m_1} \\ \quad \vdots \\ x \equiv c \pmod{m_n} \end{cases} \implies x \equiv c \pmod{m_1 \cdots m_n}.$$

Es decir,

$$\begin{cases} x \equiv c \pmod{m_1} \\ \quad \vdots \\ x \equiv c \pmod{m_n} \\ x \equiv c \pmod{m_{n+1}} \end{cases} \implies \begin{cases} x \equiv c \pmod{m_1 \cdots m_n} \\ x \equiv c \pmod{m_{n+1}} \end{cases}.$$

Pero dado que $m_1, \ldots, m_n$ son todos coprimos con m_{n+1}, se deduce que $m_1 \cdots m_n$ es coprimo con m_{n+1}. Luego

$$\begin{cases} x \equiv c \pmod{m_1 \cdots m_n} \\ x \equiv c \pmod{m_{n+1}} \end{cases} \implies \begin{cases} m_1 \cdots m_n \mid x - c \\ m_{n+1} \mid x - c \end{cases}$$

$$\underset{m_1 \cdots m_n \perp m_{n+1}}{\implies} (m_1 \cdots m_n) \cdot m_{n+1} \mid x - c$$

$$\implies x \equiv c \pmod{m_1 \cdots m_{n+1}}.$$

2. Cuando $m' \mid m$, $\forall\, x \in \mathbb{Z}$, $x \equiv c \pmod{m}$ implica $x \equiv c \pmod{m'}$ pues $m \mid x - c \Rightarrow m' \mid x - c$. Luego

$$\begin{cases} x \equiv c' \pmod{m'} \\ x \equiv c \pmod{m} \end{cases} \implies \begin{cases} x \equiv c' \pmod{m'} \\ x \equiv c \pmod{m'} \end{cases}$$

Por transitividad, $c \equiv c' \pmod{m'}$. Por lo tanto, si $c \not\equiv c' \pmod{m'}$, el sistema es incompatible. Sean entonces c, c' tales que $c \equiv c' \pmod{m'}$.

Probemos la equivalencia del sistema de la izquierda con la ecuación de la derecha:

$$\left\{\begin{array}{rcl} x & \equiv & c' \pmod{m'} \\ x & \equiv & c \pmod{m} \end{array}\right. \quad \Longrightarrow \quad x \equiv c \pmod{m},$$

pues nos estamos quedando con una de las dos condiciones. Recíprocamente,

$$x \equiv c \pmod{m} \implies x \equiv c \pmod{m'} \implies x \equiv c' \pmod{m'},$$

y por lo tanto

$$x \equiv c \pmod{m} \quad \Longrightarrow \quad \left\{\begin{array}{rcl} x & \equiv & c' \pmod{m'} \\ x & \equiv & c \pmod{m} \end{array}\right. ,$$

como se quería probar.

□

Ejemplos:

- $$\left\{\begin{array}{rcl} X & \equiv & 3 \pmod{22} \\ X & \equiv & 3 \pmod{5} \\ X & \equiv & 3 \pmod{21} \end{array}\right. \quad \leftrightsquigarrow \quad X \equiv 3 \pmod{22 \cdot 5 \cdot 21},$$

  por la Proposición 5.3.1, pues $22 = 2 \cdot 11$, 5 y $21 = 3 \cdot 7$ son coprimos dos a dos.

- De la misma forma:

$$X \equiv 50 \pmod{22 \cdot 5 \cdot 21} \leftrightsquigarrow \left\{\begin{array}{rcl} X & \equiv & 50 \pmod{22} \\ X & \equiv & 50 \pmod{5} \\ X & \equiv & 50 \pmod{21} \end{array}\right.$$
$$\leftrightsquigarrow \left\{\begin{array}{rcl} X & \equiv & 6 \pmod{22} \\ X & \equiv & 0 \pmod{5} \\ X & \equiv & 8 \pmod{21} \end{array}\right. .$$

- $$\left\{\begin{array}{rcl} X & \equiv & 3 \pmod{22} \\ X & \equiv & 3 \pmod{18} \\ X & \equiv & 4 \pmod{11} \end{array}\right.$$

  es incompatible, por la Proposición 5.3.1, pues $11 \mid 22$ pero $3 \not\equiv 4 \pmod{11}$.

- $$\left\{\begin{array}{rcl} X & \equiv & 3 \pmod{22} \\ X & \equiv & 4 \pmod{8} \end{array}\right. \quad \leftrightsquigarrow \quad \left\{\begin{array}{rcl} X & \equiv & 1 \pmod{2} \\ X & \equiv & 3 \pmod{11} \\ X & \equiv & 4 \pmod{8} \end{array}\right.$$

  y luego es incompatible pues en el sistema de la derecha la primera ecuación y la tercera son incompatibles: $2 \mid 8$ pero $4 \not\equiv 1 \pmod{2}$.

- $$\left\{\begin{array}{lcl} X & \equiv & 1 \pmod 4 \\ X & \equiv & 5 \pmod 8 \\ X & \equiv & 13 \pmod{16} \end{array}\right. \quad \leftrightsquigarrow \quad X \equiv 13 \pmod{16}$$

  por la Proposición 5.3.1: $4 \mid 8$ y $5 \equiv 1 \pmod 4$, $8 \mid 16$ y $13 \equiv 5 \pmod 8$.

- $$\left\{\begin{array}{lcll} X & \equiv & 3 & \pmod{22} \\ X & \equiv & 5 & \pmod 8 \\ X & \equiv & 17 & \pmod{20} \end{array}\right. \leftrightsquigarrow \left\{\begin{array}{lcl} X & \equiv & 1 \pmod 2 \\ X & \equiv & 3 \pmod{11} \\ X & \equiv & 5 \pmod 8 \\ X & \equiv & 1 \pmod 4 \\ X & \equiv & 2 \pmod 5 \end{array}\right.$$
  $$\leftrightsquigarrow \left\{\begin{array}{lcl} X & \equiv & 5 \pmod 8 \\ X & \equiv & 3 \pmod{11} \\ X & \equiv & 2 \pmod 5 \end{array}\right.$$

  aplicando reiteradamente la Proposición 5.3.1.

En estos ejemplos se ve que cuando el sistema no es incompatible, se reduce a resolver un sistema (5.1) *pero con la condición de que los m_i son coprimos dos a dos.* En esa situación vale el teorema siguiente:

Teorema 5.3.2. (Teorema chino del resto.)

Sean $m_1, \ldots, m_n \in \mathbb{N}$ coprimos dos a dos*, es decir $m_i \perp m_j$ para $i \neq j$. Entonces, $\forall\, c_1, \ldots, c_n \in \mathbb{Z}$, el sistema de ecuaciones de congruencia*

$$\left\{\begin{array}{lcl} X & \equiv & c_1 \pmod{m_1} \\ & \vdots & \\ X & \equiv & c_n \pmod{m_n} \end{array}\right.$$

tiene soluciones enteras.
Más aún,

$$\left\{\begin{array}{lcl} X & \equiv & c_1 \pmod{m_1} \\ & \vdots & \\ X & \equiv & c_n \pmod{m_n} \end{array}\right. \quad \leftrightsquigarrow \quad X \equiv x_0 \pmod{m_1 \cdots m_n}\ ,$$

donde $x_0 \in \mathbb{Z}$ es una solución particular cualquiera del sistema, y se tiene

$$\mathcal{S} = \{x \in \mathbb{Z} :\ x \equiv x_0 \pmod{m_1 \cdots m_n}\}.$$

En particular, existe una única solución $x_0 \in \mathbb{Z}$ que satisface $0 \leq x_0 < m_1 \cdots m_n$.

Lo interesante de la demostración de este teorema es que da un método constructivo, o sea sugiere directamente un algoritmo, para hallar x_0.

Demostración. Supongamos que ya mostramos que el sistema tiene soluciones. Entonces, sea $x_0 \in \mathbb{Z}$ una solución particular, es decir $x_0 \in \mathbb{Z}$ satisface

$$\begin{cases} x_0 & \equiv & c_1 \pmod{m_1} \\ & \vdots & \\ x_0 & \equiv & c_n \pmod{m_n} \end{cases}.$$

En ese caso, por transitividad y aplicando la Proposición 5.3.1, tendremos para una solución cualquiera x:

$$\begin{cases} x & \equiv & c_1 \pmod{m_1} \\ & \vdots & \\ x & \equiv & c_n \pmod{m_n} \end{cases} \iff \begin{cases} x & \equiv & x_0 \pmod{m_1} \\ x & \equiv & x_0 \pmod{m_2} \\ & \vdots & \\ x & \equiv & x_0 \pmod{m_n} \end{cases}$$
$$\iff x \equiv x_0 \pmod{m_1 \cdots m_n},$$

o sea probamos la equivalencia enunciada en el Teorema.

El único x_0 que satisface $0 \leq x_0 < m_1 \cdots m_n$ se obtiene reemplazando la solución particular elegida por $r_{m_1 \cdots m_n}(x_0)$.

Para probar que existen soluciones (y hallar una solución particular x_0), vamos a subdividir el sistema (5.1) en n sistemas más simples y probar que cada uno de ellos tiene soluciones. Estos sistemas S_1, S_2, ..., S_n son:

$$\underline{S_1}: \quad \begin{cases} X & \equiv & c_1 \pmod{m_1} \\ X & \equiv & 0 \pmod{m_2} \\ X & \equiv & 0 \pmod{m_3} \\ & \vdots & \\ X & \equiv & 0 \pmod{m_n} \end{cases}, \quad \underline{S_2}: \quad \begin{cases} X & \equiv & 0 \pmod{m_1} \\ X & \equiv & c_2 \pmod{m_2} \\ X & \equiv & 0 \pmod{m_3} \\ & \vdots & \\ X & \equiv & 0 \pmod{m_n} \end{cases}, \ \ldots, \quad \underline{S_n}: \quad \begin{cases} X & \equiv & 0 \pmod{m_1} \\ X & \equiv & 0 \pmod{m_2} \\ & \vdots & \\ X & \equiv & 0 \pmod{m_{n-1}} \\ X & \equiv & c_n \pmod{m_n} \end{cases}$$

Supongamos que podemos probar que cada uno de estos sistemas S_ℓ, $1 \leq \ell \leq n$ tiene soluciones, y encontramos para cada uno una solución particular x_ℓ, es decir:

$$\underline{S_1}: \quad \begin{cases} x_1 & \equiv & c_1 \pmod{m_1} \\ x_1 & \equiv & 0 \pmod{m_2} \\ x_1 & \equiv & 0 \pmod{m_3} \\ & \vdots & \\ x_1 & \equiv & 0 \pmod{m_n} \end{cases}, \quad \underline{S_2}: \quad \begin{cases} x_2 & \equiv & 0 \pmod{m_1} \\ x_2 & \equiv & c_2 \pmod{m_2} \\ x_2 & \equiv & 0 \pmod{m_3} \\ & \vdots & \\ x_2 & \equiv & 0 \pmod{m_n} \end{cases}, \ \ldots, \quad \underline{S_n}: \quad \begin{cases} x_n & \equiv & 0 \pmod{m_1} \\ x_n & \equiv & 0 \pmod{m_2} \\ & \vdots & \\ x_n & \equiv & 0 \pmod{m_{n-1}} \\ x_n & \equiv & c_n \pmod{m_n} \end{cases}$$

Entonces si definimos

$$x_0 := x_1 + x_2 + x_3 + \cdots + x_n,$$

se satisface que

$$\begin{cases} x_1 + x_2 + x_3 + \cdots + x_n & \equiv & c_1 + 0 + 0 + \cdots + 0 \pmod{m_1} \\ x_1 + x_2 + x_3 + \cdots + x_n & \equiv & 0 + c_2 + 0 + \cdots + 0 \pmod{m_2} \\ & \vdots & \\ x_1 + x_2 + x_3 + \cdots + x_n & \equiv & 0 + 0 + \cdots + 0 + c_n \pmod{m_n} \end{cases} \implies \begin{cases} x_0 & \equiv & c_1 \pmod{m_1} \\ x_0 & \equiv & c_2 \pmod{m_2} \\ & \vdots & \\ x_0 & \equiv & c_n \pmod{m_n} \end{cases}$$

es decir, x_0 es una solución (particular) del sistema original, y en particular el sistema original tiene soluciones.

Aplicando los resultados de la Sección 5.2, vamos a ver que todos los sistemas S_ℓ, $1 \leq \ell \leq n$, tienen soluciones enteras y vamos a elegir para cada uno de ellos una solución particular x_ℓ.

Miremos el sistema S_1: Como $m_2, \ldots, m_n$ son coprimos dos a dos, si ponemos $M_1 := m_2 \cdots m_n$, se tiene la equivalencia descrita en la Proposición 5.3.1:

$$\begin{cases} X \equiv c_1 \pmod{m_1} \\ X \equiv 0 \pmod{m_2} \\ \quad \vdots \\ X \equiv 0 \pmod{m_n} \end{cases} \quad \leftrightsquigarrow \quad \begin{cases} X \equiv c_1 \pmod{m_1} \\ X \equiv 0 \pmod{M_1}. \end{cases}$$

La segunda ecuación a la derecha indica que cualquier solución x tiene que satisfacer que $x = M_1\, y$ para algún $y \in \mathbb{Z}$, y luego para cumplir con la primer ecuación, se tiene que satisfacer $M_1\, y \equiv c_1 \pmod{m_1}$, o sea y es una solución de la ecuación

$$M_1\, Y \equiv c_1 \pmod{m_1}. \tag{5.2}$$

Se observa que $M_1 \perp m_1$, por ser $M_1 = m_2 \cdots m_n$ y los m_i coprimos dos a dos. Por lo tanto, sabemos que la ecuación (5.2) tiene soluciones enteras cualquiera sea $c_1 \in \mathbb{Z}$. Si y_1 es una solución particular, entonces $x_1 := M_1\, y_1$ es una solución particular del sistema S_1.

Veamos de forma análoga que para todo ℓ, $1 \leq \ell \leq n$, el sistema

$$S_\ell: \quad \begin{cases} X \equiv 0 \pmod{m_1} \\ \quad \vdots \\ X \equiv 0 \pmod{m_{\ell-1}} \\ X \equiv c_\ell \pmod{m_\ell} \\ X \equiv 0 \pmod{m_{\ell+1}} \\ \quad \vdots \\ X \equiv 0 \pmod{m_n} \end{cases}$$

tiene soluciones enteras y por lo tanto se puede elegir para él una solución particular x_ℓ.

Definamos $M_\ell := \prod_{j \neq \ell} m_j$ y repitamos lo que se hizo arriba para S_1. Se tiene $M_\ell \perp m_\ell$ por ser todos los m_i coprimos dos a dos. Luego, la ecuación de congruencia

$$M_\ell\, Y \equiv c_\ell \pmod{m_\ell}$$

tiene soluciones enteras cualquiera sea $c_\ell \in \mathbb{Z}$, y si y_ℓ es una solución particular, entonces, como arriba, $x_\ell := M_\ell\, y_\ell$ es una solución particular del sistema S_ℓ. □

Ejemplos:

- $$\begin{cases} X & \equiv & 4 & (\text{mod } 8) \\ X & \equiv & 10 & (\text{mod } 35) \\ X & \equiv & 1 & (\text{mod } 3) \end{cases}$$

  Como 8, 35 y 3 son coprimos 2 a 2, por el Teorema 5.3.2, el sistema tiene soluciones y es equivalente a $X \equiv x_0 \pmod{8 \cdot 35 \cdot 3}$, es decir $X \equiv x_0 \pmod{840}$, donde x_0 es la única solución con $0 \leq x_0 < 840$. Para hallar esta solución x_0, se consideran los tres sistemas más simples:

  $$\underline{S_1}: \begin{cases} X & \equiv & 4 & (\text{mod } 8) \\ X & \equiv & 0 & (\text{mod } 35) \\ X & \equiv & 0 & (\text{mod } 3) \end{cases}, \quad \underline{S_2}: \begin{cases} X & \equiv & 0 & (\text{mod } 8) \\ X & \equiv & 10 & (\text{mod } 35) \\ X & \equiv & 0 & (\text{mod } 3) \end{cases}, \quad \underline{S_3}: \begin{cases} X & \equiv & 0 & (\text{mod } 8) \\ X & \equiv & 0 & (\text{mod } 35) \\ X & \equiv & 1 & (\text{mod } 3) \end{cases}.$$

  Solución particular para S_1:

  $$\begin{cases} X & \equiv & 4 & (\text{mod } 8) \\ X & \equiv & 0 & (\text{mod } 35) \\ X & \equiv & 0 & (\text{mod } 3) \end{cases} \leftrightsquigarrow \begin{cases} X & \equiv & 4 & (\text{mod } 8) \\ X & \equiv & 0 & (\text{mod } 35 \cdot 3) \end{cases}$$

  Es decir una solución x satisface $x = 35 \cdot 3\, y = 105\, y$ donde y es solución de la ecuación $105\, Y \equiv 4 \pmod{8}$, o sea de la ecuación $Y \equiv 4 \pmod{8}$. Una solución particular es $y_1 = 4$, y por lo tanto $x_1 = 105\, y_1 = 420$ es una solución particular del sistema S_1.

  Solución particular para S_2:

  $$\begin{cases} X & \equiv & 0 & (\text{mod } 8) \\ X & \equiv & 10 & (\text{mod } 35) \\ X & \equiv & 0 & (\text{mod } 3) \end{cases} \leftrightsquigarrow \begin{cases} X & \equiv & 10 & (\text{mod } 35) \\ X & \equiv & 0 & (\text{mod } 8 \cdot 3) \end{cases}.$$

  Es decir una solución x satisface $x = 8 \cdot 3\, y = 24\, y$ donde y es solución de la ecuación $24\, Y \equiv 10 \pmod{35}$. Dado que $(24 : 10) = 2 \perp 35$, podemos simplificar por 2 y el sistema es equivalente a $12\, Y \equiv 5 \pmod{35}$. Podemos encontrar rápidamente la solución a ojo del modo siguiente:

  $$\begin{aligned} 12 \cdot 3 \equiv 1 \pmod{35} &\Longrightarrow 12 \cdot (3 \cdot 5) \equiv 1 \cdot 5 \pmod{35} \\ &\Longrightarrow 12 \cdot 15 \equiv 5 \pmod{35}. \end{aligned}$$

  Luego, una solución particular es $y_2 = 15$, y por lo tanto $x_2 = 24\, y_2 = 360$ es una solución particular del sistema S_2.

  Solución particular para S_3:

  $$\begin{cases} X & \equiv & 0 & (\text{mod } 8) \\ X & \equiv & 0 & (\text{mod } 35) \\ X & \equiv & 1 & (\text{mod } 3) \end{cases} \leftrightsquigarrow \begin{cases} X & \equiv & 1 & (\text{mod } 3) \\ X & \equiv & 0 & (\text{mod } 8 \cdot 35) \end{cases}.$$

Es decir una solución x satisface $x = 8 \cdot 35\, y = 280\, y$, donde y es solución de la ecuación $280\, Y \equiv 1 \pmod 3$, o sea de la ecuación $Y \equiv 1 \pmod 3$. Una solución particular es $y_3 = 1$, por lo tanto $x_3 = 280\, y_3 = 280$ es una solución particular de S_3.

Por lo tanto, aplicando la construcción del Teorema 5.3.2,

$$x_0 := x_1 + x_2 + x_3 = 240 + 360 + 280 = 1060$$

es una solución particular del sistema original, y éste es equivalente a $X \equiv 1060 \pmod{840}$. Como $1060 \equiv 220 \pmod{840}$, se tiene que la única solución x_0 con $0 \leq x_0 < 840$ es $x_0 = 220$:

$$\begin{cases} X \equiv 4 \pmod 8 \\ X \equiv 10 \pmod{35} \\ X \equiv 1 \pmod 3 \end{cases} \quad \rightsquigarrow \quad X \equiv 220 \pmod{840}.$$

Es decir, $\mathcal{S} = \{x \in \mathbb{Z} :\ x \equiv 220 \pmod{840}\}$.

- $$\begin{cases} X \equiv 3 \pmod{10} \\ X \equiv 1 \pmod{11} \\ X \equiv 3 \pmod 7 \end{cases}$$

Nuevamente, $10, 11$ y 7 son coprimos 2 a 2, luego por el teorema el sistema tiene soluciones y es equivalente a $X \equiv x_0 \pmod{10 \cdot 11 \cdot 7}$, es decir $X \equiv x_0 \pmod{770}$, donde x_0 es la única solución con $0 \leq x_0 < 770$. Ahora bien, observemos que por la Proposición 5.3.1, la primera ecuación y la tercera se pueden juntar en la ecuación $X \equiv 3 \pmod{70}$, al ser 10 y 7 coprimos. Por lo tanto para hallar una solución particular, es suficiente aquí considerar los dos sistemas:

$$\underline{S_1}: \quad \begin{cases} X \equiv 3 \pmod{70} \\ X \equiv 0 \pmod{11} \end{cases}, \qquad \underline{S_2}: \quad \begin{cases} X \equiv 0 \pmod{70} \\ X \equiv 1 \pmod{11} \end{cases}.$$

Solución particular para S_1:

Una solución particular x_1 satisface $x_1 = 11\, y_1$ donde y_1 es solución particular de la ecuación $11\, Y \equiv 3 \pmod{70}$. Por ejemplo $y_1 = 13$ (pues por el algoritmo de Euclides $1 = 3 \cdot 70 - 19 \cdot 11$, y por lo tanto $y_1 \equiv 3 \cdot (-19) \pmod{70}$, o sea se puede tomar $y_1 = 13$). Luego $x_1 = 11 \cdot 13 = 143$.

Solución particular para S_2:

Una solución particular x_2 satisface $x_2 = 70\, y_2$ donde y_2 es solución particular de la ecuación $70\, Y \equiv 1 \pmod{11}$, o sea $4\, Y \equiv 1 \pmod{11}$. Por ejemplo $y_2 = 3$, y por lo tanto $x_2 = 70\, y_2 = 210$.

Así, $x_0 := x_1 + x_2 = 143 + 210 = 353$ es solución particular del sistema original. Además es la única solución con $0 \leq x_0 < 770$. Se tiene la equivalencia

$$\left\{ \begin{array}{rcl} X & \equiv & 3 \pmod{10} \\ X & \equiv & 1 \pmod{11} \\ X & \equiv & 3 \pmod{7} \end{array} \right. \quad \leftrightsquigarrow \quad X \equiv 353 \pmod{770},$$

es decir, $\mathcal{S} = \{x \in \mathbb{Z} : \ x \equiv 353 \pmod{770}\}$.

Pero en este caso este mismo ejemplo se puede resolver más "a mano" usando la fuerza del TCR:

$$\left\{ \begin{array}{rcl} X & \equiv & 3 \pmod{70} \\ X & \equiv & 1 \pmod{11} \end{array} \right. .$$

Sabemos que el sistema tiene solución y es equivalente a

$$X \equiv x_0 \pmod{770}$$

donde $x_0 \in \mathbb{Z}$ es la única solución particular del sistema con $0 \leq x_0 < 770$. Veamos si podemos encontrar ese x_0 "a ojo". Para ello investiguemos los valores entre 0 y 770 que cumplen la primera ecuación. Estos son de la forma $3 + 70\,k$, $k \in \mathbb{Z}$, es decir

$$3,\ 73,\ 143,\ 213,\ 283,\ 353,\ 423,\ 493,\ \ldots$$

Entre ellos, ¿cuál es el único que cumple también la segunda ecuación?

$$\not{3},\ \not{7}3,\ 1\not{4}3,\ 2\not{1}3,\ 2\not{8}3,\ 353$$

El número 353 cumple $353 \equiv 1 \pmod{11}$. ¡Ya está! ¡encontramos uno, entonces ese es x_0 y el sistema es equivalente a la ecuación $X \equiv 353 \pmod{770}$!

- Volvamos al último ejemplo antes del enunciado del TCR:

$$\left\{ \begin{array}{rcll} X & \equiv & 3 & \pmod{22} \\ X & \equiv & 5 & \pmod{8} \\ X & \equiv & 17 & \pmod{20} \end{array} \right. \quad \leftrightsquigarrow \quad \left\{ \begin{array}{rcl} X & \equiv & 5 \pmod{8} \\ X & \equiv & 3 \pmod{11} \\ X & \equiv & 2 \pmod{5} \end{array} \right.$$

Como 8, 11 y 5 son coprimos dos a dos, sabemos que el sistema es equivalente a

$$X \equiv x_0 \pmod{8 \cdot 11 \cdot 5}, \quad \text{es decir} \quad X \equiv x_0 \pmod{440},$$

donde x_0, es la única solución del sistema con $0 \leq x_0 < 440$. Empecemos por investigar los que cumplen las dos ecuaciones con el módulo más grande. Para ello escribimos primero los números entre 0 y

$11 \cdot 8 = 88$ que cumplen la ecuación con el módulo 11, o sea de la forma $3 + 11\,k, k \in \mathbb{Z}$:

$$3,\ 14,\ 25,\ 36,\ 47,\ 58,\ 69,\ \ldots$$

¿Cuál cumple la condición con el módulo 8?

$$\not{3},\ \not{1}4,\ \not{2}5,\ \not{3}6,\ \not{4}7,\ \not{5}8, 69:$$

El número 69 cumple $69 \equiv 5 \pmod 8$, luego los que resuelven esas dos ecuaciones son $x \equiv 69 \pmod{88}$. Ahora, vamos escribiendo los números entre 0 y 440 que cumplen esa condición, investigando cuál es el que cumple la ecuación con el módulo 5:

$$\not{6}9,\ 157$$

El número 157 cumple $157 \equiv 2 \pmod 5$ ¡Ya está!

$$\left\{\begin{array}{rcll} X & \equiv & 3 & (\text{mod } 22) \\ X & \equiv & 5 & (\text{mod } 8) \\ X & \equiv & 17 & (\text{mod } 20) \end{array}\right. \quad \leftrightsquigarrow \quad X \equiv 157 \ (\text{mod } 440),$$

es decir, $\mathcal{S} = \{x \in \mathbb{Z} :\ x \equiv 157 \pmod{440}\}$.

- Un ejemplo donde las ecuaciones iniciales no están en la forma $X \equiv c_\ell \pmod{m_\ell}\}$:

$$\left\{\begin{array}{rcl} 3\,X & \equiv & 2 \pmod 7 \\ 7\,X & \equiv & 5 \pmod 8 \\ 6\,X & \equiv & 8 \pmod{10} \end{array}\right. .$$

Primero se puede simplificar todo lo que se puede (en este caso el factor común 2 en la tercera ecuación), y luego como en lo que resulta los módulos son coprimos dos a dos, resolver cada ecuación por separado, dándola en la forma $X \equiv c_\ell \pmod{m_\ell}$ para aplicar el TCR:

$$\left\{\begin{array}{rcl} 3\,X & \equiv & 2\ (7) \\ 7\,X & \equiv & 5\ (8) \\ 6\,X & \equiv & 8\ (10) \end{array}\right. \leftrightsquigarrow \left\{\begin{array}{rcl} 3\,X & \equiv & 2\ (7) \\ 7\,X & \equiv & 5\ (8) \\ 3\,X & \equiv & 4\ (5) \end{array}\right. \leftrightsquigarrow \left\{\begin{array}{rcl} X & \equiv & 3\ (7) \\ X & \equiv & 3\ (8) \\ X & \equiv & 3\ (5) \end{array}\right. \leftrightsquigarrow X \equiv 3\ (280),$$

pues 7, 8 y 5 son coprimos dos a dos. Es decir

$$\mathcal{S} = \{x \in \mathbb{Z} :\ x \equiv 3 \pmod{280}\}.$$

- Sea $x \in \mathbb{Z}$ tal que $r_9(4\,x) = 2$, $r_{14}(3\,x) = 5$ y $r_{20}(3\,x) = 1$. Calcular los posibles restos de dividir a x por $9 \cdot 14 \cdot 20 = 2520$:
Se tiene que x es solución del sistema

$$\left\{\begin{array}{rcl} 4\,X & \equiv & 2\ (9) \\ 3\,X & \equiv & 5\ (14) \\ 3\,X & \equiv & 1\ (20) \end{array}\right. \leftrightsquigarrow \left\{\begin{array}{rcl} 2\,X & \equiv & 1\ (9) \\ 3\,X & \equiv & 5\ (2) \\ 3\,X & \equiv & 5\ (7) \\ 3\,X & \equiv & 1\ (4) \\ 3\,X & \equiv & 1\ (5) \end{array}\right. \leftrightsquigarrow \left\{\begin{array}{rcl} X & \equiv & 5\ (9) \\ X & \equiv & 1\ (2) \\ X & \equiv & 4\ (7) \\ X & \equiv & 3\ (4) \\ X & \equiv & 2\ (5) \end{array}\right. \leftrightsquigarrow \left\{\begin{array}{rcl} X & \equiv & 5\ (9) \\ X & \equiv & 4\ (7) \\ X & \equiv & 3\ (4) \\ X & \equiv & 2\ (5) \end{array}\right.$$

por aplicación reiterada de la Proposición 5.3.1. Al resolver este sistema con el método dado por el TCR, se obtiene que el sistema original es equivalente a

$$X \equiv 1607\ (9 \cdot 7 \cdot 4 \cdot 5 = 1260) \quad \rightsquigarrow \quad X \equiv 347\ (1260).$$

Luego el resto de dividir a x por 1260 es 347, pero como se quiere los posibles restos de dividir a x por $2520 = 2 \cdot 1260$, éstos son 347 y $347 + 1260 = 1607$, los dos números entre 0 y 2520 que son congruentes con 347 módulo 1260.

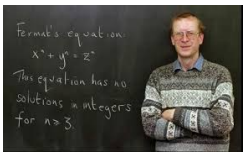
5.4 El Pequeño Teorema de Fermat (PTF)

Este teorema es uno de los tantos que debemos al abogado y mayor matemático amateur de todos los tiempos, el francés *Pierre de Fermat*, 1601–1665. Fermat dejó una obra importantísima en Teoría de Números, además de ser un pionero en Teoría de Probabilidades, Cálculo Variacional y Geometría Analítica.

Poseía la traducción latina de la Aritmética de Diofanto, realizada por Bachet a fines del Siglo XVI, y tenía la particularidad de escribir en los márgenes de ese libro enunciados matemáticos y comentarios, la mayoría de las veces sin demostraciones.

El Pequeño Teorema fue luego demostrado y generalizado por el matemático suizo *Leonhard Euler*, 1707–1783. Euler demostró la casi totalidad de los resultados enunciados por Fermat, con la excepción de la afirmación —inspirada en el teorema de Pitágoras— conocida como el "último teorema de Fermat":

Cualquiera sea $n > 2$, *no existen* $a, b, c \in \mathbb{N}$ *tales que* $a^n + b^n = c^n$.



Esta importante conjetura, que motivó el desarrollo de toda la rama de la matemática conocida como la Teoría de Números, recién fue probada en los años 1993–1994 por el matemático inglés Andrew Wiles (en una parte con su discípulo Richard Taylor).

Teorema 5.4.1. (Pequeño Teorema de Fermat - PTF.)

Sea p *un* primo *positivo. Entonces,* $\forall\, a \in \mathbb{Z}$,

1. $a^p \equiv a \pmod{p}$
2. $p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$

Observación 5.4.2.

El teorema es falso en general si p no es primo: por ejemplo $3^4 = 81 \not\equiv 3 \pmod 4$. Sin embargo existen números n no primos para los cuales vale el enunciado del PTF: $a^n \equiv a \pmod n$ para todo $a \in \mathbb{Z}$.

Esos números se suelen llamar "seudoprimos" o "números de Carmichael" por el matemático americano Robert Carmichael, 1879–1967, que descubrió en 1909 el más chico de ellos: el número $n := 561 = 3 \cdot 11 \cdot 17$.

En 1994, los matemáticos Red Alford, Andrew Granville y Carl Pomerance lograron probar la conjetura que afirmaba que existen infinitos seudoprimos.

Observación 5.4.3. Las dos afirmaciones del PTF son equivalentes:

(*1* $\Rightarrow$ *2*) Por hipótesis, $a^p \equiv a \pmod p$. Si $p \nmid a$, es decir $a \perp p$, se puede simplificar un a de los dos lados (justificar!) y queda $a^{p-1} \equiv 1 \pmod p$.

(*2* $\Rightarrow$ *1*) Hay que probar que para $a \in \mathbb{Z}$ cualquiera, $a^p \equiv a \pmod p$. Si $p \nmid a$, por (*2*) vale que $a^{p-1} \equiv 1 \pmod p$, luego multiplicando por a se obtiene $a^p \equiv a \pmod p$. Mientras que si $p \mid a$, entonces tanto a como a^p son congruentes con 0 módulo p (pues p los divide), así, $a^p \equiv 0 \equiv a \pmod p$ también.

Demostración. (del PTF.)

Por la observación anterior, para probar el PTF alcanza con probar el caso (*2*) en que $p \nmid a$, es decir $a \perp p$, que es el caso interesante y no trivial. Vamos a hacer aquí la demostración de Euler, que permite obtener una formulación del teorema para no primos conocida como Teorema de Euler, que no probaremos en estas notas.

Fijamos $a \in \mathbb{Z}$ tal que $p \nmid a$ y definimos la siguiente función:

$$\begin{array}{rccc} \Phi: & \{1,2,\ldots,p-1\} & \longrightarrow & \{1,2,\ldots,p-1\} \\ & k & \longmapsto & r_p(k\,a) \end{array}$$

Por ejemplo, $\Phi(1) = r_p(a)$, $\Phi(2) = r_p(2\,a)$, $\Phi(3) = r_p(3\,a)$, etc. (Observemos en particular que $\Phi(k) = r_p(k\,a) \equiv k\,a \pmod p$.)

Veamos primero que esta función está bien definida (es decir que la imagen $\mathrm{Im}(\Phi)$ de la función Φ realmente está incluída en el codominio) y luego que es biyectiva.

- $\mathrm{Im}(\Phi) \subseteq \{1,2,\ldots,p-1\}$:

  Por definición de resto módulo p, está claro que $\mathrm{Im}(\Phi) \subseteq \{0,1,2,\ldots,p-1\}$. Hay que probar que nunca se obtiene el 0, es decir que no existe $k \in \{1,\ldots,p-1\}$ tal que $\Phi(k) = 0$. Pero

$$\Phi(k) = 0 \iff r_p(k\,a) = 0 \iff p \mid k\,a \underset{p \text{ primo}}{\iff} p \mid k \;\text{ ó }\; p \mid a,$$

lo que es absurdo pues por hipótesis $p \nmid a$ y $p \nmid k$ por ser $k \in \{1, \ldots, p-1\}$ más chico que p.

- Para probar que Φ es biyectiva, dado que es una función de un conjunto finito en sí mismo, alcanza con probar que es inyectiva:

  Supongamos que para $1 \leq j \leq k \leq p-1$, se tiene que $\Phi(k) = \Phi(j)$, queremos probar que entonces $k = j$. Pero de la misma forma que probamos la buena definición,

$$\begin{aligned} \Phi(k) = \Phi(j) &\iff r_p(k\,a) = r_p(j\,a) \\ &\iff p \mid k\,a - j\,a = (k-j)\,a \\ &\underset{p \text{ primo}}{\iff} p \mid k-j \;\text{ ó }\; p \mid a, \end{aligned}$$

  lo que se cumple únicamente si $p \mid k-j$ pues $p \nmid a$. Ahora bien, como $1 \leq j \leq k \leq p-1$, se tiene que $k-j \in \{0, \ldots, p-1\}$, luego

$$p \mid k-j \iff k-j = 0 \iff k = j.$$

Por lo tanto Φ es biyectiva, es decir suryectiva también, con lo cual $\mathrm{Im}(\Phi) = \{1, 2, \ldots, p-1\}$. Esto implica

$$\Phi(1) \cdot \Phi(2) \cdots \Phi(p-1) = 1 \cdot 2 \cdots (p-1).$$

Es decir,

$$r_p(a) \cdot r_p(2\,a) \cdots r_p((p-1)\,a) = 1 \cdot 2 \cdots (p-1).$$

Pero como $k\,a \equiv r_p(k\,a) \pmod{p}$ para $1 \leq k \leq p-1$, se deduce

$$a \cdot 2\,a \cdots (p-1)\,a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

Es decir

$$(p-1)!\,a^{p-1} \equiv (p-1)! \pmod{p}.$$

Pero se puede simplificar $(p-1)!$ en el último renglón dado que $p \nmid (p-1)!$ (ya que $p \mid (p-1)!$ si y solo si existe k con $1 \leq k \leq p-1$ tal que $p \mid k$), luego

$$a^{p-1} \equiv 1 \pmod{p},$$

como se quería probar. □

Corolario 5.4.4. (Congruencia y potencias.)

Sea p un primo positivo. Entonces $\forall\, a \in \mathbb{Z}$ tal que $p \nmid a$ y $n \in \mathbb{N}$, se tiene

$$n \equiv r \ \big(\mathrm{mod}\,(p-1)\big) \implies a^n \equiv a^r \pmod{p}.$$

En particular,

$$p \nmid a \implies a^n \equiv a^{r_{p-1}(n)} \pmod{p}.$$

Demostración.

$$n = k\,(p-1)+r \implies a^n = a^{k(p-1)+r} = (a^{(p-1)})^k\,a^r \underset{\text{PTF}}{\equiv} 1^k\,a^r \equiv a^r \pmod{p}.$$

□

Ejemplos:

- Calcular $r_{11}(27^{2154})$:

  Como $27 \equiv 5 \pmod{11}$, $27^{2154} \equiv 5^{2154} \pmod{11}$. También, como $11 \nmid 5$, se tiene que

  $$5^{2154} \equiv 5^{r_{10}(2154)} \equiv 5^4 \equiv 25^2 \equiv 3^2 \equiv 9 \pmod{11}.$$

  Por lo tanto $r_{11}(27^{2154}) = 9$.

- Calcular $r_{11}(24^{13^{1521}})$:

  $$24^{13^{1521}} \equiv 2^{13^{1521}} \pmod{11}.$$

  Como $11 \nmid 2$, necesitamos calcular $r_{10}(13^{1521})$:

  $$13^{1521} \equiv 3^{1521} \equiv (3^2)^{760}\,3 \equiv (-1)^{760}\,3 \equiv 3 \pmod{10}.$$

  Por lo tanto $r_{10}(13^{1521}) = 3$, y

  $$2^{13^{1521}} \equiv 2^3 \equiv 8 \pmod{11},$$

  es decir $r_{11}(24^{13^{1521}}) = 8$.

- Determinar los $n \in \mathbb{N}$ tales que $4^n \equiv 1 \pmod{7}$:

  $4^n \equiv 4^r \pmod{7}$ si $n \equiv r \pmod{6}$, por el PTF ya que $7 \nmid 4$. Luego alcanza con investigar los valores de 4^r con $0 \le r < 6$:

  $$\begin{aligned}
  n \equiv 0 \pmod{6} &\implies 4^n \equiv 4^0 \equiv 1 \pmod{7},\\
  n \equiv 1 \pmod{6} &\implies 4^n \equiv 4^1 \equiv 4 \pmod{7},\\
  n \equiv 2 \pmod{6} &\implies 4^n \equiv 4^2 \equiv 2 \pmod{7},\\
  n \equiv 3 \pmod{6} &\implies 4^n \equiv 4^3 \equiv 4^2 \cdot 4 \equiv 2 \cdot 4 \equiv 1 \pmod{7},\\
  n \equiv 4 \pmod{6} &\implies 4^n \equiv 4^4 \equiv 4^3 \cdot 4 \equiv 1 \cdot 4 \equiv 4 \pmod{7},\\
  n \equiv 5 \pmod{6} &\implies 4^n \equiv 4^5 \equiv 4^3 \cdot 4^2 \equiv 1 \cdot 2 \equiv 2 \pmod{7}.
  \end{aligned}$$

  Se concluye que $4^n \equiv 1 \pmod{7} \iff n \equiv 0 \pmod{6}$ o $n \equiv 3 \pmod{6}$, es decir:

  $$4^n \equiv 1 \pmod{7} \iff n \equiv 0 \pmod{3}.$$

- Probar que $\forall\ a \in \mathbb{Z},\ 7 \mid a^{362} - a^{62}$:

  Aquí para usar la versión más rápida del PTF, es conveniente separar los casos en que $7 \mid a$ y $7 \nmid a$:

$$\begin{aligned} 7 \mid a &\Longrightarrow a^{362} \equiv 0 \pmod 7 \ \text{ y } \ a^{62} \equiv 0 \pmod 7 \\ &\Longrightarrow a^{362} \equiv a^{62} \pmod 7, \\ 7 \nmid a &\Longrightarrow a^{362} \equiv a^2 \pmod 7 \ \text{ y } \ a^{62} \equiv a^2 \pmod 7 \\ &\Longrightarrow a^{362} \equiv a^{62} \pmod 7. \end{aligned}$$

  Por lo tanto, en ambos casos, $a^{362} \equiv a^{62} \pmod 7$.

- Calcular el resto de dividir $n := 3^{2^{25}}$ por 390:

  Como $390 = 2 \cdot 3 \cdot 5 \cdot 13$ es un producto de primos distintos, se puede averiguar el resto de dividir n por cada uno de esos primos (aplicando si fuera necesario el PTF) y luego combinar los resultados por medio del TCR.

  - $r_2(n)$:
$$3^{2^{25}} \equiv 1^{2^{25}} \equiv 1 \pmod 2.$$
  - $r_3(n)$:
$$3^{2^{25}} \equiv 0^{2^{25}} \equiv 0 \pmod 3.$$
  - $r_5(n)$:
    Por el PTF (Consecuencia 5.4.4), ya que 5 es primo,
$$3^{2^{25}} \underset{5\nmid 3}{\equiv} 3^{r_4(2^{25})} \underset{4\mid 2^{25}}{\equiv} 3^0 \equiv 1 \pmod 5.$$
  - $r_{13}(n)$:
    Como $13 \nmid 3$, para aplicar el PTF, necesitamos conocer $r_{12}(2^{25})$. Para ello alcanza con conocer $r_3(2^{25})$ y $r_4(2^{25})$ y luego aplicar el TCR.
$$\begin{aligned} 2^{25} &\underset{\text{PTF},3\nmid 2}{\equiv} 2^{r_2(25)} \equiv 2^1 \equiv 2 \pmod 3 \quad \text{y} \quad 2^{25} \equiv 0 \pmod 4 \\ &\underset{\text{TCR}}{\Longrightarrow} \ 2^{25} \equiv 8 \pmod{12}. \end{aligned}$$
    Así,
$$3^{2^{25}} \equiv 3^{r_{12}(2^{25})} \equiv 3^8 \equiv (3^3)^2 \cdot 3^2 \equiv 9 \pmod{13}.$$

  Podemos ahora calcular $r_{390}(3^{2^{25}})$ por medio del TCR:

$$\begin{cases} n \equiv 1 \pmod 2 \\ n \equiv 0 \pmod 3 \\ n \equiv 1 \pmod 5 \\ n \equiv 9 \pmod{13} \end{cases} \underset{\text{TCR}}{\Longleftrightarrow} \quad n \equiv 321 \pmod{390}.$$

Se concluye que $r_{390}(3^{2^{25}}) = 321$.

- Determinar todos los $a \in \mathbb{Z}$ tales que $(12\,a^{41} - a^{31} - a : 55) = 11$:

  Como $55 = 5 \cdot 11$, para $b \in \mathbb{Z}$ cualquiera, el valor de $(b : 55)$ puede ser en principio 1, 5, 11 o 55. Por lo tanto, se observa que

  $$(b : 55) = 11 \iff 11 \mid b \text{ y } 5 \nmid b.$$

  Determinamos entonces para qué valores de $a \in \mathbb{Z}$, $11 \mid 12\,a^{41} - a^{31} - a$ y $5 \nmid 12\,a^{41} - a^{31} - a$:

  - Para el 11:

    $$11 \mid 12\,a^{41} - a^{31} - a = a\,(12\,a^{40} - a^{30} - 1) \underset{11 \text{ primo}}{\iff} 11 \mid a \text{ o } 11 \mid 12\,a^{40} - a^{30} - 1.$$

    Pero si $11 \nmid a$, por el PTF, $a^n \equiv a^{r_{10}(n)} \pmod{11}$. Luego en ese caso,

    $$12\,a^{40} - a^{30} - 1 \equiv 1\,a^0 - a^0 - 1 \equiv -1 \pmod{11} \implies 11 \nmid a^{40} - a^{30} - 1.$$

    Por lo tanto

    $$11 \mid 12\,a^{41} - a^{31} - a \iff 11 \mid a.$$

  - Para el 5:

    $$5 \mid 12\,a^{41} - a^{31} - a = a\,(12\,a^{40} - a^{30} - 1) \underset{5 \text{ primo}}{\iff} 5 \mid a \text{ o } 5 \mid 12\,a^{40} - a^{30} - 1.$$

    Pero si $5 \nmid a$, entonces, por el PTF, $12\,a^{40} - a^{30} - 1 \equiv 2\,a^0 - a^2 - 1 \equiv 1 - a^2 \pmod{5}$. Mirando las posibles congruencias de $a^2 \pmod{5}$, se tiene

    $$1 - a^2 \equiv 0 \pmod{5} \iff a^2 \equiv 1 \pmod{5} \iff a \equiv 1 \text{ o } 4 \pmod{5}.$$

    Por lo tanto

    $$\begin{aligned} 5 \mid 12\,a^{41} - a^{31} - a &\iff a \equiv 0 \text{ o } 1 \text{ o } 4 \pmod{5}, \\ 5 \nmid 12\,a^{41} - a^{31} - a &\iff a \equiv 2 \text{ ó } 3 \pmod{5}. \end{aligned}$$

  Se concluye aplicando el TCR:

  $$\begin{aligned} (12\,a^{41} - a^{31} - a : 55) = 11 &\iff \begin{cases} a \equiv 0 \pmod{11} \\ a \equiv 2 \text{ o } 3 \pmod{5} \end{cases} \\ &\iff a \equiv 22 \text{ o } 33 \pmod{55}. \end{aligned}$$

- Determinar todos los $a \in \mathbb{Z}$ tales que

$$a \equiv 1 \pmod 4 \quad \text{y} \quad (11\,a + 3 \cdot 2^{150} : 3\,a - 2^{151}) = 31.$$

Veamos primero cuáles son los posibles valores del mcd para ver las condiciones que necesitamos. Sea d un divisor común. Entonces:

$$\left\{ \begin{array}{l} d \mid 11\,a + 3 \cdot 2^{150} \\ d \mid 3\,a - 2^{151} \end{array} \right. \implies \left\{ \begin{array}{l} d \mid 33\,a + 9 \cdot 2^{150} \\ d \mid 33\,a - 11 \cdot 2^{151} \end{array} \right. \implies d \mid 31 \cdot 2^{150}.$$

$$\left\{ \begin{array}{l} d \mid 11\,a + 3 \cdot 2^{150} \\ d \mid 3\,a - 2^{151} \end{array} \right. \implies \left\{ \begin{array}{l} d \mid 22\,a + 3 \cdot 2^{151} \\ d \mid 9\,a - 3 \cdot 2^{151} \end{array} \right. \implies d \mid 31 \cdot a.$$

Ahora bien,

$$d \mid 31 \cdot 2^{150} \ \text{ y } \ d \mid 31 \cdot a \iff d \mid (31 \cdot 2^{150} : 31 \cdot a) = 31\,(2^{150} : a) = 31$$

pues $a \equiv 1 \pmod 4$ implica que a es impar, por lo tanto coprimo con 2^{150}.

Por lo tanto, el mcd puede ser 1 o 31. Para que sea 31 nos tenemos que asegurar que $31 \mid 11\,a + 3 \cdot 2^{150}$ y que $31 \mid 3\,a - 2^{151}$. Pero por el PTF, al ser 31 primo que no divide a 2, se tiene:

$$\begin{aligned} 31 \mid 11\,a + 3 \cdot 2^{150} &\iff 11\,a + 3 \cdot 2^{150} \equiv 0 \pmod{31} \\ &\underset{\text{PTF}}{\iff} 11\,a + 3 \cdot 2^{r_{30}(150)} \equiv 0 \pmod{31} \\ &\iff 11\,a + 3 \equiv 0 \pmod{31} \\ &\iff a \equiv 11 \pmod{31}. \end{aligned}$$

Hay que verificar entonces si $a \equiv 11 \pmod{31}$ implica $31 \mid 3\,a - 2^{151}$:

$$a \equiv 11 \pmod{31} \underset{\text{PTF}}{\implies} 3\,a - 2^{151} \equiv 3 \cdot 11 - 2^{r_{30}(151)} \equiv 33 - 2 \equiv 0 \pmod{31}.$$

Se concluye el ejercicio con el TCR:

$$\left\{ \begin{array}{l} a \equiv 1 \pmod 4 \\ a \equiv 11 \pmod{31} \end{array} \right. \iff a \equiv 73 \pmod{124}.$$

- Determinar $r_{315}(5\,a^{18} + 7\,b^{115} + 8^{40})$ sabiendo que $(5\,a : 7\,b) = 15$.

Como $315 = 3^2 \cdot 5 \cdot 7$, conviene encontrar los restos módulo 3^2, 5 y 7 para luego aplicar el TCR.

– Para el 3^2:
Como $(5\,a : 7\,b) = 15$, se tiene

$$15 \mid 5\,a \implies 3 \mid a, \quad \text{y por lo tanto } 3^2 \mid a^{18}$$
$$15 \mid 7\,b \underset{15\perp 7}{\iff} 15 \mid b, \quad \text{y por lo tanto } 3^2 \mid b^{115}.$$

Luego

$$5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 8^{40} \equiv (-1)^{40} \equiv 1 \pmod{3^2}.$$

– Para el 5:
Por lo visto arriba, $5 \mid b$, y así:

$$5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 3^{40} \underset{\text{PTF}}{\equiv} 1 \pmod 5.$$

– Para el 7:
La condición $(5\,a : 7\,b) = 15$ dice en particular que $7 \nmid a$ (pues sino, como $7 \mid 7\,b$, se tendría que 7 divide al mcd). Por lo tanto

$$5\,a^{18} + 7\,b^{115} + 8^{40} \underset{\text{PTF}}{\equiv} 5 \cdot 1 + 1^{40} \equiv 6 \pmod 7.$$

Se concluye aplicando el TCR:

$$\begin{cases} 5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 1 \pmod{3^2} \\ 5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 1 \pmod 5 \\ 5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 6 \pmod 7 \end{cases} \iff 5\,a^{18} + 7\,b^{115} + 8^{40} \equiv 181 \pmod{315}.$$

Por lo tanto $r_{315}(5\,a^{18} + 7\,b^{115} + 8^{40}) = 181$.

5.4.1 Tests probabilísticos de primalidad.

El PTF permite obtener directamente tests de primalidad, que funcionan muy rápido y son muy utilizados constantemente. Estos tests funcionan de la manera siguiente: dado un número $m \in \mathbb{N}$ del cual se quiere averiguar si es un número primo, se elije al azar un número a, $1 < a < m$, y se hace un test (generalmente se chequea una igualdad que involucra a m y a, asociada al test). Si la igualdad no se satisface, es que m es un número compuesto (y a es un testigo del hecho que m es compuesto). Si la igualdad se satisface, m puede ser primo o compuesto. Repitiendo el test eligiendo al azar otro número a se puede mejorar la probabilidad de éxito del test. La ventaja de estos tests es que son rápidos (más rápidos obviamente que la Criba de Eratóstenes y cualquiera de su variantes, pero también que el test de primalidad AKS que comentamos antes, cuya mejor versión hace del orden de (algo más que) $\log(m)^6$ cuentas), y los números que los pasan pueden ser considerados primos "a efectos prácticos". En la próxima sección,

veremos el sistema criptográfico RSA que necesita generar números primos muy grandes, en forma rápida...

Vamos a describir aquí dos tests probabilísticos de primalidad sencillos, que usan sólo herramientas conocidas, más que nada para dar un sabor de cómo funcionan.

- **El test del Pequeño Teorema de Fermat:** ¿$a^{m-1} \equiv 1 \pmod{m}$?

  Dado $m \in \mathbb{N}$, $m \geq 2$, se elige al azar a, $1 < a < m$, y se calcula $a^{m-1} \pmod{m}$.

  - Si $a^{m-1} \not\equiv 1 \pmod{m}$, claramente m no puede ser primo, luego es compuesto.
  - Si $a^{m-1} \equiv 1 \pmod{m}$, m es declarado "probablemente primo": puede ser primo o compuesto.

  Por ejemplo, para $m = 341 = 11 \cdot 31$, es fácil ver que para $a = 2$, $2^{340} \equiv 1 \pmod{341}$, y sin embargo m es compuesto.

  Lo interesante es que por ejemplo hay solamente 21853 números compuestos menores que $25 \cdot 10^9$ que pasan el test para $a = 2$, o sea menos que $1/1000000$... Este test funciona como una buena limpieza inicial de números compuestos.

  Lo malo es que como sabemos existen números compuestos, los seudoprimos o números de Carmichael, que pasan el test para (casi) cualquier elección de $a < m$ (salvo que uno caiga justo en uno de los divisores de m). O sea que aún eligiendo al azar distintos valores de a no aumentamos la probabilidad de obtener un resultado correcto para esos números, y hay infinitos números de Carmichael!

- **El test de primalidad de Miller-Rabin.**

  Este test fue originalmente propuesto por Gary Miller en 1976, pero dependía de un importante conjetura matemática no probada aún, la *Hipótesis de Riemann*. Fue modificado en 1980 por Michael Rabin para volverlo probabilístico.

  Se basa en el resultado siguiente.

  Proposición 5.4.5. *Sea $p > 2$ un número primo, y sea $p - 1 = 2^s d$ donde d es un número impar. Sea $a \in \mathbb{N}$, $1 \leq a < p$. Entonces se tiene que $a^{2^r d} \equiv -1 \pmod{p}$ para algún r con $s - 1 \geq r \geq 0$ o sino $a^d \equiv 1 \pmod{p}$.*

  Demostración. Sabemos por el PTF que $a^{p-1} = a^{2^s d} \equiv 1 \pmod{p}$ pues $a < p$ implica $a \perp p$. Como $p - 1$ es par, se tiene $s \geq 1$ y por

Miller

Rabin

lo tanto

$$a^{2^s d} - 1 = (a^{2^{s-1} d})^2 - 1 = (a^{2^{s-1} d} + 1)(a^{2^{s-1} d} - 1).$$

Luego

$$p \mid a^{2^s d} - 1 \implies p \mid a^{2^{s-1} d} + 1 \text{ o } p \mid a^{2^{s-1} d} - 1,$$

por ser p primo. Es decir

$$a^{p-1} = a^{2^s d} \equiv 1 \pmod{p} \implies a^{2^{s-1} d} \equiv -1 \pmod{p} \text{ o } a^{2^{s-1} d} \equiv 1 \pmod{p}.$$

Si $a^{2^{s-1} d} \equiv -1 \pmod{p}$ ya está. Sino, $a^{2^{s-1} d} \equiv 1 \pmod{p}$ y podemos repetir el procedimiento (si $s - 1 \geq 1$):

$$a^{2^{s-2} d} \equiv -1 \pmod{p} \text{ o } a^{2^{s-2} d} \equiv 1 \pmod{p}.$$

Nuevamente, si $a^{2^{s-2} d} \equiv -1 \pmod{p}$ ya está. Sino, $a^{2^{s-2} d} \equiv 1 \pmod{p}$ y repetimos el procedimiento, hasta llegar eventualmente a $a^{2d} \equiv 1 \pmod{p}$. Lo que implica

$$a^d \equiv -1 \pmod{p} \text{ o } a^d \equiv 1 \pmod{p}.$$

□

El test de primalidad de Miller-Rabin funciona negando la conclusión de esta proposición.

Dado $m \in \mathbb{N}$, m impar tal que $m - 1 = 2^s d$, se elige al azar $a \in \mathbb{N}$, $1 < a < m$, y se calcula $a^d \pmod{m}$ y $a^{2^r d} \pmod{m}$ para $0 \leq r \leq s - 1$.

- Si $a^d \not\equiv 1 \pmod{m}$ y $a^{2^r d} \not\equiv -1 \pmod{m}$ para $0 \leq r \leq s - 1$, entonces m es compuesto.
- Si $a^d \equiv 1 \pmod{m}$ o $\exists r$, $0 \leq r \leq s - 1$, tal que $a^{2^r d} \equiv -1 \pmod{m}$, entonces am es *probablemente primo*, o sea puede existir la posibilidad que sea compuesto pero "en general" será primo.

Por ejemplo para $m = 221 = 13 \cdot 17$, si se toma $a = 174$, resulta que m pasa el test y sin embargo m es compuesto. Sin embargo en este caso si se toma $a = 137$, a no pasa el test y se concluye que 221 es compuesto.

Lo interesante y que hace funcionar muy bien este test probabilístico, es que para cada número impar compuesto m hay al menos un testigo a para el cual el test falla, o sea que prueba que a es compuesto (en ese sentido es mucho mejor que el test descrito arriba). Es más, para cada m compuesto, se puede probar que hay del orden de $3m/4$ testigos a que prueban que m es compuesto. Por lo tanto, al repetir el test se aumenta la probabilidad de dar una respuesta correcta. Lo malo es que no se sabe a priori, dado un m, quiénes son esos testigos...

Si se corre este algoritmo k veces, la cantidad de cuentas que se hace es el orden de $k \log^3 m$ (lineal en esa cantidad) y la probabilidad de que un número sea declarado probablemente primo siendo compuesto es menor que $1/4^k$.

5.5 El sistema criptográfico RSA.

Este sistema criptográfico, que fue introducido en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman, es un sistema de clave pública-clave privada y de firma digital, que se basa en una generalización del Pequeño Teorema de Fermat para números de la forma $n = p \cdot q$, donde p y q son dos primos distintos.

La aplicación va a ser descrita en forma muy resumida aquí, y no va a contemplar los aspectos de implementación sino simplemente tener en cuenta los aspectos teóricos matemáticos. Para más información se recomienda buscar en Internet.

¿Cuál es el objetivo de la criptografía? Mandar mensajes en forma secreta y segura... Codificar información (un mensaje) de manera que solo el receptor al cual va dirigido el mensaje lo pueda decodificar (entender) y ninguna otra persona que llegue a interceptar el mensaje lo pueda entender. Convenimos que un mensaje es un número a, por ejemplo simplemente asignándole a cada letra del alfabeto un valor numérico y yuxtaponiendo esos valores. También podemos convenir en que ese número a es menor o igual que cierto número n, recortando el mensaje a original en bloquecitos si hace falta.

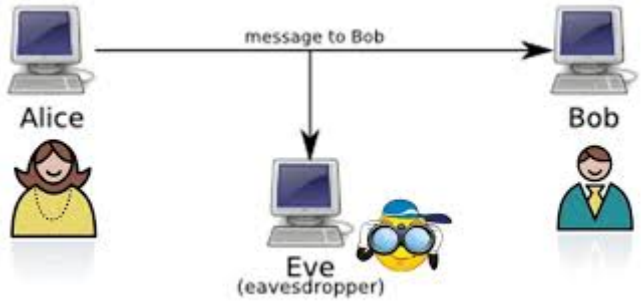
¿Qué se entiende por clave pública-clave privada? Un señor, Bob, va a generar dos claves, una que se llama *clave privada* que va a ser conocida sólo por él, y la otra, que se llama *clave pública* que va a distribuir al resto del mundo. Tanto la clave pública como la privada sirven para codificar o decodificar mensajes, pero una sola de ellas no puede hacer las dos cosas

Rivest

Shamir

Adleman

a la vez. Cuando Bob mantiene secreta su clave privada y le distribuye al resto del mundo su clave pública, el sistema RSA sirve para lo siguiente:



- Cualquier persona del resto del mundo, por ejemplo Alice, le puede mandar un mensaje encriptado a Bob usando la clave pública. Bob es el único que puede decodificar el mensaje, usando su clave privada. Ninguna otra persona del resto del mundo, por ejemplo Eve, puede decodificar ese mensaje.

- Bob le puede mandar al resto del mundo un mensaje encriptado usando su clave privada. Cualquiera del resto del mundo, al usar la clave pública de Bob, puede decodificar y luego entender ese mensaje, y por lo tanto, como el mensaje tiene sentido, tiene garantía que el emisor (el firmante) del mensaje fue realmente Bob.

Para seguir con esto, necesitamos esta pequeña generalización del pequeño teorema de Fermat, que es un caso particular del teorema de Euler mencionado previamente.

Proposición 5.5.1. (PTF para $p\,q$.)

Sean p, q dos primos positivos distintos, y sea $a \in \mathbb{Z}$ coprimo con $p\,q$. Entonces

$$a^{(p-1)(q-1)} \equiv 1 \pmod{p\,q}.$$

Y por lo tanto, $\forall\, m \in \mathbb{N}$,

$$m \equiv r \ \big(\mathrm{mod}\,(p-1)(q-1)\big) \implies a^m \equiv a^r \pmod{p\,q}.$$

Demostración. Como a es coprimo con $p\,q$, es en particular coprimo con p y con q. Luego, por el PTF,

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{y} \quad a^{q-1} \equiv 1 \pmod{q}.$$

Por lo tanto,

$$\begin{aligned} a^{(p-1)(q-1)} &= \big(a^{p-1}\big)^{q-1} \equiv 1^{q-1} \equiv 1 \pmod{p} \quad \text{y} \\ a^{(p-1)(q-1)} &= \big(a^{q-1}\big)^{p-1} \equiv 1^{p-1} \equiv 1 \pmod{q}. \end{aligned}$$

Por lo tanto, por la Proposición 5.3.1,

$$a^{(p-1)(q-1)} \equiv 1 \pmod{p\,q}.$$

La segunda afirmación se prueba como el Corolario 5.4.4:

$$\begin{aligned} &m = k\,(p-1)(q-1) + r \\ &\quad \Longrightarrow\ a^m = a^{k(p-1)(q-1)+r} = (a^{(p-1)(q-1)})^k\,a^r \equiv 1^k\,a^r \equiv a^r \pmod{p\,q}. \end{aligned}$$

□

¿Cómo funciona el sistema criptográfico RSA?

- Bob elige dos primos distintos muy grandes p y q (hay generadores de primos para eso) y los multiplica entre sí creándose el número $n = p\,q$. (Como ya se comentó, una vez multiplicados los dos primos, es muy costoso recuperarlos, es decir es muy costoso factorizar n.)

- Luego elige e coprimo con $(p-1)\,(q-1)$, con $1 \leq e \leq (p-1)\,(q-1)$. (Lo puede hacer ya que conoce p y q, por lo tanto puede calcular $p-1$ y $q-1$, y el producto $(p-1)(q-1)$, y verificar si e es coprimo con $(p-1)(q-1)$ se hace mediante el algoritmo de Euclides.)

- Finalmente calcula d con $1 \leq d \leq (p-1)\,(q-1)$ tal que $e\,d \equiv 1 \pmod{(p-1)(q-1)}$. (Como $e \perp (p-1)(q-1)$ la ecuación tiene solución, que se puede calcular utilizando el algoritmo de Euclides, pero para calcular d se necesita conocer $(p-1)(q-1)$, o sea p y q.)

Ahora fija las claves:

- Clave privada de Bob: (n, e).

- Clave pública de Bob: (n, d).

Observación 5.5.2. (Propiedad clave por la cual funciona el algoritmo RSA.)

Sean $n = p \cdot q$, d, e como arriba. Sea $a \in \mathbb{N}$ con $1 \leq a < n$. Entonces

$$a^{e\,d} \equiv a \pmod{n}.$$

Demostración.

- Si $a \perp p\,q$, entonces $a^{(p-1)(q-1)} \equiv 1 \pmod{n}$ y luego por la Proposición 5.5.1,
$$a^{e\,d} \equiv a^1 \pmod{n}.$$

- Si $p \mid a$ pero $q \nmid a$, entonces

$$\begin{aligned} a \equiv 0 \pmod{p} &\implies a^{e\,d} \equiv 0 \pmod{p} \implies a^{e\,d} \equiv a \pmod{p} \\ a^{q-1} \equiv 1 \pmod{q} &\implies a^{(p-1)(q-1)} \equiv 1 \pmod{q} \\ &\implies a^{e\,d} \equiv a^1 \equiv a \pmod{q}. \end{aligned}$$

  Por lo tanto, $a^{e\,d} \equiv a \pmod{p\,q}$.

  Análogamente se prueba que $a^{e\,d} \equiv a \pmod{p\,q}$ para $p \nmid a$ pero $q \mid a$.

- Si $p \mid a$ y $q \mid a$, entonces

$$a \equiv 0 \pmod{p\,q} \implies a^{e\,d} \equiv 0 \pmod{p\,q} \implies a^{e\,d} \equiv a \pmod{p\,q}.$$

□

Mecanismo del sistema criptográfico RSA:

Dado el mensaje a, $0 \leq a < n$, notemos por $C(a)$ el mensaje encriptado.

1. Caso 1: Alice le quiere mandar a Bob el mensaje a y que solo Bob lo entienda: le manda el mensaje encriptado $C(a)$, donde:

   $$C(a) \equiv a^d \pmod{n} \text{ con } 0 \leq C(a) < n.$$

   Para decodificarlo, Bob aplica la aplicación "inversa" que consiste en elevar a la e y tomar resto módulo n. Se tiene

   $$C(a)^e \equiv (a^d)^e \equiv a^{e\,d} \equiv a \pmod{n},$$

   luego el resto módulo n de $C(a)^e$ coincide con el mensaje a.

2. Caso 2: Bob le quiere mandar el mensaje a "firmado por él" al resto del mundo: manda el mensaje encriptado $C(a)$ donde

$$C(a) \equiv a^e \pmod{n} \text{ con } 0 \leq C(a) < n.$$

Para decodificarlo, el resto del mundo aplica la aplicación "inversa" que consiste en elevar a la d y tomar resto módulo n. Se tiene

$$C(a)^d \equiv (a^e)^d \equiv a^{e\,d} \equiv a \pmod{n},$$

luego el resto módulo n de $C(a)^d$ coincide con a.

5.6 El anillo $\mathbb{Z}/m\mathbb{Z}$ y el cuerpo $\mathbb{Z}/p\mathbb{Z}$.

5.6.1 El anillo $\mathbb{Z}/m\mathbb{Z}$.

Ejemplos:

- Consideremos primero la relación de equivalencia congruencia módulo 2, y sus clases de equivalencia. Sabemos que $a \equiv b \pmod{2} \Leftrightarrow r_2(a) = r_2(b)$: todos los pares son congruentes entre sí y todos los impares son congruentes entre sí. Por lo tanto, hay dos clases de equivalencia, determinadas por los dos restos módulo 2, que son 0 y 1:

$$\overline{0} = \{a \in \mathbb{Z} : \ a \equiv 0 \pmod{2}\} = \{a \in \mathbb{Z} : \ a \text{ es par }\},$$
$$\overline{1} = \{a \in \mathbb{Z} : \ a \text{ es impar }\}.$$

Así, $\mathbb{Z} = \overline{0} \cup \overline{1}$ es la partición de $\mathbb{Z}$ asociada a la relación de equivalencia *congruencia módulo* 2. Pero más aún, es claro que la suma de pares siempre da par, la suma de impares siempre da par, la suma de un par y un impar siempre da impar, independientemente de qué par o qué impar se elija. O sea se puede considerar la operación suma en el conjunto $\{\overline{0}, \overline{1}\}$ de las clases de equivalencia:

$$\overline{0} + \overline{0} = \overline{0}, \quad \overline{1} + \overline{0} = \overline{1}, \quad \overline{0} + \overline{1} = \overline{1}, \quad \overline{1} + \overline{1} = \overline{0}.$$

Lo mismo ocurre con el producto: multiplicar un par por cualquier número siempre da par, y multiplicar impar por impar da impar. Así:

$$\overline{0} \cdot \overline{0} = \overline{0}, \quad \overline{1} \cdot \overline{0} = \overline{0}, \quad \overline{0} \cdot \overline{1} = \overline{0}, \quad \overline{1} \cdot \overline{1} = \overline{1}.$$

Estas operaciones $+$ y $\cdot$ en el conjunto $\{\overline{0}, \overline{1}\}$ de clases de equivalencia satisfacen todas las propiedades de anillo conmutativo: la suma es

conmutativa, asociativa, hay un elemento neutro que es el $\overline{0}$ y todo elemento tiene opuesto aditivo: $-\overline{0} = \overline{0}, -\overline{1} = \overline{1}$, o sea $(\{\overline{0}, \overline{1}\}, +)$ es un grupo abeliano. El producto es conmutativo, asociativo, hay un elemento neutro que es el $\overline{1}$. Y además el producto es distributivo sobre la suma. Por lo tanto $(\{\overline{0}, \overline{1}\}, +, \cdot)$ es un anillo conmutativo. Este conjunto de restos módulo 2 se nota $\mathbb{Z}/2\mathbb{Z}$. O sea $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ es un anillo conmutativo con la suma y el producto.

Más aún, en este caso, todo elemento distinto del $\overline{0}$, es decir el $\overline{1}$, tiene inverso multiplicativo pues $\overline{1} \cdot \overline{1} = \overline{1}$ implica $\overline{1}^{-1} = \overline{1}$. Luego $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$ es más que un anillo conmutativo, es un *cuerpo*, al igual que $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$. Pero es un cuerpo finito ¡con solo 2 elementos!

- Miremos ahora la relación de equivalencia congruencia módulo 6: Sabemos que $a \in \mathbb{Z}$ es congruente módulo 6 a su resto $r_6(a)$, y que dos restos distintos no son congruentes entre sí. Dicho de otra manera, en $\mathbb{Z}$ se tienen 6 clases de equivalencia mod 6:

$$\begin{aligned}
\overline{0} &= \{a \in \mathbb{Z} : \ a \equiv 0 \pmod 6\} &&= \{\dots, -12, -6, 0, 6, 12, \dots\} \\
\overline{1} &= \{a \in \mathbb{Z} : \ a \equiv 1 \pmod 6\} &&= \{\dots, -11, -5, 1, 7, 13, \dots\} \\
\overline{2} &= \{a \in \mathbb{Z} : \ a \equiv 2 \pmod 6\} &&= \{\dots, -10, -4, 2, 8, 14, \dots\} \\
\overline{3} &= \{a \in \mathbb{Z} : \ a \equiv 3 \pmod 6\} &&= \{\dots, -9, -3, 3, 9, 15, \dots\} \\
\overline{4} &= \{a \in \mathbb{Z} : \ a \equiv 4 \pmod 6\} &&= \{\dots, -8, -2, 4, 10, 16, \dots\} \\
\overline{5} &= \{a \in \mathbb{Z} : \ a \equiv 5 \pmod 6\} &&= \{\dots, -7, -1, 5, 11, 17, \dots\}
\end{aligned}$$

y $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4} \cup \overline{5}$ es la partición de $\mathbb{Z}$ asociada a esta relación de equivalencia. Notemos

$$\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}.$$

También sabemos que si $a \in \overline{r_1}$ y $b \in \overline{r}_2$, eso significa que $a \equiv r_1 \pmod 6$ y $b \equiv r_2 \pmod 6$, y por lo tanto, $a + b \equiv r_1 + r_2 \pmod 6$ y $a \cdot b \equiv r_1 \cdot r_2 \pmod 6$. Es decir, $a + b \in \overline{r_1 + r_2}$ y $a \cdot b \in \overline{r_1 \cdot r_2}$.

Así tiene sentido considerar en el conjunto de clases de restos $\mathbb{Z}/6\mathbb{Z}$ las operaciones suma y producto entre clases dadas por las tablas siguientes:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{2}$	$\overline{4}$

y

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

(Aquí no importa en qué sentido se hacen las operaciones: si columna + fila o fila + columna, etc., pues son claramente conmutativas.) Estas operaciones hacen de $(\mathbb{Z}/6\mathbb{Z}), +, \cdot)$ un anillo conmutativo ¡con

6 elementos! El elemento neutro para la suma es el $\overline{0}$ (notemos que $-\overline{0}=\overline{0}$, $-\overline{1}=\overline{5}$, $-\overline{2}=\overline{4}$, $-\overline{3}=\overline{3}$, $-\overline{4}=\overline{2}$ y $-\overline{5}=\overline{1}$) y el elemento neutro para el producto es $\overline{1}$. Pero en este caso $\mathbb{Z}/6\mathbb{Z}$ no es un cuerpo, pues por ejemplo $\overline{2}$ no tiene inverso multiplicativo: no existe otro elemento tal que multiplicado por él de $\overline{1}$.

Enunciemos ahora sin demostrar todos los detalles el resultado en el caso general.

Teorema 5.6.1. (El anillo $\mathbb{Z}/m\mathbb{Z}$.)

Sea $m \in \mathbb{N}$ y consideremos en $\mathbb{Z}$ la relación de equivalencia congruencia módulo m. *Entonces*

1. *Sea $0 \leq r < m$. La clase de equivalencia $\overline{r}$ de r es*

$$\overline{r} = \{a \in \mathbb{Z} : \ a \equiv r \pmod{m}\}$$

y

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \cdots \cup \overline{m-1}$$

es la partición de $\mathbb{Z}$ asociada a esta relación de equivalencia.

2. *Notemos*

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\},$$

y sean $+$ y $\cdot$ las operaciones en $\mathbb{Z}/m\mathbb{Z}$ definidas por

$$\overline{r}_1 + \overline{r}_2 = \overline{r_1 + r_2} \quad y \quad \overline{r}_1 \cdot \overline{r}_2 = \overline{r_1 \cdot r_2}, \quad para \ \ 0 \leq r_1, r_2 < m.$$

Entonces $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ es un anillo conmutativo.

5.6.2 El cuerpo $\mathbb{Z}/p\mathbb{Z}$.

Como vimos en el Corolario 5.2.4, cuando a y m son coprimos, la ecuación de congruencia $a \cdot X \equiv c \pmod{m}$ siempre tiene solución independientemente de quién sea c. En particular tiene solución para $c = 1$. Esto implica directamente el resultado siguiente:

Proposición 5.6.2. (La ecuación de congruencia $a \cdot X \equiv 1 \pmod{m}$.)

Sea $m \in \mathbb{N}$ y sea $a \in \mathbb{Z}$. Entonces la ecuación de congruencia $a \cdot X \equiv 1 \pmod{m}$ tiene soluciones si y solo si $a \perp m$. En ese caso, hay una única solución x_0 con $1 \leq x_0 < m$.

Demostración. Cuando $a \not\perp m$, no hay solución pues $(a : m) \nmid 1$.

Por el contrario, cuando $a \perp m$, la ecuación tiene solución. Todas las soluciones son de la forma $X \equiv x_0 \pmod{m}$ donde x_0 es la única solución

que satisface $0 \leq x_0 < m$. Pero no puede ser $x_0 = 0$ pues sino se tendría $a \cdot 0 \equiv 1 \pmod{m}$, contradicción! Luego $1 \leq x_0 < m$.

□

Ejemplo: Soluciones de la ecuación $a \cdot X \equiv 1 \pmod{10}$ para $a = 1, 3, 7, 9$.

- $1 \cdot X \equiv 1 \pmod{10} \leftrightsquigarrow X \equiv 1 \pmod{10}$ $(x_0 = 1)$.
- $3 \cdot X \equiv 1 \pmod{10} \leftrightsquigarrow X \equiv 7 \pmod{10}$ $(x_0 = 7)$.
- $7 \cdot X \equiv 1 \pmod{10} \leftrightsquigarrow X \equiv 3 \pmod{10}$ $(x_0 = 3)$.
- $9 \cdot X \equiv 1 \pmod{10} \leftrightsquigarrow X \equiv 9 \pmod{10}$ $(x_0 = 9)$.

Apliquemos la Proposición 5.6.2 al caso en que m es un número primo p.

Corolario 5.6.3. (La ecuación de congruencia $a \cdot X \equiv 1 \pmod{p}$.)

Sea p un primo positivo y sea $a \in \mathbb{N}$ tal que $p \nmid a$. Entonces la ecuación de congruencia $a \cdot X \equiv 1 \pmod{p}$ tiene una única solución x_0 con $1 \leq x_0 < p$.

Ejemplo: Soluciones de la ecuación $a \cdot X \equiv 1 \pmod{7}$ para $a = 1, 2, 3, 4, 5, 6$.

- $1 \cdot X \equiv 1 \pmod{7} \leftrightsquigarrow X \equiv 1 \pmod{7}$ $(x_0 = 1)$.
- $2 \cdot X \equiv 1 \pmod{7} \leftrightsquigarrow X \equiv 4 \pmod{7}$ $(x_0 = 4)$.
- $3 \cdot X \equiv 1 \pmod{7} \leftrightsquigarrow X \equiv 5 \pmod{7}$ $(x_0 = 5)$.
- $4 \cdot X \equiv 1 \pmod{7} \leftrightsquigarrow X \equiv 2 \pmod{7}$ $(x_0 = 2)$.
- $5 \cdot X \equiv 1 \pmod{7} \leftrightsquigarrow X \equiv 3 \pmod{7}$ $(x_0 = 3)$.
- $6 \cdot X \equiv 1 \pmod{7} \leftrightsquigarrow X \equiv 6 \pmod{7}$ $(x_0 = 6)$.

La Proposición 5.6.2 permite también determinar directamente quiénes son los elementos inversibles del anillo $\mathbb{Z}/m\mathbb{Z}$.

Corolario 5.6.4. (Los elementos inversibles de $\mathbb{Z}/m\mathbb{Z}$.)

Sea $m \in \mathbb{N}$, y sea $\overline{r} \in \mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$.

Entonces, $\overline{r}$ es inversible en $\mathbb{Z}/m\mathbb{Z}$ si y solo si $r \perp m$.

Demostración. Se tiene $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$. El elemento $\overline{r}$ es inversible en $\mathbb{Z}/m\mathbb{Z}$ si y solo si existe $\overline{x} \in \mathbb{Z}/m\mathbb{Z}$ tal que $\overline{r} \cdot \overline{x} = \overline{1}$. Pero por la definición del producto en $\mathbb{Z}/m\mathbb{Z}$, $\overline{r} \cdot \overline{x} = \overline{r \cdot x}$, luego hay que determinar x tal que $\overline{r \cdot x} = \overline{1}$, o lo que es lo mismo $r \cdot x \equiv 1 \pmod{m}$. Se concluye por la Proposición 5.6.2. □

Ejemplo: En $\mathbb{Z}/10\mathbb{Z}$,

$$\overline{1}^{\,-1} = \overline{1},\ \overline{3}^{\,-1} = \overline{7},\ \overline{7}^{\,-1} = \overline{3} \text{ y } \overline{9}^{\,-1} = \overline{9}.$$

Traduciendo el Corolario 5.6.4 al anillo $\mathbb{Z}/p\mathbb{Z}$ de enteros módulo p, se obtiene directamente el importante resultado siguiente.

Teorema 5.6.5. ($\mathbb{Z}/p\mathbb{Z}$ es un cuerpo.)

Sea p un primo positivo. Entonces $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ es un cuerpo.

Es decir, además de ser un anillo conmutativo con la suma y el producto definidos en el Teorema 5.6.1, se satisface que todo elemento no nulo de $\mathbb{Z}/p\mathbb{Z}$ es inversible.

Ejemplo: En $\mathbb{Z}/7\mathbb{Z}$,

$$\overline{1}^{\,-1} = \overline{1},\ \overline{2}^{\,-1} = \overline{4},\ \overline{3}^{\,-1} = \overline{5},\ \overline{4}^{\,-1} = \overline{2},\ \overline{5}^{\,-1} = \overline{3} \text{ y } \overline{6}^{\,-1} = \overline{6}.$$

5.7 Ejercicios.

Ecuaciones diofánticas y de congruencia

1. Determinar, cuando existan, todos los $(a, b) \in \mathbb{Z}^2$ que satisfacen

   i) $7a + 11b = 10$
   ii) $20a + 16b = 36$
   iii) $39a - 24b = 6$
   iv) $1555a - 300b = 11$

2. Determinar todos los $(a, b) \in \mathbb{Z}^2$ que satisfacen simultáneamente $4 \mid a$, $8 \mid b$ y $33a + 9b = 120$.

3. Si se sabe que cada unidad de un cierto producto A cuesta 39 pesos y que cada unidad de un cierto producto B cuesta 48 pesos, ¿cuántas unidades de cada producto se pueden comprar gastando exactamente 135 pesos?

4. Hallar, cuando existan, todas las soluciones de las siguientes ecuaciones de congruencia

   i) $17X \equiv 3\ (11)$
   ii) $56X \equiv 28\ (35)$
   iii) $56X \equiv 2\ (884)$
   iv) $78X \equiv 30\ (12126)$

5. Hallar todos los $(a, b) \in \mathbb{Z}^2$ tales que $b \equiv 2a \pmod 5$ y $28a + 10b = 26$.

6. Hallar el resto de la división de un entero a por 18, sabiendo que el resto de la división de $7a$ por 18 es 5.

7. Hallar todas las soluciones $(x, y) \in \mathbb{Z}^2$ de la ecuación

$$110x + 250y = 100$$

que satisfacen simultáneamente que $37^2 \mid (x - y)^{4321}$.

8. Hallar todos los $a \in \mathbb{Z}$ para los cuales $(2a - 3 : 4a^2 + 10a - 10) \neq 1$.

9. Describir los valores de $(5a + 8 : 7a + 3)$ en función de los valores de $a \in \mathbb{Z}$.

Teorema chino del resto

10. Hallar, cuando existan, todos los enteros a que satisfacen simultáneamente:

i) $\begin{cases} a \equiv 3 & (10) \\ a \equiv 2 & (7) \\ a \equiv 5 & (9) \end{cases}$ ii) $\begin{cases} a \equiv 1 & (6) \\ a \equiv 2 & (20) \\ a \equiv 3 & (9) \end{cases}$ iii) $\begin{cases} a \equiv 1 & (12) \\ a \equiv 7 & (10) \\ a \equiv 4 & (9) \end{cases}$

11. Hallar, cuando existan, todos los enteros a que satisfacen simultáneamente:

i) $\begin{cases} 3\,a \equiv 4 & (5) \\ 5\,a \equiv 4 & (6) \\ 6\,a \equiv 2 & (7) \end{cases}$ ii) $\begin{cases} 3\,a \equiv 1 & (10) \\ 5\,a \equiv 3 & (6) \\ 9\,a \equiv 1 & (14) \end{cases}$ iii) $\begin{cases} 15\,a \equiv 10 & (35) \\ 21\,a \equiv 15 & (8) \\ 18\,a \equiv 24 & (30) \end{cases}$

12. i) Sabiendo que los restos de la división de un entero a por 6, 10 y 8 son 5, 3 y 5 respectivamente, hallar los posibles restos de la división de a por 480.

ii) Hallar el menor entero positivo a tal que el resto de la división de a por 21 es 13 y el resto de la división de $6a$ por 15 es 9.

13. En un depósito se almacenan latas de gaseosa. El viernes por la noche, un empleado realizó un control de inventario y observó que:

- Al poner las latas en cajas de 12 unidades sobraban 4.

- Al poner las latas en cajas de 63 unidades sobraban 43.
- Había por lo menos 12.600 latas y no más de 13.000, pero no tomó nota de la cantidad exacta.

¿Cuántas latas de gaseosa había en el depósito el viernes por la noche?

14. Hallar los posibles restos de dividir a un entero a por 238 sabiendo que $a^2 \equiv 21\ (238)$.

Pequeño teorema de Fermat

15. Hallar el resto de la división de a por p en los casos

    i) $a = 71^{22283}$, $p = 11$

    ii) $a = 5 \cdot 7^{2451} + 3 \cdot 65^{2345} - 23 \cdot 8^{138}$, $p = 13$

16. Resolver en $\mathbb{Z}$ las ecuaciones de congruencia

    i) $2^{194}X \equiv 7\ (97)$ ii) $5^{86}X \equiv 3\ (89)$

17. Probar que para todo $a \in \mathbb{Z}$ vale

    i) $728 \mid a^{27} - a^3$ ii) $\dfrac{2a^7}{35} + \dfrac{a}{7} - \dfrac{a^3}{5} \in \mathbb{Z}$

18. Sea $a \in \mathbb{Z}$ coprimo con 561. Probar que $a^{560} \equiv 1\ (561)$.
    (Un número $n \in \mathbb{N}$ se dice un *seudoprimo o número de Carmichael* si satisface el Pequeño Teorema de Fermat sin ser primo, es decir, si a es un entero coprimo con n, entonces $a^{n-1} \equiv 1 \pmod{n}$. Estos números se llaman así por Robert Carmichael, matemático estadounidense, 1879-1967. En 1994 se probó finalmente que hay infinitos números de Carmichael.)

19. Resolver en $\mathbb{Z}$ los siguientes sistemas lineales de ecuaciones de congruencia

    i) $\begin{cases} 2^{2013}X \equiv 6 & (13) \\ 5^{2013}X \equiv 4 & (7) \\ 7^{2013}X \equiv 2 & (5) \end{cases}$ ii) $\begin{cases} 10^{49}X & \equiv 17 & (39) \\ 5X & \equiv 7 & (9) \end{cases}$

20. Hallar el resto de la división de

    i) $3 \cdot 7^{135} + 24^{78} + 11^{222}$ por 70

    ii) $\sum_{i=1}^{1759} i^{42}$ por 56

21. Hallar el resto de la división de 2^{2^n} por 13 para cada $n \in \mathbb{N}$.

22. Resolver en $\mathbb{Z}$ la ecuación de congruencia $7\,X^{45} \equiv 1 \pmod{46}$.

23. Hallar todos los divisores positivos de 25^{70} que sean congruentes a 2 módulo 9 y a 3 módulo 11.

24. Hallar todos los primos $p \in \mathbb{N}$ que satisfacen:

    i) $2p \mid 38^{2p^2-p-1} + 3p + 171$ ii) $3p \mid 5^{p-1} + 3^{p^2+2} + 833$

25. Hallar los posibles restos de dividir a un entero a por 44 sabiendo que $(a^{760} + 11a + 10 : 88) = 2$.

El anillo $\mathbb{Z}/m\mathbb{Z}$

26. Escribir las tablas de suma y producto en $\mathbb{Z}/m\mathbb{Z}$ para $m = 5$ y 8. ¿Alguno de estos anillos es un cuerpo?

27. Un elemento $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ es un *cuadrado* (en $\mathbb{Z}/m\mathbb{Z}$) si existe $\overline{b} \in \mathbb{Z}/m\mathbb{Z}$ tal que $\overline{a} = \overline{b}^2$ en $\mathbb{Z}/m\mathbb{Z}$.

    i) Calcular los cuadrados en $\mathbb{Z}/m\mathbb{Z}$ para $m = 2$, 3, 4, 9 y 11. ¿Cuántos hay en cada caso?

    ii) Sea $p \in \mathbb{N}$ primo. Probar que, en $\mathbb{Z}/p\mathbb{Z}$, si $\overline{a}^2 = \overline{b}^2$ entonces $\overline{a} = \overline{b}$ ó $\overline{a} = -\overline{b}$. Deducir que si p es impar, entonces hay exactamente $\dfrac{p-1}{2}$ cuadrados no nulos en $\mathbb{Z}/p\mathbb{Z}$.

28. Describir el conjunto $\{\overline{3}^n : n \in \mathbb{N}\}$ en $\mathbb{Z}/7\mathbb{Z}$ y en $\mathbb{Z}/11\mathbb{Z}$. Observar la diferencia que hay en el primer caso con respecto al segundo caso, y hallar si se puede un elemento $\overline{a} \in \mathbb{Z}/11\mathbb{Z}$ que cumpla que $\{\overline{a}^n : n \in \mathbb{N}\} = \mathbb{Z}/11\mathbb{Z} - \{\overline{0}\}$.

29. Sea p un primo. Probar que en $\mathbb{Z}/p\mathbb{Z}$ vale que $(\overline{a} + \overline{b})^p = \overline{a}^p + \overline{b}^p$, $\forall\, \overline{a}, \overline{b} \in \mathbb{Z}/p\mathbb{Z}$ (sug: ver Ej. 25 Práctica 4). ¿Vale lo mismo en $\mathbb{Z}/m\mathbb{Z}$ si m no es primo?

30. *Test de Primalidad de Wilson:*
El objetivo de este ejercicio es probar que si $n \in \mathbb{N}$ es distinto de 1, entonces

$$(n-1)! \equiv -1 \pmod{n} \iff n \text{ es primo .}$$

i) Verificar que $3! \not\equiv -1\,(4)$ y probar que si $n \geq 5$ es compuesto, entonces $(n-1)! \equiv 0 \pmod{n}$. ¿Qué implicación se prueba con esto?

ii) Sea p un primo positivo. Se recuerda que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo. Probar que $\overline{a} = \overline{a}^{-1}$ en $\mathbb{Z}/p\mathbb{Z}$ si y solo si $\overline{a} = \pm\overline{1}$. Deducir que $(p-1)! \equiv -1 \pmod{p}$.

(Este test de primalidad debe su nombre al matemático inglés John Wilson, 1741-1793, pero era conocido mucho antes por los árabes, y fue de hecho probado por primera vez por el matemático italiano Joseph-Louis Lagrange en 1771).

Capítulo 6

Números Complejos.

El próximo capítulo tratará sobre los polinomios con coeficientes en un cuerpo K. Hasta ahora mencionamos en la materia varios ejemplos de cuerpos: el cuerpo de los números racionales $\mathbb{Q}$, el cuerpo de los números reales $\mathbb{R}$, el cuerpo de los números complejos $\mathbb{C}$, los cuerpos finitos $\mathbb{Z}/p\mathbb{Z}$, para p un número primo, aunque nunca introdujimos la definición formal. A continuación definimos la noción de cuerpo y hacemos un repaso exhaustivo del cuerpo de los números complejos orientado a lo que nos interesa que es estudiar polinomios con coeficientes complejos.

6.1 Cuerpos.

Definición 6.1.1. (Cuerpo.)

Sea K un conjunto, y sean $+, \cdot : K \times K \to K$ dos operaciones en K (usualmente la suma y el producto). Se dice que $(K, +, \cdot)$ es un *cuerpo* si

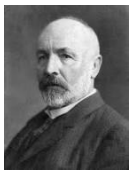
- $+$ y $\cdot$ son operaciones asociativas y conmutativas. Es decir $\forall\, x, y, z \in K$ se tiene $(x+y)+z = x+(y+z)$ y $(x\cdot y)\cdot z = x\cdot(y\cdot z)$ (asociatividad) y $\forall\, x, y \in K$ se tiene $x + y = y + x$ y $x \cdot y = y \cdot x$.
- Existe un elemento neutro para la suma, que se nota 0_K, es decir $\forall\, x \in K$ se tiene $x + 0_K = x$, y un elemento neutro para el producto, que se nota 1_K, es decir $\forall\, x \in K$ se tiene $x \cdot 1_K = x$.
- Cualquiera sea $x \in K$, x tiene un inverso aditivo, u opuesto, que se nota $-x$, es decir $x + (-x) = 0_K$, y cualquiera sea $x \in K$, $x \neq 0$, x tiene un inverso multiplicativo que se nota x^{-1}, es decir $x \cdot x^{-1} = 1_K$.
- La operación $\cdot$ es distributiva sobre $+$, es decir $\forall\, x, y, z \in K$ se tiene $x \cdot (y + z) = x \cdot y + x \cdot z$.

Estas propiedades implican en particular que $0 \cdot x = 0$, $\forall x \in K$, pues $0 = 0 + 0 \Rightarrow 0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, y por lo tanto sumando de cada lado $-0 \cdot x$ se obtiene $0 \cdot x = 0$. También se deduce que $\forall x, y \in K$ no nulos, vale que $x \cdot y \neq 0$ pues si fuera $x \cdot y = 0$ con $x \neq 0$ entonces, como existe x^{-1}, se tendría $y = x^{-1} \cdot x \cdot y = x^{-1} \cdot 0 = 0$.

En particular, cuando K es un cuerpo, notando $K^\times := K - \{0\}$, se tiene que $\cdot : K^\times \times K^\times \to K^\times$, y tanto $(K, +)$ como $(K^\times, \cdot)$ son grupos abelianos.

La información siguiente es en su mayoría extraída de Wikipedia.

Lo números naturales ya eran conocidos desde el principio de los tiempos, pero claro, no se podía "restar". Los números racionales positivos, las fracciones positivas, (que permiten "dividir") ya eran utilizadas de alguna manera por los Egipcios alrededor del año 1000 AC, y luego también por los griegos. Los números negativos aparecieron por primera vez en un libro de matemática de la Dinastía Han en China (202 AC-202 DC), y también en un manuscrito indio escrito en algún momento entre los años 200 AC y 400 DC. Matemáticos indios $\sim$ 700 AC y griegos $\sim$ 500 AC ya reconocían el concepto de irracionalidad (en particular con $\sqrt{2}$). Durante el Medioevo los árabes ya trataban a los números irracionales como entidades algebraicas, y asociaron los conceptos de números y magnitudes.



En el Siglo XVI apareció la notación decimal de los números reales, pero fue recién en 1871 cuando Georg Cantor realizó la descripción rigurosa de los números reales, uno de los avances matemáticos más importantes del Siglo XIX, mostrando en particular que hay muchos más números irracionales que racionales.

6.2 Números complejos: forma binomial.

Con respecto a los números complejos, la primera referencia conocida a raíces cuadradas de números negativos proviene del trabajo de los matemáticos griegos, como Herón de Alejandría en el Siglo I AC, como resultado de una imposible sección de una pirámide.

Los complejos se hicieron más patentes en el Siglo XVI, cuando la búsqueda de fórmulas que dieran las raíces exactas de los polinomios de grado 3 fueron encontradas por matemáticos italianos como Scipione del Ferro (1465-1526), Niccolo Fontana Tartaglia (1499-1557) y Gerolamo Cardano (1501-1576): aunque sólo estaban interesados en las raíces reales de este tipo de ecuaciones, se encontraban con la necesidad de lidiar con raíces de números negativos. Las reglas para la suma, resta, producto y división fueron desarrolladas por el matemático italiano Rafael Bombelli (1526-1572). El término imaginario para estas cantidades (y real para los números reales) fue acuñado por Descartes en el Siglo XVII. Muchos matemáticos contribu-

del Ferro

Tartaglia

Cardano

Bombelli

yeron al desarrollo completo de los números complejos.

Lo que todos sabemos es que no existe ningún número real r que satisface $r^2 = -1$, dado que el cuadrado de un número real siempre es un número real ≥ 0. Luego se introduce una cantidad *imaginaria* i, que no pertenece a $\mathbb{R}$, que satisface $i^2 = -1$. Se "agrega" esa cantidad al cuerpo de los números reales, construyendo el "menor" conjunto que contiene a $\mathbb{R}$ y a i, y donde se puede sumar y multiplicar (respetando la distributividad): a este conjunto lo llamamos el conjunto de los números *complejos* $\mathbb{C}$.

Al estar $a, b \in \mathbb{R} \subset \mathbb{C}$ e $i \in \mathbb{C}$, tiene que estar $b \cdot i \in \mathbb{C}$, y luego también $a + b \cdot i \in \mathbb{C}$. O sea $\{z = a + b \cdot i;\ a, b \in \mathbb{R}\} \subset \mathbb{C}$.

Pero observemos que dados $a+b\cdot i, c+d\cdot i \in \mathbb{C}$, con $a, b, c, d \in \mathbb{R}$, entonces si operamos respetando la distributividad,

- $(a + b \cdot i) + (c + d \cdot i) = (a + c) + (b + d) \cdot i$.
- $(a+b\cdot i)\cdot(c+d\cdot i) = ac+ad\cdot i+bc\cdot i+bd\cdot i^2 = (ac-bd)+(ad+bc)\cdot i$.

O sea la suma y el producto de estos números tienen la misma forma: un número real + otro número real multiplicado por i. Es decir, el menor conjunto donde tiene sentido sumar y multiplicar números de la forma $a+b\cdot i$ con $a, b \in \mathbb{R}$ es el conjunto

$$\mathbb{C} = \{z = a + b \cdot i;\ a, b \in \mathbb{R}\},$$

donde si $z = a + b \cdot i$, $\omega = c + d \cdot i \in \mathbb{C}$ con $a, b, c, d \in \mathbb{R}$, entonces $z = \omega \Leftrightarrow a = c$ y $b = d$.

Teorema 6.2.1. (El cuerpo de los números complejos.)

$$(\mathbb{C}, +, \cdot) \text{ es un cuerpo.}$$

Demostración. • La operación $+$ es conmutativa y es asociativa pues lo es sobre los números reales. Además $0 = 0 + 0 \cdot i \in \mathbb{C}$ es el elemento neutro para la suma, y el opuesto aditivo de $z = a+b\cdot i$, con $a, b \in \mathbb{R}$, es $-z = -a - b \cdot i \in \mathbb{C}$.

- Se puede verificar que la operación $\cdot$ es conmutativa y asociativa también. El elemento $1 = 1 + 0 \cdot i \in \mathbb{C}$ es el elemento neutro para el producto, y para todo $z = a + b \cdot i \neq 0$, con $a, b \in \mathbb{R}$, se tiene que existe

$$z^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} \cdot i \ \in \ \mathbb{C},$$

pues si $z \neq 0$, $a^2 + b^2 > 0$, por lo tanto es un denominador permitido, y es fácil verificar que $(a + bi) \cdot \Big(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i\Big) = \frac{a^2 - (-b^2)}{a^2 + b^2} + \frac{\big(a(-b) + ba\big)}{a^2 + b^2} = 1 + 0\, i = 1$.

- También se puede verificar que la operación $\cdot$ es distributiva sobre $+$ pues lo es en $\mathbb{R}$: para todo $z, \omega, \omega' \in \mathbb{C}$ se tiene

$$z(\omega + \omega') = z\omega + z\omega'.$$

□

Por lo tanto el cuerpo $\mathbb{C}$ es un cuerpo que "contiene" al cuerpo de los números reales $\mathbb{R}$: $\forall\, a \in \mathbb{R},\ a = a + 0 \cdot i \in \mathbb{C}$.

Se gana al extender de esa forma el cuerpo $\mathbb{R}$ que la ecuación $X^2 + 1 = 0$ tiene solución en $\mathbb{C}$, y probaremos más adelante que todas las ecuaciones cuadráticas $z\, X^2 + \omega\, X + u = 0$ con $z, \omega, u \in \mathbb{C}$, z, ω no ambos nulos, tienen solución en $\mathbb{C}$. En realidad veremos sin demostración un resultado mucho más general: que todas las ecuaciones de cualquier grado con coeficientes complejos tienen solución en $\mathbb{C}$ (éste es el renombrado Teorema Fundamental del Álgebra).

Se pierde que en $\mathbb{C}$ no se puede establecer ningún orden $\geq$ como tienen los números reales: no hay ninguna forma de establecer un orden completo $\geq$ en $\mathbb{C}$ (es decir una relación reflexiva, antisimétrica y transitiva, que satisface además $z \geq \omega$ o $\omega \geq z$, $\forall\, z, \omega \in \mathbb{C}$) que respete la suma ($z \geq z' \Rightarrow z + \omega \geq z' + \omega$, $\forall\, \omega \in \mathbb{C}$) y el producto por no negativos ($z \geq 0$ y $\omega \geq 0 \ \Rightarrow\ z\,\omega \geq 0$): pues si $i \geq 0$ entonces $i^2 = -1 \geq 0$ implica $0 = -1 + 1 \geq 0 + 1 = 1$, pero por otro lado, $1 = (-1)^2 \geq 0^2 = 0$. Es decir $0 \geq 1$ y $1 \geq 0$. Por la antisimetría, eso tendría que implicar $0 = 1$, contradicción. Un razonamiento análogo prueba que no puede ser $0 \geq i$.

Ejemplos:

- $i^2 = -1,\ i^3 = -i,\ i^4 = 1$ y en general,

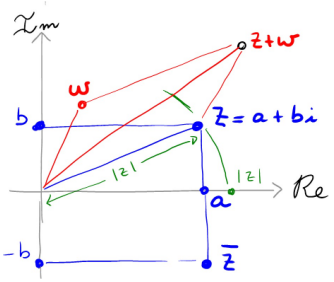
$$i^{4n} = 1,\ i^{4n+1} = i,\ i^{4n+2} = -1,\ i^{4n+3} = -i, \quad \forall\, n \in \mathbb{N}_0.$$

- Para todo $a, b \in \mathbb{R}$, $(a+b\,i)^2 = a^2 - b^2 + 2\,a\,b\,i$ y $(a+b\,i)\cdot(a-b\,i) = a^2+b^2 \in \mathbb{R}_{\geq 0}$.

Definición 6.2.2. (Forma binomial, parte real, parte imaginaria, conjugado, módulo.)

- Dado $z \in \mathbb{C}$, la forma $z = a + b\cdot i$ con $a, b \in \mathbb{R}$ se llama la *forma binomial* de z, su parte real es $\Re e(z) := a \in \mathbb{R}$ y su parte imaginaria es $\Im m(z) := b \in \mathbb{R}$.
- Dado $z = a + b\,i$ con $a, b \in \mathbb{R}$, el *conjugado* de z es $\overline{z} := a - b\,i \in \mathbb{C}$, y el *módulo* de z es $|z| = \sqrt{a^2+b^2} \in \mathbb{R}_{\geq 0}$. Observemos que $|z| = 0 \Leftrightarrow z = 0$, y que si $z \neq 0$, entonces $|z| \in \mathbb{R}_{>0}$.

Se representa z y esas cantidades en el *plano complejo*, así como la operación suma, que se hace con la regla del paralelogramo. Se nota que por el Teorema de Pitágoras, $|z| = \operatorname{dist}(z, 0)$, es decir $|z| \geq 0$ mide la distancia del número complejo z al origen 0.



Además se tiene las siguientes relaciones entre $\overline{z}$ y $|z|$:

$$z\cdot\overline{z} = |z|^2, \quad \forall\, z \in \mathbb{C} \qquad \text{y} \qquad z^{-1} = \frac{\overline{z}}{|z|^2}, \quad \forall\, z \in \mathbb{C}^\times.$$

Proposición 6.2.3. (Propiedades del conjugado y del módulo.)

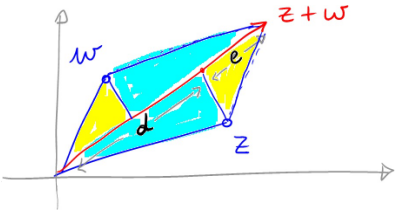
Para todo $z \in \mathbb{C}$, se tiene

- $\overline{\overline{z}} = z$,
- $z = \overline{z} \;\Leftrightarrow\; z \in \mathbb{R}$,
- $z + \overline{z} = 2\,\Re e(z)$,
- $z - \overline{z} = 2\,\Im m(z)\,i$,
- $|\Re e(z)| \leq |z|$ e $|\Im m(z)| \leq |z|$.

Además, para todo $z, \omega \in \mathbb{C}$, se tiene

- $\overline{z+\omega} = \overline{z} + \overline{\omega}$.
- $\overline{z\cdot\omega} = \overline{z}\cdot\overline{\omega}$.
- *Si* $z \neq 0$, $\overline{z^{-1}} = \overline{z}^{-1}$.
- *Si* $z \neq 0$, $\overline{z^k} = \overline{z}^k$, $\forall\, k \in \mathbb{Z}$.
- $|z+\omega| \leq |z| + |\omega|$.
- $|z\cdot\omega| = |z|\cdot|\omega|$
- *Si* $z \neq 0$, $|z^{-1}| = |z|^{-1}$.
- *Si* $z \neq 0$, $|z^k| = |z|^k$, $\forall\, k \in \mathbb{Z}$.

La propiedad $|z+\omega| \le |z| + |\omega|$ se llama la *desigualdad triangular* y se puede comprobar geométricamente:



$d \le |z|$, $e \le |\omega| \implies |z+\omega| = d+e \le |z|+|\omega|$

Podemos probar aquí en forma muy simple que al construir $\mathbb{C}$ agregándole a $\mathbb{R}$ la raíz cuadrada i de -1, se consigue que en $\mathbb{C}$ todos los números complejos tengan raíces cuadradas, y no solo -1 o los números reales negativos b, cuyas raíces cuadradas son $\pm\sqrt{|b|}\,i$.

Proposición 6.2.4. (Raíces cuadradas de números complejos.)

Sea $z \in \mathbb{C}$. Entonces existe $\omega \in \mathbb{C}$ tal que $\omega^2 = (-\omega)^2 = z$. Si $z \neq 0$, entonces z tiene exactamente dos raíces cuadradas distintas, que son ω y $-\omega$.

Hagamos un ejemplo antes de hacer la demostración.

Ejemplo: Calcular las raíces cuadradas complejas de $z = 3 - 4\,i$.

Planteemos $\omega^2 = z$ donde $\omega = x + y\,i \in \mathbb{C}$ con $x, y \in \mathbb{R}$ a determinar. Esto implica $|\omega^2| = |z|$, es decir $|\omega|^2 = |z|$ también. Por lo tanto, de $\omega^2 = 3 - 4\,i$ y $|\omega|^2 = |3 - 4\,i| = \sqrt{25} = 5$, obtenemos las ecuaciones:

$$\begin{cases} x^2 - y^2 + 2xy\,i = 3 - 4\,i \\ x^2 + y^2 = 5 \end{cases} \iff \begin{cases} x^2 - y^2 = 3 \\ 2xy = -4 \\ x^2 + y^2 = 5. \end{cases}$$

De la primera ecuación $2x^2 = 5 + 3 = 8$, y de la tercera $2y^2 = 5 - 3 = 2$. Luego

$$x = \pm\sqrt{\frac{8}{2}} = \pm\sqrt{4} = \pm 2 \quad \text{e} \quad y = \pm\sqrt{\frac{2}{2}} = \pm\sqrt{1} = \pm 1.$$

O sea que en principio tenemos 4 posibilidades, eligiendo x e y positivos y/o negativos. Pero la segunda condición nos dice que $x\,y = -2$, el producto es negativo, por lo tanto si se toma $x = 2$ se debe tomar $y = -1$ y si se toma $x = -2$ se debe tomar $y = 1$: los candidatos a raíces cuadradas son entonces

$$\omega = 2 - i \quad \text{y} \quad \omega' = -\omega = -2 + i.$$

Efectivamente, es inmediato verificar que $\omega^2 = (-\omega)^2 = (4-1) + 2(-2)\,i = 3 - 4\,i$.

Demostración. (de la Proposición 6.2.4.)

Sea $z = a + b\,i \in \mathbb{C}$, con $a, b \in \mathbb{R}$, y planteemos $\omega^2 = z$ donde $\omega = x + y\,i \in \mathbb{C}$ con $x, y \in \mathbb{R}$ a determinar.

Si $z = 0$, entonces $\omega = 0$.

Luego podemos asumir $z \neq 0$. La condición $\omega^2 = z$ implica $|\omega^2| = |z|$, es decir $|\omega|^2 = |z|$ también. Por lo tanto, de $\omega^2 = z$ y $|\omega|^2 = |z|$ obtenemos las ecuaciones:

$$\begin{cases} x^2 - y^2 + 2xy\,i = a + b\,i \\ x^2 + y^2 = \sqrt{a^2 + b^2} \end{cases} \iff \begin{cases} x^2 - y^2 = a \\ 2xy = b \\ x^2 + y^2 = \sqrt{a^2 + b^2} \end{cases}$$

De la primera ecuación y la tercera deducimos

$$2x^2 = \sqrt{a^2 + b^2} + a \quad \text{y} \quad 2y^2 = \sqrt{a^2 + b^2} - a.$$

Observemos que tanto $\sqrt{a^2 + b^2} + a$ como $\sqrt{a^2 + b^2} - a$ son números reales no negativos por la propiedad $|\Re e(z)| \leq |z|$ que dice que valen tanto $a \leq \sqrt{a^2 + b^2}$ como $-a \leq \sqrt{a^2 + b^2}$. Por lo tanto existen las raíces cuadradas reales

$$x = \pm\sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} \in \mathbb{R} \quad \text{e} \quad y = \pm\sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}} \in \mathbb{R}.$$

Esto nos daría en principio 4 posibles candidatos para ω. Pero solo dos de ellas son en realidad candidatos: las dos que cumplen con la segunda condición $2xy = b$: si $b \geq 0$, hay que tomar

$$x = \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}}\,, y = \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}} \quad \text{y}$$
$$x = -\sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}}\,, y = -\sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}},$$

mientras que si $b < 0$, hay que tomar

$$x = \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}}\,, y = -\sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}} \quad \text{y}$$
$$x = -\sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}}\,, y = \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}}.$$

Observemos que en ambos casos se obtiene $\omega = x + y\,i$ y $\omega' = -\omega$. Verifiquemos finalmente que estas dos candidatos a solución ω y $\omega' = -\omega$ son efectivamente raíces cuadradas de z cuando $z \neq 0$. Como claramente $(-\omega)^2 = \omega^2$, alcanza con probarlo para

$$\omega = \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} \pm \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}}\,i$$

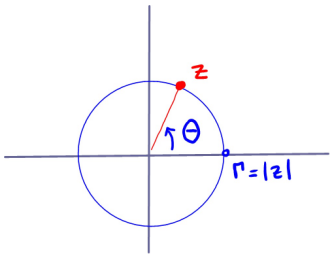
donde el $\pm$ es $+$ o $-$ dependiendo de si $b \geq 0$ o $b < 0$.

$$\begin{aligned}\omega^2 &= \Big(\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} \pm \sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\, i\Big)^2 \\ &= \Big(\frac{\sqrt{a^2+b^2}+a}{2} - \frac{\sqrt{a^2+b^2}-a}{2}\Big) \pm 2\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\, i \\ &= a \pm 2\sqrt{\frac{\sqrt{a^2+b^2}^{\,2}-a^2}{4}}\, i \;=\; a \pm \sqrt{b^2}\, i \;=\; a \pm |b|\, i \;=\; a + b\, i,\end{aligned}$$

pues si $b \geq 0$, $|b| = b$ y el signo en $\pm$ era $+$ mientras que si $b < 0$, $|b| = -b$ pero el signo en $\pm$ era $-$. □

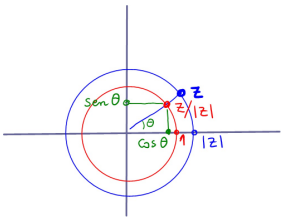
Más adelante probaremos que no sólo se consigue que todo número complejo tiene raíces cuadradas de números complejos, sino también que todo número complejo tiene raíces n-ésimas, para todo $n \in \mathbb{N}$, es decir que dado n, para todo $z \in \mathbb{C}$ existe $\omega \in \mathbb{C}$ tal que $\omega^n = z$. Para ello introducimos la forma trigonométrica o polar de los números complejos.

6.3 Números complejos: forma trigonométrica.



Sea $z \in \mathbb{C}^\times$. Entonces z no solo está determinado por su parte real $\Re e(z) \in \mathbb{R}$ y su parte imaginaria $\Im m(z) \in \mathbb{R}$, pero también se lo puede determinar de otra forma por su módulo $r = |z| \in \mathbb{R}_{>0}$, que determina en qué circunferencia se encuentra z, y por un ángulo θ con respecto a (por ejemplo) el semieje real positivo, como lo muestra el dibujo.

Dado $z \in \mathbb{C}^\times$, $z/|z|$ pertenece a la circunferencia unidad, pues $\big|z/|z|\big| = |z|/|z| = 1$, y por lo tanto sus coordenadas son de la forma $(\cos\theta, \operatorname{sen}\theta)$:



Luego,

$$z = r\,(\cos\theta + i\,\operatorname{sen}\theta)$$

donde

$$r = |z| \quad \text{y} \quad \theta \text{ es tal que } \cos\theta = \frac{\Re e(z)}{|z|} \text{ y } \operatorname{sen}\theta = \frac{\Im m(z)}{|z|}.$$

Vamos a adoptar para la expresión $\cos\theta + i\,\operatorname{sen}\theta$ la notación exponencial $e^{\theta i}$, que se denomina la *Fórmula de Euler* ya que él fue el primero en demostrar su validez:

$$e^{\theta i} = \cos\theta + i\,\operatorname{sen}\theta, \quad \forall\,\theta \in \mathbb{R}.$$

Por lo tanto $z = r\,e^{\theta i}$ donde $r = |z| \in \mathbb{R}_{>0}$ y $\theta \in \mathbb{R}$ es tal que $\cos\theta = \frac{\Re e(z)}{|z|}$ y $\operatorname{sen}\theta = \frac{\Im m(z)}{|z|}$.

El ángulo $\theta \in \mathbb{R}$ está por convención dado en radianes, que es una unidad de medida de ángulos sumamente útil ya que se corresponde con el perímetro del sector angular de la circunferencia unidad comprendido entre el ángulo 0 y el ángulo θ (contando todas las vueltas completas a la circunferencia que se dio). Por ejemplo el ángulo 2π radianes se corresponde con el perímetro 2π de la circunferencia unidad, el ángulo $\pi/2$ radianes se corresponde con el perímetro de un cuarto de circunferencia, y el ángulo 4π es lo que mide dar dos vueltas completas en la circunferencia unidad.

Claramente, el ángulo no está determinado en forma única, ya que sabemos que $\cos\theta = \cos(\theta + 2k\pi)$ y $\operatorname{sen}\theta = \operatorname{sen}(\theta + 2k\pi)$, $\forall\, k \in \mathbb{Z}$. Así,

$$e^{\theta i} = e^{(\theta+2k\pi)i}, \quad \forall\, k \in \mathbb{Z},$$

y más aún, para $r, s \in \mathbb{R}_{>0}$ y $\theta, \varphi \in \mathbb{R}$, se tiene

$$s\,e^{\varphi i} = r\,e^{\theta i} \iff \begin{cases} s = r \\ \varphi = \theta + 2k\pi \quad \text{para algún } k \in \mathbb{Z}. \end{cases}$$

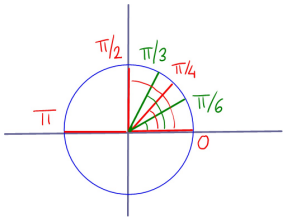
Si elegimos θ con $0 \le \theta < 2\pi$, entonces este ángulo está determinado en forma única y se denomina el *argumento de* z que se denota $\arg(z)$.

La *forma trigonométrica* o *polar* de $z \in \mathbb{C}^\times$ es

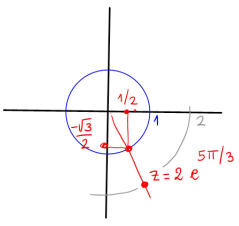
$$z = r\,(\cos\theta + i\,\operatorname{sen}\theta) \;=\; r\,e^{\theta i} \quad \text{con} \quad r \in \mathbb{R}_{>0} \;\text{ y }\; 0 \le \theta < 2\pi.$$

Repasemos los ángulos típicos con sus coseno y seno:

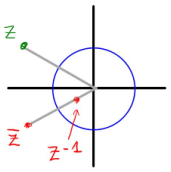
θ	0	$\pi/6$	$\pi/4$	$\pi/3$	$\pi/2$	π
$\cos\theta$	1	$\sqrt{3}/2$	$\sqrt{2}/2$	$1/2$	0	-1
$\operatorname{sen}\theta$	0	$1/2$	$\sqrt{2}/2$	$\sqrt{3}/2$	1	0



Ejemplo: Sea $z = 1 - \sqrt{3}\,i$. Entonces $z = r\,e^{i\theta}$ donde $r = |z| = \sqrt{1+3} = 2$ y $\theta \in \mathbb{R}$ es un ángulo tal que $\cos\theta = 1/2$, $\operatorname{sen}\theta = -\sqrt{3}/2$. Por lo tanto $\theta = -\pi/3$ o $\theta = -\pi/3 + 2k\pi$, $k \in \mathbb{Z}$. Se tiene $\arg(z) = -\pi/3 + 2\pi = 5\pi/3$, y $z = 2\,e^{\frac{5\pi}{3}i}$ es la forma trigonométrica de z.



Observación 6.3.1. Sea $z = r\,(\cos\theta + i\,\operatorname{sen}\theta) = r\,e^{\theta i}$ con $r \in \mathbb{R}_{>0}$ y $\theta \in \mathbb{R}$. Entonces



- $\overline{z} = r\,\big(\cos(-\theta) + i\,\operatorname{sen}(-\theta)\big) = r\,e^{-\theta i}$,
- $z^{-1} = r^{-1}\,\big(\cos(-\theta) + i\,\operatorname{sen}(-\theta)\big) = r^{-1}\,e^{-\theta i}$.

Demostración. El segundo inciso es porque $z^{-1} = \dfrac{\overline{z}}{|z|^2}$ y $|z^{-1}| = |z|^{-1}$. Por lo tanto z^{-1} está en la misma semirrecta que $\overline{z}$ (ya que es un múltiplo de $\overline{z}$ que se obtiene al multiplicar $\overline{z}$ por el número real positivo $1/|z|^2$). Por lo tanto $\overline{z}$ y z^{-1} vienen definidos por el mismo ángulo $-\theta$. □

A continuación vamos a recordar la Fórmula de de Moivre, que debe su nombre al matemático francés Abraham de Moivre, 1667-1754.

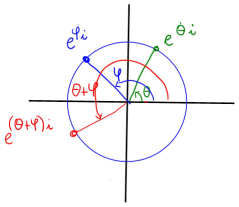
Teorema 6.3.2. (Fórmula de de Moivre.)

Sean $z = r\,(\cos\theta + i\,\operatorname{sen}\theta) = r\,e^{\theta i}$ *y* $\omega = s(\cos\varphi + i\,\operatorname{sen}\varphi) = s\,e^{\varphi i}$ *con* $r, s \in \mathbb{R}_{>0}$ *y* $\theta, \varphi \in \mathbb{R}$. *Entonces*

$$z \cdot \omega = rs\,\big(\cos(\theta+\varphi) + i\,\operatorname{sen}(\theta+\varphi)\big) = rs\,e^{(\theta+\varphi)i}.$$

Es decir

$$r\,e^{\theta i} \cdot s\,e^{\varphi i} = rs\,e^{(\theta+\varphi)i}.$$



En particular,

$$\arg(z \cdot \omega) = \arg(z) + \arg(\omega) - 2k\pi$$

con $k = 0$ *o* 1 *elegido de modo tal que*

$$0 \le \arg(z) + \arg(\omega) - 2k\pi < 2\pi.$$

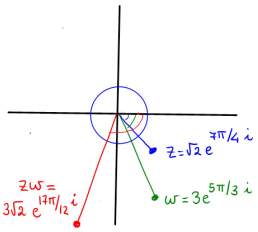
Demostración. Es una consecuencia muy simple de cómo es el producto de números complejos, y las fórmulas del coseno y seno de la suma de ángulos:

$$\begin{aligned} z \cdot \omega &= r\,(\cos\theta + i\,\operatorname{sen}\theta) \cdot s(\cos\varphi + i\,\operatorname{sen}\varphi) \\ &= rs\,\big((\cos\theta\cos\varphi - \operatorname{sen}\theta\operatorname{sen}\varphi) + i\,(\cos\theta\operatorname{sen}\varphi + \operatorname{sen}\theta\cos\varphi)\big) \\ &= rs\,\big((\cos(\theta+\varphi) + i\,(\operatorname{sen}(\theta+\varphi)\big). \end{aligned}$$

□

Ejemplo: Sean $z = \sqrt{2}\, e^{\frac{7\pi}{4} i}$ y $\omega = 3\, e^{\frac{5\pi}{3} i}$. Entonces

$$z \cdot \omega = \sqrt{2}\, e^{\frac{7\pi}{4} i} \cdot 3\, e^{\frac{5\pi}{3} i} = 3\sqrt{2}\, e^{(\frac{7\pi}{4} + \frac{5\pi}{3})i}$$
$$= 3\sqrt{2}\, e^{\frac{41\pi}{12} i} = 3\sqrt{2}\, e^{(\frac{41\pi}{12} - 2\pi)\, i} = 3\sqrt{2}\, e^{\frac{17\pi}{12} i}.$$



Por inducción en $n \in \mathbb{N}$ se puede deducir la fórmula para cualquier potencia n-ésima, $n \in \mathbb{Z}$.

Corolario 6.3.3. (Expresión trigonométrica de una potencia.)
Sean $z = r\,(\cos\theta + i\,\operatorname{sen}\theta) = r\, e^{\theta i}$ *y* $\omega = s(\cos\varphi + i\,\operatorname{sen}\varphi) = s\, e^{\varphi i}$ *con* $r, s \in \mathbb{R}_{>0}$ *y* $\theta, \varphi \in \mathbb{R}$. *Entonces*

- $\dfrac{z}{\omega} = \dfrac{r}{s}\left(\cos(\theta - \varphi) + i\,\operatorname{sen}(\theta - \varphi)\right) = \dfrac{r}{s}\, e^{(\theta - \varphi)i}$.
- $z^n = r^n \left(\cos(n\theta) + i\,\operatorname{sen}(n\theta)\right) = r^n\, e^{n\theta i}$, *para todo* $n \in \mathbb{Z}$.

En particular, $\arg(z^n) = n\,\arg(z) - 2k\pi$ *con* $k \in \mathbb{Z}$ *elegido de modo tal que* $0 \le n\,\arg(z) - 2k\pi < 2\pi$.

Ejemplos:

- Calcular la forma binomial de $\left(\dfrac{-1+i}{-2-2\sqrt{3}i}\right)^{10}$:

  Se tiene que $-1 + i = \sqrt{2}\, e^{\theta i}$ con $\theta \in \mathbb{R}$ tal que $\cos\theta = \frac{-1}{\sqrt{2}} = -\frac{\sqrt{2}}{2}$, $\operatorname{sen}\theta = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$, o sea $-1 + i = \sqrt{2}\, e^{\frac{3\pi}{4} i}$. Del mismo modo, $-2 - 2\sqrt{3}i = 4\, e^{\frac{4\pi}{3} i}$. Por lo tanto

  $$\left(\frac{-1+i}{-2-2\sqrt{3}i}\right)^{10} = \left(\frac{\sqrt{2}}{4}\right)^{10} e^{10\left(\frac{3\pi}{4} - \frac{4\pi}{3}\right)i} = \frac{2^5}{2^{20}}\, e^{\frac{-70\pi}{12} i}$$
  $$= 2^{-15}\, e^{(\frac{-70\pi}{12} + 3\cdot 2\pi)i} = 2^{-15}\, e^{\frac{\pi}{6} i} = \frac{\sqrt{3}}{2^{16}} + \frac{1}{2^{16}}\, i.$$

- Calcular todos los $n \in \mathbb{N}$ tales que $(1+i)^{2n} = (\sqrt{3} - i)^n$:

  Se tiene $1 + i = \sqrt{2}\, e^{\frac{\pi}{4} i}$ y por lo tanto

  $$(1+i)^{2n} = \sqrt{2}^{2n}\, e^{\frac{2n\pi}{4} i} = 2^n\, e^{\frac{n\pi}{2} i},$$

  y $\sqrt{3} - i = 2\, e^{\frac{-\pi}{6} i}$, y por lo tanto

  $$(\sqrt{3} - i)^n = 2^n\, e^{\frac{-n\pi}{6} i}.$$

Esto implica

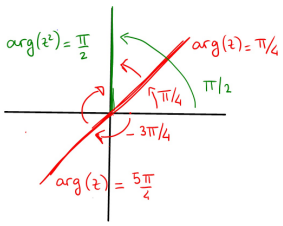
$$\begin{aligned}(1+i)^{2n} = (\sqrt{3}-i)^n &\iff \frac{n\pi}{2} = \frac{-n\pi}{6} + 2k\pi \text{ para algún } k \in \mathbb{Z} \\ &\iff \frac{2n\pi}{3} = 2k\pi \text{ para algún } k \in \mathbb{Z} \\ &\iff 2n\pi = 6k\pi \text{ para algún } k \in \mathbb{Z} \\ &\iff 3 \mid n.\end{aligned}$$

- Determinar todos los $z \in \mathbb{C}$ tales que $\arg(z^2) = \dfrac{\pi}{2}$:

  Sea $z = r\,e^{\theta i}$ con $0 \le \theta < 2\pi$. Entonces $\arg(z^2) = 2\theta - 2k\pi$ con $k \in \mathbb{Z}$ de modo tal que $0 \le 2\theta - 2k\pi < 2\pi$. Se tiene

  $$2\theta - 2k\pi = \frac{\pi}{2} \iff 2\theta = \frac{\pi}{2} + 2k\pi \iff \theta = \frac{\pi}{4} + k\pi.$$

  Para $k = 0$ se obtiene $\theta_0 = \dfrac{\pi}{4}$ y para $k = 1$ se obtiene $\theta_1 = 5\pi/4$. Luego los ángulos se van repitiendo:

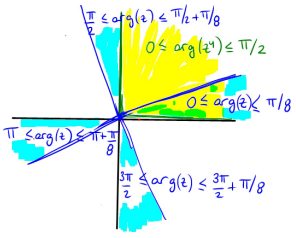
  - $k = 2j \;\Rightarrow\; \theta_k = \dfrac{\pi}{4} + 2j\pi$, i.e. $\theta_k = \theta_0 + 2j\pi$
  - $k = 2j+1 \;\Rightarrow\; \theta_k = \dfrac{5\pi}{4} + 2j\pi$, i.e. $\theta_k = \theta_1 + 2j\pi$.

- Determinar todos los $z \in \mathbb{C}$ tales que $0 \le \arg(z^4) \le \dfrac{\pi}{2}$:

  Sea $z = r\,e^{\theta i}$ con $0 \le \theta < 2\pi$. Entonces $\arg(z^4) = 4\theta - 2k\pi$ con $k \in \mathbb{Z}$ de modo tal que $0 \le 4\theta - 2k\pi < 2\pi$. Se tiene

  $$0 \le 4\theta - 2k\pi \le \frac{\pi}{2} \iff \frac{k\pi}{2} \le \theta \le \frac{k\pi}{2} + \frac{\pi}{8}.$$

  - Para $k = 0$ se obtiene el sector $0 \le \theta \le \dfrac{\pi}{8}$.
  - Para $k = 1$ se obtiene el sector $\dfrac{\pi}{2} \le \theta \le \dfrac{\pi}{2} + \dfrac{\pi}{8}$.
  - Para $k = 2$ se obtiene el sector $\pi \le \theta \le \pi + \dfrac{\pi}{8}$.
  - Para $k = 3$ se obtiene el sector $\dfrac{3\pi}{2} \le \theta \le \dfrac{3\pi}{2} + \dfrac{\pi}{8}$.

6.4 Raíces n-ésimas de números complejos.

Sea $z \in \mathbb{C}^\times$. Hallar las raíces n-ésimas de z consiste en determinar todos los $\omega \in \mathbb{C}$ que satisfacen $\omega^n = z$. Hagamos primero un ejemplo.

Ejemplo: Las raíces sextas de $z = 1 + i$.

Queremos determinar los $\omega \in \mathbb{C}$ tales que $\omega^6 = 1 + i$. Como comparar potencias es más fácil con la forma trigonométrica, planteemos $\omega = r\, e^{\theta i}$ con $r \in \mathbb{R}_{>0}$ y $\theta \in \mathbb{R}$, y comparemos $\omega^6 = r^6\, e^{6\theta i}$ con $1 + i = \sqrt{2}\, e^{\frac{\pi}{4} i}$:

$$r^6\, e^{6\theta i} = \sqrt{2}\, e^{\frac{\pi}{4} i} \iff \begin{cases} r^6 = \sqrt{2} \\ 6\theta = \dfrac{\pi}{4} + 2k\pi \quad \text{para algún} \quad k \in \mathbb{Z}. \end{cases}$$

O sea,

$$r = \sqrt{2}^{1/6} = 2^{1/12} \quad \text{y} \quad \theta = \frac{\pi}{24} + \frac{2k\pi}{6} \quad \text{para algún} \quad k \in \mathbb{Z},$$

Es decir

$$\omega = 2^{1/12}\, e^{(\frac{\pi}{24} + \frac{2k\pi}{6})i} \quad \text{para algún} \quad k \in \mathbb{Z}.$$

Observemos que si $\ell = 6j + k$ con $0 \le k < 6$, entonces

$$\frac{2\ell\pi}{6} = \frac{2(6j+k)\pi}{6} = \frac{2k\pi}{6} + 2j\pi,$$

y por lo tanto

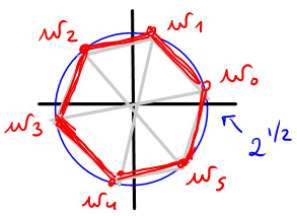
$$\theta_\ell := \frac{\pi}{24} + \frac{2\ell\pi}{6} = \frac{\pi}{24} + \frac{2k\pi}{6} + 2j\pi =: \theta_k + 2j\pi.$$

Se deduce que

$$\omega_\ell = 2^{1/12}\, e^{\theta_\ell i} = 2^{1/12}\, e^{\theta_k i} = \omega_k.$$

Para $k = 0, 1, \ldots, 5$, se obtienen los 6 ángulos, y luego las 6 soluciones

$$\begin{aligned}
\theta_0 &= \frac{\pi}{24} + \frac{2\cdot 0\pi}{6} = \frac{\pi}{24} && \Longrightarrow \quad \omega_0 = 2^{1/12}\, e^{\frac{\pi}{24} i} \\
\theta_1 &= \frac{\pi}{24} + \frac{2\cdot 1\pi}{6} = \frac{9\pi}{24} && \Longrightarrow \quad \omega_1 = 2^{1/12}\, e^{\frac{9\pi}{24} i} \\
\theta_2 &= \frac{\pi}{24} + \frac{2\cdot 2\pi}{6} = \frac{17\pi}{24} && \Longrightarrow \quad \omega_2 = 2^{1/12}\, e^{\frac{17\pi}{24} i} \\
\theta_3 &= \frac{\pi}{24} + \frac{2\cdot 1\pi}{6} = \frac{25\pi}{24} && \Longrightarrow \quad \omega_3 = 2^{1/12}\, e^{\frac{25\pi}{24} i} \\
\theta_4 &= \frac{\pi}{24} + \frac{2\cdot 1\pi}{6} = \frac{33\pi}{24} && \Longrightarrow \quad \omega_4 = 2^{1/12}\, e^{\frac{33\pi}{24} i} \\
\theta_5 &= \frac{\pi}{24} + \frac{2\cdot 1\pi}{6} = \frac{41\pi}{24} && \Longrightarrow \quad \omega_5 = 2^{1/12}\, e^{\frac{41\pi}{24} i},
\end{aligned}$$



que son todas distintas pues $0 \le \theta_k < 2\pi$ son todos argumentos distintos.

Teorema 6.4.1. (Las raíces n-ésimas de $z \in \mathbb{C}^\times$.)

Sea $n \in \mathbb{N}$ y sea $z = s\,e^{\varphi i} \in \mathbb{C}^\times$, con $s \in \mathbb{R}_{>0}$ y $0 \le \varphi < 2\pi$. Entonces z tiene n raíces n-ésimas $\omega_0, \ldots, \omega_{n-1} \in \mathbb{C}$, donde

$$\omega_k = s^{1/n}\, e^{\theta_k i} \quad \textit{donde} \quad \theta_k = \frac{\varphi + 2k\pi}{n} \quad \textit{para } 0 \le k \le n-1.$$

Demostración. La prueba es igual que en el ejemplo. Tenemos que determinar los $\omega \in \mathbb{C}$ tales que $\omega^n = z$. Planteemos $\omega = r\,e^{\theta i}$ con $r \in \mathbb{R}_{>0}$ y $\theta \in \mathbb{R}$, y comparemos $\omega^n = r^n\, e^{n\theta i}$ con $z = s\,e^{\varphi i}$:

$$r^n\, e^{n\theta i} = s\, e^{\varphi i} \iff \begin{cases} r^n = s \\ n\,\theta = \varphi + 2k\pi \ \text{ para algún } \ k \in \mathbb{Z} \end{cases}$$
$$\iff \begin{cases} r = s^{1/n} \\ \theta = \dfrac{\varphi + 2k\pi}{n} \ \text{ para algún } \ k \in \mathbb{Z}. \end{cases}$$

Es decir

$$\omega = s^{1/n}\, e^{\frac{\varphi + 2k\pi}{n} i} \ \text{ para algún } \ k \in \mathbb{Z}.$$

Observemos que si $\ell = jn + k$ con $0 \le k < n$, entonces

$$\theta_\ell := \frac{\varphi + 2\ell\pi}{n} = \frac{\varphi + 2(jn+k)\pi}{n} = \frac{\varphi + 2k\pi}{n} + 2j\pi =: \theta_k + 2j\pi,$$

y por lo tanto

$$\omega_\ell = s^{1/n}\, e^{\theta_\ell i} = s^{1/n}\, e^{\theta_k i} = \omega_k.$$

Pero más aún, para $0 \le k < n$, $\theta_k = \dfrac{\varphi + 2k\pi}{n}$ son todos distintos y satisfacen $0 \le \theta_k < 2\pi$ pues $0 \le \varphi < 2\pi$ y $0 \le k \le n-1$ implica

$$0 \le \frac{\varphi + 2k\pi}{n} < \frac{2\pi + 2(n-1)\pi}{n} = \frac{2n\pi}{n} = 2\pi.$$

Por lo tanto son todos argumentos distintos, es decir $\omega_k \ne \omega_{k'}$ para $0 \le k \ne k' < n$. Se obtienen por lo tanto las n raíces distintas

$$\omega_k = s^{1/n}\, e^{\theta_k i} \quad \text{donde} \quad \theta_k = \frac{\varphi + 2k\pi}{n} \quad \text{para } 0 \le k \le n-1.$$

□

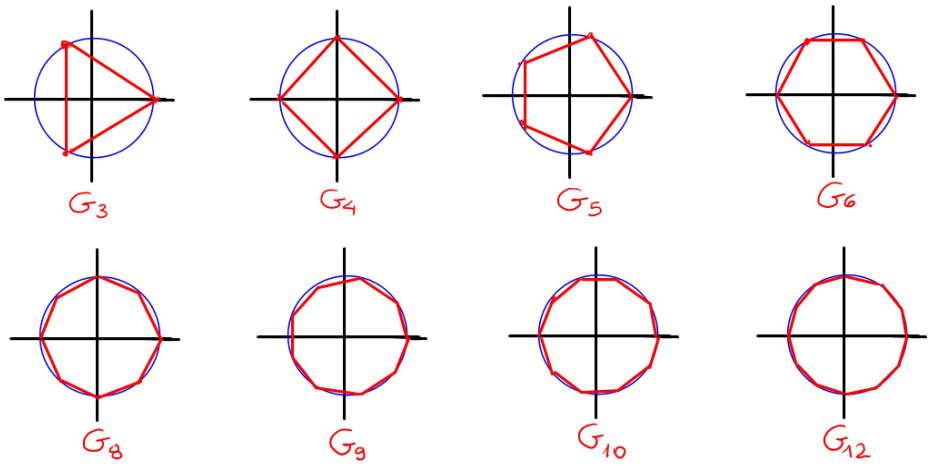
6.4.1 El grupo G_n de raíces n-ésimas de la unidad.

Cuando $z = 1$, buscamos las raíces n-é simas de 1, es decir los $\omega \in \mathbb{C}$ tales que $\omega^n = 1$. Según el Teorema 6.4.1, como $1 = e^0$, se tiene que las soluciones son $\omega_0, \ldots, \omega_{n-1}$ donde

$$\omega_k = e^{\frac{2\,k\,\pi}{n} i}, \quad 0 \le k \le n-1.$$

Éstas se llaman las *raíces n-ésimas de la unidad.*

Todas las raíces n-ésimas de 1 están sobre la circunferencia unidad, $\omega_0 = 1$ y las demás se obtienen dividiendo el ángulo 2π por n, o sea forman un n-ágono regular en la circunferencia unidad, empezando por el 1, como lo muestran las figuras para los valores de $n = 3$, $n = 4$, $n = 5$, $n = 6$, $n = 8$, $n = 9$, $n = 10$ y $n = 12$.



A continuación, estudiamos más en detalle el comportamiento del conjunto de raíces n-ésimas de la unidad para un $n \in \mathbb{N}$ fijo.

Definición 6.4.2. (El conjunto G_n.)

Sea $n \in \mathbb{N}$. El conjunto G_n es el conjunto de raíces n-ésimas de la unidad, es decir

$$G_n := \{\omega \in \mathbb{C} : \omega^n = 1\} \;=\; \{\omega_k = e^{\frac{2k\pi}{n}i},\ 0 \leq k \leq n-1\} \;\subseteq\; \mathbb{C}.$$

El conjunto G_n contiene n números complejos distintos, que forman un n-ágono regular en la circunferencia unidad del plano complejo, empezando

desde el 1. Por ejemplo,

$$\begin{aligned}
G_1 &= \{e^0\} = \{1\},\\
G_2 &= \{e^0, e^{\pi}\} = \{1, -1\},\\
G_3 &= \{e^{\frac{2k\pi}{3}i}, 0 \le k \le 2\} = \{1, -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i\}\\
G_4 &= \{e^{\frac{2k\pi}{4}i}, 0 \le k \le 3\} = \{\pm 1, \pm i\},\\
G_5 &= \{e^{\frac{2k\pi}{5}i}, 0 \le k \le 4\}\\
G_6 &= \{e^{\frac{2k\pi}{6}i}, 0 \le k \le 5\} = \{\pm 1, \pm\frac{1}{2} \pm \frac{\sqrt{3}}{2}i\},\\
G_8 &= \{e^{\frac{2k\pi}{8}i}, 0 \le k \le 7\} = \{\pm 1, \pm i, \pm\frac{\sqrt{2}}{2} \pm \frac{\sqrt{2}}{2}i\}.
\end{aligned}$$

En particular, si $n \neq m$, $G_n \neq G_m$ pues G_n tiene n elementos y G_m tiene m elementos.

Podemos conjeturar de los dibujos un montón de propiedades, que se pueden demostrar incluso sin conocer la forma particular de los elementos de G_n, pero solamente usando la definición: que $\omega \in G_n \Leftrightarrow \omega^n = 1$.

Proposición 6.4.3. ($(G_n, \cdot)$ es un grupo abeliano.)

Sea $n \in \mathbb{N}$.

1. $\forall\, \omega, z \in G_n$ *se tiene que* $\omega \cdot z \in G_n$.
2. $1 \in G_n$.
3. $\forall\, \omega \in G_n$, *existe* $\omega^{-1} \in G_n$.

Estas tres propiedades muestran que G_n es un grupo abeliano dentro del grupo multiplicativo $(\mathbb{C}^{\times}, \cdot)$: es un subconjunto de $\mathbb{C}$ cerrado para la operación producto, el producto es claramente asociativo y conmutativo (pues es el producto de $\mathbb{C}$ que lo es), el elemento neutro 1 de $\mathbb{C}$ pertenece a ese subconjunto, y además cada elemento de G_n tiene inverso en G_n.

Demostración.

1. $\omega, z \in G_n$ si y solo si por definición $\omega^n = 1$ y $z^n = 1$. Por lo tanto $(\omega \cdot z)^n = \omega^n \cdot z^n = 1 \cdot 1 = 1$ también. O sea $\omega \cdot z \in G_n$.
2. $1 \in G_n$ pues $1^n = 1$.
3. Dado $\omega \in G_n$, como $\omega \in \mathbb{C}$ y $\omega \neq 0$ (pues $0^n \neq 1$), se tiene que ω tiene un inverso $\omega^{-1} \in \mathbb{C}$. Alcanza con probar que ese inverso pertenece a G_n. Pero $(\omega^{-1})^n = (\omega^n)^{-1} = 1^{-1} = 1$ también, y por lo tanto $\omega^{-1} \in G_n$.

□

También se pueden inferir las propiedades siguientes de los elementos de G_n, del estudio de los ejemplos anteriores. Por ejemplo podemos observar (y probar) que

$$-1 \in G_n \;\Leftrightarrow\; n \text{ es par},$$

pues $(-1)^n = 1 \;\Leftrightarrow\; n$ es par. Aquí van más propiedades:

Proposición 6.4.4. (Más propiedades de G_n.)

Sea $n \in \mathbb{N}$ y sea $\omega \in G^n$. Entonces

1. $|\omega| = 1$.
2. *Sea $m \in \mathbb{Z}$ tal que $n \mid m$. Entonces $\omega^m = 1$.*
3. *Sean $m, m' \in \mathbb{Z}$ tales que $m \equiv m' \pmod{n}$, entonces $\omega^m = \omega^{m'}$. En particular $\omega^m = \omega^{r_n(m)}$.*
4. $\omega^{-1} = \overline{\omega} = \omega^{n-1}$.

Demostración. 1. Esto ya lo sabemos porque ya conocemos la forma particular de los elementos de G_n, pero se puede probar directamente de la definición: $\omega^n = 1 \;\Rightarrow\; 1 = |\omega^n| = |\omega|^n$, y por lo tanto $|\omega| = 1$.

2. Si $n \mid m$, entonces $m = kn$ y por lo tanto $\omega^m = \omega^{kn} = (\omega^n)^k = 1^k = 1$.

3. Sea $k \in \mathbb{Z}$ tal que $m = k\,n + m'$. Entonces $\omega^m = \omega^{kn+m'} = (\omega^n)^k \cdot \omega^{m'} = 1^k \cdot \omega^{m'} = \omega^{m'}$.

4. $\omega^{-1} = \dfrac{\overline{\omega}}{|\omega|^2}$ pero $|\omega| = 1$, por lo tanto $\omega^{-1} = \overline{\omega}$. La segunda igualdad es una consecuencia del inciso anterior, dado que $-1 \equiv n-1 \pmod{n}$.

□

<u>*Ejemplo:*</u> Para cada $\omega \in G_5$, calcular $\omega^{103} + \omega^{27} + \omega^{-4} + \overline{\omega}$:

Por la Proposición 6.4.4 (3,4), se tiene

$$\omega^{103} + \omega^{27} + \omega^{-4} + \overline{\omega} = \omega^3 + \omega^2 + \omega + \omega^4 = \begin{cases} 4 & \text{si } \omega = 1, \\ -1 & \text{si } \omega \neq 1. \end{cases}$$

ya que

$$1 + \omega + \omega^2 + \omega^3 + \omega^4 = \sum_{i=0}^{4} \omega^i = \begin{cases} 5 & \text{si } \omega = 1, \\ \dfrac{\omega^5 - 1}{\omega - 1} = \dfrac{1-1}{\omega-1} = 0 & \text{si } \omega \neq 1, \end{cases}$$

por la fórmula de la serie geométrica.

También se pueden comparar distintos G_n.

Proposición 6.4.5. **($G_n \cap G_m = G_{(n:m)}$).**

Sean $n, m \in \mathbb{N}$.

1. $n \mid m \;\Rightarrow\; G_n \subset G_m$.
2. $G_n \cap G_m = G_{(n:m)}$.
3. $G_n \subset G_m \;\Leftrightarrow\; n \mid m$.

Demostración. 1. $n \mid m \;\Rightarrow\; m = k\,n$ para algún $k \in \mathbb{Z}$. Por lo tanto, si $\omega \in G_n$, $\omega^m = \omega^{kn} = (\omega^n)^k = 1^k = 1$, o sea $\omega \in G_m$.

2. Como $(n : m) \mid n$ y $(n : m) \mid m$, $G_{(n:m)} \subset G_n$ y $G_{(n:m)} \subset G_m$ por el inciso anterior, y por lo tanto $G_{(n:m)} \subset G_n \cap G_m$.

   Falta probar la otra inclusión: se sabe que existen $s, t \in \mathbb{Z}$ tales que $(n : m) = sn + tm$, por lo tanto $\omega^{(n:m)} = \omega^{sn+tm} = (\omega^n)^s \cdot (\omega^m)^t$. Si $\omega \in G_n \cap G_m$, entonces $\omega^n = \omega^m = 1$ y por lo tanto, $\omega^{(n:m)} = 1^s \cdot 1^t = 1$, es decir $\omega \in G_{(n:m)}$ también.

3. Ya sabemos que vale $(\Leftarrow)$ por el inciso 1. Probemos $(\Rightarrow)$:

   $G_n \subset G_m \;\Rightarrow\; G_n \cap G_m = G_n$. Pero por el inciso anterior, se sabe que $G_n \cap G_m = G_{(n:m)}$. Por lo tanto $G_n = G_{(n:m)}$. Esto implica $n = (n : m)$ (pues hemos visto que distintos G_n tienen distinta cantidad de elementos) y por lo tanto $n \mid m$ como se quería probar.

□

Saquemos ahora provecho de la forma particular de los elementos de G_n:

$$G_n := \{\omega_k = e^{\frac{2\,k\,\pi}{n}i},\ 0 \le k \le n-1.\}$$

Proposición 6.4.6. **(G_n es un grupo cíclico.)**

Sea $n \in \mathbb{N}$. *Existe* $\omega \in G_n$ *tal que*

$$G_n = \{1, \omega, \omega^2, \ldots, , \omega^{n-1}\} = \{\omega^k,\ 0 \le k \le n-1\}.$$

Demostración. Se puede tomar por ejemplo $\omega := \omega_1 = e^{\frac{2\,\pi}{n}i}$, ya que sabemos por la fórmula de de Moivre que

$$\omega_1^k = \left(e^{\frac{2\,\pi}{n}i}\right)^k = e^{k\frac{2\,\pi}{n}i} = e^{\frac{2k\,\pi}{n}i} = \omega_k, \quad 0 \le k \le n-1.$$

□

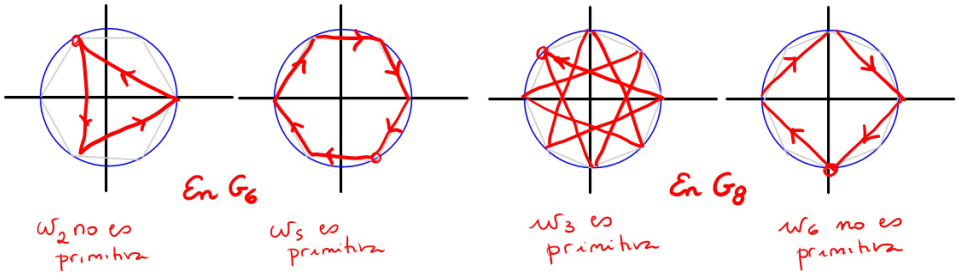
Pero ω_1 no es la única elección posible en esta demostración, por ejemplo también podríamos haber tomado $\omega_{n-1} = \overline{\omega_1}$ pues $\overline{\omega_1}^k = \overline{\omega_1^k} = \overline{\omega_k} = \omega_{n-k}$ para $0 \leq k \leq n-1$, es decir $\omega_{n-1}^k = \omega_{n-k}$ para $0 \leq k \leq n-1$. Esto motiva la definición siguiente.

Definición 6.4.7. (Raíz n-ésima primitiva de la unidad.)

Sea $n \in \mathbb{N}$. Se dice que $\omega \in \mathbb{C}$ es una raíz *n-ésima primitiva* de la unidad si

$$G_n = \{1, \omega, \ldots, \omega^{n-1}\} = \{\omega^k,\ 0 \leq k \leq n-1\}.$$

Ejemplo:



Observación 6.4.8. Sea ω una raíz primitiva de orden n de la unidad, es decir $G_n = \{1, \omega, \ldots, \omega^{n-1}\}$. Entonces para $0 \leq k \neq j \leq n-1$ se tiene que $\omega^k \neq \omega^j$, pues ya sabemos que G_n tiene n elementos distintos, y por la tanto no pueden coincidir dos potencias distintas de ω en el rango $0 \leq k, j \leq n-1$.

Proposición 6.4.9. (Caracterización de las raíces n-ésimas primitivas de la unidad.)

Sea $n \in \mathbb{N}$, y sea $\omega \in \mathbb{C}$. Entonces ω es una raíz n-ésima primitiva de la unidad si y solo si

$$\forall\, m \in \mathbb{Z}, \quad \omega^m = 1 \iff n \mid m.$$

Demostración. ($\Rightarrow$) Sea ω una raíz n-ésima primitiva de la unidad. Queremos probar que $\omega^m = 1 \Leftrightarrow n \mid m$.

Como ω es raíz n-ésima de la unidad, sabemos por la Proposición 6.4.4(4) que si $n \mid m$, entonces $\omega^m = 1$.

Queremos probar la recíproca, que si $\omega^m = 1$ entonces $n \mid m$. Pero por la Proposición 6.4.4(5), $\omega^m = \omega^{r_n(m)}$. Luego $\omega^m = 1$ implica $\omega^{r_n(m)} = 1 = \omega^0$, lo que implica por la Observación anterior que $r_n(m) = 0$, o sea $n \mid m$.

($\Leftarrow$) Queremos probar que si ω satisface $\omega^m = 1 \Leftrightarrow n \mid m$, entonces $G_n = \{\omega^k,\ 0 \leq k \leq n-1\}$.

Pero $\omega^m = 1 \Leftrightarrow n \mid m$ implica $\omega^n = 1$ y $\omega^k \neq 1$ para $1 \leq k \leq n-1$. Por lo tanto $\omega \in G_n$, lo que implica que $\omega^k \in G_n$, $0 \leq k \leq n-1$. Así $\{\omega^k,\ 0 \leq k \leq n-1\} \subset G_n$.

Pero además se cumple que $\omega^\ell \neq \omega^j$ para todo $0 \leq \ell < j \leq n-1$, pues si para algún $0 \leq \ell < j \leq n$ se tuviera $\omega^\ell = \omega^j$, entonces $\omega^{j-\ell} = 1$ con $1 \leq j - \ell \leq n-1$, lo que es una contradicción (tomando $k = j - \ell$) con $\omega^k \neq 1$ para $1 \leq k \leq n-1$. Por lo tanto $\#\{\omega^k;\ 0 \leq k \leq n-1\} = n = \#G_n$ implica que $\{\omega^k,\ 0 \leq k \leq n-1\} = G_n$. □

Corolario 6.4.10. (Raíces primitivas y potencias.)

Sean $n, k \in \mathbb{N}$ y sea $\omega \in \mathbb{C}$ una raíz n-ésima primitiva de la unidad. Entonces ω^k es una raíz n-ésima primitiva de la unidad si y solamente si $(n : k) = 1$.

Demostración. ($\Leftarrow$) Alcanza con probar, según la proposición anterior, que $(\omega^k)^m = 1 \Leftrightarrow n \mid m$, sabiendo que, al ser ω una raíz *primitiva* de la unidad de orden n, cualquiera sea el exponente j, $\omega^j = 1 \Leftrightarrow n \mid j$. Pero

$$1 = (\omega^k)^m = \omega^{km} \iff n \mid k\,m \underset{(n:k)=1}{\Longleftrightarrow} n \mid m,$$

como se quería probar.

($\Rightarrow$) Lo demostramos por la contrarecíproca: Supongamos que $(n : k) = d \neq 1$. Entonces

$$(\omega^k)^{\frac{n}{d}} = (\omega)^{\frac{kn}{d}} = (\omega^n)^{\frac{k}{d}} = 1^{\frac{k}{d}} = 1$$

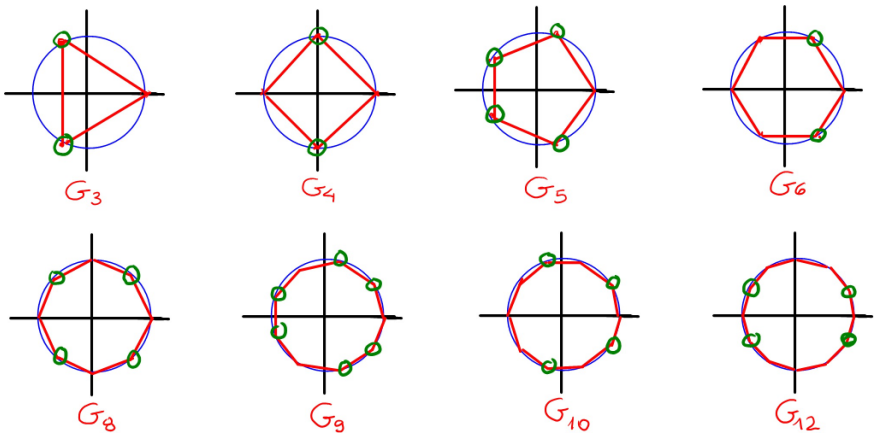
y por lo tanto ω^k no es una raíz n-ésima primitiva de la unidad, pues $n \nmid \dfrac{n}{d}$ y se contradice la Proposición 6.4.9. □

Corolario 6.4.11. (Las raíces primitivas en G_n.)

Sea $n \in \mathbb{N}$, y sea $\omega_k = e^{\frac{2k\pi}{n}i}$, $0 \leq k \leq n-1$. Entonces ω_k es raíz n-ésima primitiva de la unidad si y solamente si $(n : k) = 1$.

Demostración. Pues sabemos que ω_1 es raíz n-ésima primitiva de la unidad y $\omega_k = (\omega_1)^k$. □

En los ejemplos siguientes, las raíces primitivas están marcadas con un círculo verde:



Corolario 6.4.12. (Las raíces primitivas en G_p.)

Sea p un primo. Entonces cualquiera sea k, $1 \leq k \leq p-1$, se tiene que $\omega_k = e^{\frac{2k\pi}{p}i}$ es ráiz p-ésima primitiva de la unidad. Es decir $\forall\, \omega \in G_p$, $\omega \neq 1$, se tiene que ω es una raíz p-ésima primitiva de la unidad.

Ejemplo: Sea ω una raíz primitiva de la unidad de orden 15.

- Probar que ω^3 es una raíz primitiva de la unidad de orden 5: Se tiene $(\omega^3)^5 = \omega^{15} = 1$, por lo tanto ω^3 es una raíz de la unidad de orden 5. Pero $\omega^3 \neq 1$ pues ω es *primitiva* de orden 15, por lo tanto $\omega^3 \in G_5 - \{1\}$ implica que ω^3 es primitiva de orden 5, pues 5 es primo, y todas las raíces de la unidad de orden 5 salvo el 1 son primitivas.
- Calcular $\omega^{159} + \overline{\omega}^{27} - \omega^{27} + \omega^6 + 2\omega^{-3}$:

  Se tiene

$$\omega^{159} + \overline{\omega}^{27} - \omega^{27} + \omega^6 + 2\omega^{-3} = \omega^9 + \omega^3 - \omega^{12} + \omega^6 + 2\omega^{12}$$
$$= \sum_{k=1}^{4} (\omega^3)^k = \frac{(\omega^3)^5 - 1}{\omega^3 - 1} - (\omega^3)^0 = -1,$$

  pues $\omega^3 \neq 1$ al ser ω *primitiva* de orden 15.

Terminemos este capítulo con una propiedad general de las raíces de la unidad.

Proposición 6.4.13. (Suma y producto de los elementos de G_n.)

Sea $n \in \mathbb{N}$ con $n > 1$. Entonces

$$\sum_{\omega \in G_n} \omega = 0 \qquad y \qquad \prod_{\omega \in G_n} \omega = \begin{cases} 1 & si \quad n \text{ es impar}, \\ -1 & si \quad n \text{ es par}. \end{cases}$$

Demostración. Sabemos que G_n es un grupo cíclico, es decir existe $\omega \in G_n$ tal que $G_n = \{1, w, \ldots, w^{n-1}\}$, por ejemplo $\omega = \omega_1$. Por lo tanto,

$$\sum_{\omega \in G_n} \omega = \sum_{k=0}^{n-1} \omega_1^k = \frac{\omega_1^n - 1}{\omega_1 - 1} = \frac{1-1}{\omega - 1} = 0,$$

por la suma geométrica, ya que $\omega_1 \neq 1$, y porque $\omega_1^n = 1$.

Con respecto al producto, en G_n sabemos que cada vez que está ω también está $\omega^{-1} = \overline{\omega} \neq \omega$ si $\omega \neq \pm 1$. Por lo tanto, cuando n es impar (caso en que $-1 \notin G_n$), las raíces de la unidad vienen de a pares inversos, cuyo producto da 1, además de la raíz 1, y por lo tanto el producto da 1. Cuando n es par (caso en que $-1 \in G_n$), las raíces de la unidad vienen de a pares inversos, cuyo producto da 1, además de las raíces 1 y -1, y por lo tanto el producto da -1. □

6.5 Ejercicios.

1. Para los siguientes $z \in \mathbb{C}$, hallar $\mathrm{Re}(z)$, $\mathrm{Im}(z)$, $|z|$, $\mathrm{Re}(z^{-1})$ e $\mathrm{Im}(i \cdot z)$

   i) $z = 5\,i(1+i)^4$

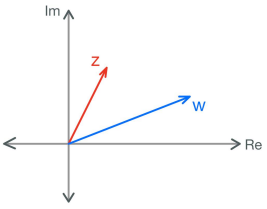
   ii) $z = (\sqrt{2} + \sqrt{3}\,i)^2(\overline{1 - 3\,i})$

   iii) $z = i^{17} + \frac{1}{2}\,i(1-i)^3$

   iv) $z = \left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}\,i\right)^{10}$

   v) $z = \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}\,i\right)^{-1}$.

2. Dados los siguientes $z, w \in \mathbb{C}$ en el plano:



   representar en un gráfico aproximado los números complejos de cada inciso

   i) $z, w, z + w$ y $z - w$

   ii) $z, -z, 2z, \frac{1}{2}z, iz$ y $\overline{z}$

   iii) $z, w, |z|, |z + w|$ y $|\overline{w - z}|$.

3. Hallar todos los números complejos z tales que

   i) $z^2 = -36$
   ii) $z^2 = i$
   iii) $z^2 = 7 + 24i$
   iv) $z^2 + 15 - 8i = 0$

4. Calcular los módulos y los argumentos de los siguientes números complejos

   i) $(2 + 2\,i)(\sqrt{3} - i)$
   ii) $(-1 + \sqrt{3}\,i)^5$
   iii) $(-1 + \sqrt{3}\,i)^{-5}$
   iv) $\dfrac{1 + \sqrt{3}\,i}{1 - i}$

5. Graficar en el plano complejo

   i) $\{z \in \mathbb{C} \,/\, \mathrm{Re}(z) + 5\,\mathrm{Im}(z) \leq 8\}$.
   ii) $\{z \in \mathbb{C} - \{0\} \,/\, |z| \geq 2 \text{ y } \dfrac{\pi}{4} \leq \arg(z) \leq \dfrac{2\pi}{3}\}$.
   iii) $\{z \in \mathbb{C} - \{0\} \,/\, \mathrm{Im}(z) > 2 \text{ y } \arg(-i\,z) = \dfrac{\pi}{4}\}$.
   iv) $\{z \in \mathbb{C} - \{0\} \,/\, \arg(z^4) = \arg\left((-1 + i)\overline{z}^2\right)\}$.

6. i) Determinar la forma binomial de $\left(\dfrac{1 + \sqrt{3}\,i}{1 - i}\right)^{17}$.
   ii) Determinar la forma binomial de $(-1 + \sqrt{3}\,i)^n$ para cada $n \in \mathbb{N}$.

7. Hallar todos los $n \in \mathbb{N}$ tales que

   i) $(\sqrt{3} - i)^n = 2^{n-1}(-1 + \sqrt{3}\,i)$.
   ii) $(-\sqrt{3} + i)^n \left(\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}i\right)$ es un número real negativo.
   iii) $\arg\left((-1 + i)^{2n}\right) = \dfrac{\pi}{2}$ y $\arg\left((1 - \sqrt{3}i)^{n-1}\right) = \dfrac{2}{3}\pi$.

8. Hallar en cada caso las raíces n-ésimas de $z \in \mathbb{C}$:

   i) $z = 8,\ n = 6$
   ii) $z = -4,\ n = 3$
   iii) $z = -1 + i,\ n = 7$
   iv) $z = (2 - 2i)^{12},\ n = 6$.

9. Hallar todos los $z \in \mathbb{C}$ tales que $3z^5 + 2|z|^5 + 32 = 0$.

10. Hallar todos los $n \in \mathbb{N}$ para los cuales la ecuación

$$z^n + i\overline{z}^2 = 0$$

tenga exactamente 6 soluciones, y resolver en ese caso.

11. i) Calcular $w + \overline{w} + (w + w^2)^2 - w^{38}(1 - w^2)$ para cada $w \in G_7$.
    ii) Calcular $w^{73} + \overline{w} \cdot w^9 + 8$ para cada $w \in G_3$.
    iii) Calcular $1 + w^2 + w^{-2} + w^4 + w^{-4}$ para cada $w \in G_{10}$.
    iv) Calcular $w^{14} + w^{-8} + \overline{w}^4 + \overline{w^{-3}}$ para cada $w \in G_5$.

12. i) Sea $w \in G_{36}$, $w^4 \neq 1$. Calcular $\sum_{k=7}^{60} w^{4k}$.
    ii) Sea $w \in G_{11}$, $w \neq 1$. Calcular $\operatorname{Re}\left(\sum_{k=0}^{60} w^k\right)$.

13. Sea $w = e^{\frac{2\pi i}{3}}$ raíz cúbica de la unidad y sea $(z_n)_{n\in\mathbb{N}}$ la sucesión de números complejos definida por

$$z_1 = 1 + w \quad \text{y} \quad z_{n+1} = \overline{1 + z_n^2}, \ \forall\, n \in \mathbb{N}.$$

    Probar que para todo $n \in \mathbb{N}$ vale que $z_n = \begin{cases} e^{\frac{2\pi i}{6}} \text{ si } n \text{ impar} \\ e^{\frac{-2\pi i}{6}} \text{ si } n \text{ par} \end{cases}$.
    Concluir que $z_n \in G_6$ para todo $n \in \mathbb{N}$.

14. Se define en $\mathbb{C} - \{0\}$ la relación $\mathcal{R}$ dada por

$$z \,\mathcal{R}\, \omega \iff z\,\overline{\omega} \in \mathbb{R}_{>0}.$$

    i) Probar que $\mathcal{R}$ es una relación de equivalencia.
    ii) Dibujar en el plano complejo la clase de equivalencia de $z = 1 + i$.

15. Se define la siguiente relación $\Re$ en G_{20}:

$$z \,\Re\, \omega \iff z\,\omega^9 \in G_2.$$

    i) Probar que $\Re$ es una relación de equivalencia.
    ii) Calcular la cantidad de elementos que hay en cada clase de equivalencia.

Capítulo 7

Polinomios.

7.1 El anillo de polinomios $K[X]$: generalidades.

Sea K un cuerpo, por ejemplo $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ o $\mathbb{Z}/p\mathbb{Z}$, donde p es un número primo (positivo). Se dice que f es un *polinomio con coeficientes en* K si f es de la forma

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = \sum_{i=0}^{n} a_i X^i,$$

para algún $n \in \mathbb{N}_0$, donde X es una indeterminada sobre K y $a_i \in K$ para $0 \leq i \leq n$. Los elementos $a_i \in K$ se llaman los *coeficientes* de f. Se conviene que dos polinomios son iguales si y solo si coinciden todos sus coeficientes, es decir si $f = \sum_{i=0}^{n} a_i X^i$ y $g = \sum_{i=0}^{n} b_i X^i$, entonces $f = g \Leftrightarrow a_i = b_i,\ 0 \leq i \leq n$.

El conjunto de todos los polinomios f con coeficientes en K se nota $K[X]$.

Si f no es el polinomio nulo, es decir $f \neq 0$, entonces se puede escribir para algún $n \in \mathbb{N}_0$ en la forma

$$f = \sum_{i=0}^{n} a_i X^i \quad \text{con} \quad a_n \neq 0.$$

En ese caso n es el *grado* de f y se nota $\mathrm{gr}(f)$, a_n es el *coeficiente principal* de f y lo notaremos aquí $\mathrm{cp}(f)$, y a_0 se denomina el *coeficiente constante* o *término independiente* de f. El polinomio nulo no tiene grado. Cuando el coeficiente principal de f es igual a 1, se dice que el polinomio es *mónico*. Notemos que para todo $f \in K[X] - \{0\}$, se tiene $\mathrm{gr}(f) \in \mathbb{N}_0$.

7.1.1 Operaciones en $K[X]$.

Las operaciones $+$ y $\cdot$ del cuerpo K se trasladan al conjunto $K[X]$ en forma natural, se suma coeficiente a coeficiente y se multiplica aplicando la distributividad:

- Si $f = \sum_{i=0}^{n} a_i X^i,\ g = \sum_{i=0}^{n} b_i X^i \in K[X]$, entonces

$$f + g = \sum_{i=0}^{n} (a_i + b_i) X^i \in K[X].$$

- Si $f = \sum_{i=0}^{n} a_i X^i,\ g = \sum_{j=0}^{m} b_j X^j \in K[X]$, entonces

$$f \cdot g = \sum_{k=0}^{n+m} c_k X^k \in K[X] \quad \text{donde } c_k = \sum_{i+j=k} a_i b_j.$$

Ejemplos:

- Sean $f = 5X^4 - 2X^3 + 3X^2 - X + 1$ y $g = 3X^3 - X^2 + X - 3$. Entonces

  $f + g = 5X^4 + X^3 + 2X^2 - 2,$
  $f \cdot g = 15X^7 - 11X^6 + 16X^5 - 23X^4 + 13X^3 - 11X^2 + 4X - 3.$

  En este caso, $\operatorname{gr}(f+g) = 4 = \max\{\operatorname{gr}(f), \operatorname{gr}(g)\}$, y $\operatorname{gr}(f \cdot g) = 7 = \operatorname{gr}(f) + \operatorname{gr}(g)$, más aún, $\operatorname{cp}(f \cdot g) = 15 = 5 \cdot 3 = \operatorname{cp}(f) \cdot \operatorname{cp}(g)$.

- Sean $f = 2X^3 + 3X - 1$, $g = -2X^3 + 2X^2 - 1$ y $h = -3X^3 - 2$. Entonces $f + g = 2X^2 + 3X - 2$ y $f + h = -X^3 + 3X - 3$. En este caso $\operatorname{gr}(f+g) = 2 < \max\{\operatorname{gr}(f), \operatorname{gr}(g)\}$ pues los dos polinomios tienen el mismo grado y se cancelaron los coeficientes principales, pero $\operatorname{gr}(f+h) = 3 = \max\{\operatorname{gr}(f), \operatorname{gr}(g)\}$ pues por más que los dos polinomios tienen mismo grado, no se cancelaron los coeficientes principales.

Observación 7.1.1. (Grado de la suma y del producto.)

Sea K un cuerpo y sean $f, g \in K[X]$ *no nulos*. Entonces

- Si $f + g \neq 0$, entonces $\operatorname{gr}(f+g) \leq \max\{\operatorname{gr}(f), \operatorname{gr}(g)\}$. Más precisamente,

  $\operatorname{gr}(f+g) = \max\{\operatorname{gr}(f), \operatorname{gr}(g)\}$ si $\operatorname{gr}(f) \neq \operatorname{gr}(g)$ o $\operatorname{gr}(f) = \operatorname{gr}(g)$ pero $\operatorname{cp}(f) + \operatorname{cp}(g) \neq 0$.

  $\operatorname{gr}(f+g) < \max\{\operatorname{gr}(f), \operatorname{gr}(g)\}$ si $\operatorname{gr}(f) = \operatorname{gr}(g)$ y $\operatorname{cp}(f) + \operatorname{cp}(g) = 0$.

- $\operatorname{cp}(f \cdot g) = \operatorname{cp}(f) \cdot \operatorname{cp}(g)$. En particular, $f \cdot g \neq 0$ y $\operatorname{gr}(f \cdot g) = \operatorname{gr}(f) + \operatorname{gr}(g)$.

Ejemplo: Calcular el coeficiente principal, el coeficiente constante y el que acompaña a X de

$$f = (X^3 + 2)^{10}(2X + 3)^5$$

- El coeficiente principal de f se obtiene multiplicando los coeficientes principales de los factores:

$$\mathrm{cp}(f) = \mathrm{cp}(X^3 + 2)^{10}\mathrm{cp}(2X + 3)^5 = 1^{10} \cdot 2^5 = 2^5.$$

- El coeficiente constante de f se obtiene multiplicando los coeficientes constantes de los factores, en este caso:

$$2^{10} \cdot 3^5.$$

- ¿Cómo se obtiene el coeficiente que acompaña a X en este producto? La única forma es eligiendo el coeficiente constante en $(X^3 + 2)^{10}$, esto es 2^{10}, y calculando en $(2X + 3)^5$ el coeficiente que acompaña a X, es decir eligiendo en uno de los 5 paréntesis de $(2X + 3)^5$ una vez el $2X$ y 4 veces el 3, esto es $\binom{5}{1}2 \cdot 3^4 = 5 \cdot 2 \cdot 3^4$. El resultado es entonces:

$$2^{10} \cdot 5 \cdot 2 \cdot 3^4 = 2^{11} \cdot 3^4 \cdot 5.$$

Teorema 7.1.2. (El anillo $(K[X], +, \cdot)$.)

Sea K un cuerpo. Entonces, $(K[X], +, \cdot)$ es un anillo conmutativo *(al igual que $\mathbb{Z}$). Más aún, al igual que en $\mathbb{Z}$, si se multiplican dos elementos no nulos, el resultado es no nulo, o dicho de otra manera:*

$$\forall\, f, g \in K[X], \quad f \cdot g = 0 \implies f = 0 \ o \ g = 0.$$

(Esto se llama ser un dominio íntegro*.)*

Demostración. Las propiedades conmutativa y asociativa de las operaciones $+$ y $\cdot$ son consecuencia de las definiciones de las operaciones y del hecho que valen las mismas propiedades en K. El elemento neutro para la suma es el polinomio 0, y el opuesto aditivo de $f = \sum_{i=0}^{n} a_i X^i$ es $-f = \sum_{i=0}^{n}(-a_i)X^i$. El elemento neutro para el producto es el polinimio 1. Pero en ese caso no todo $f \neq 0$ tiene inverso multiplicativo, como veremos a continuación.

La segunda afirmación es una consecuencia de la observación anterior: si f y g son no nulos, entonces fg es no nulo. □

Como consecuencia de la observación sobre el grado del producto se deduce inmediatamente quiénes son los polinomios en $K[X]$ que tienen inverso multiplicativo.

Observación 7.1.3. (Inversibles de $K[X]$.)

Sea K un cuerpo. Entonces $f \in K[X]$ es inversible si y solo si $f \in K^\times$. O sea los elementos inversibles de $K[X]$ son los polinomios de grado 0.

Demostración.

- ($\Rightarrow$) Sea $f \in K[X]$ inversible. Es decir existe $g \in K[X]$ tal que $f \cdot g = 1$. Por lo tanto tanto f como g son no nulos, y $\mathrm{gr}(1) = \mathrm{gr}(f \cdot g)$, es decir $0 = \mathrm{gr}(f) + \mathrm{gr}(g)$. Como $\mathrm{gr}(f), \mathrm{gr}(g) \in \mathbb{N}_0$, la única posibilidad es $\mathrm{gr}(f) = 0 = \mathrm{gr}(g)$ y por lo tanto $f, g \in K$, y no nulos.

- ($\Leftarrow$) Sea $f \in K - \{0\}$, o sea f es una constante no nula de K. Por lo tanto, como K es un cuerpo, f es inversible y existe $g \in K - \{0\}$ tal que $f \cdot g = 1$, es decir f es inversible.

□

7.1.2 Divisibilidad, Algoritmo de División y MCD en $K[X]$.

Por lo que vimos en la sección anterior, $K[X]$ es un anillo conmutativo (más bien un dominio íntegro) que, al igual que $\mathbb{Z}$, no es un cuerpo ya que no todo elemento no nulo es inversible: sabemos que los únicos polinomios inversibles son los polinomios constantes (no nulos). Tiene sentido entonces estudiar la *divisibilidad* así como hicimos en $\mathbb{Z}$. En esta sección haremos todo un paralelismo con la teoría desarrollada en $\mathbb{Z}$.

Definición 7.1.4. (Divisibilidad.)

Sean $f, g \in K[X]$ con $g \neq 0$. Se dice que g *divide a* f, y se nota $g \mid f$, si existe un polinomio $q \in K[X]$ tal que $f = q \cdot g$. O sea:

$$g \mid f \iff \exists\, q \in K[X] \,:\, f = q \cdot g.$$

En caso contrario, se dice que g no divide a f, y se nota $g \nmid f$.

Propiedades 7.1.5. (Propiedades de la divisibilidad.)

- Todo polinomio $g \neq 0$ satisface que $g \mid 0$ pues $0 = 0 \cdot g$ (aquí $q = 0$).
- $g \mid f \Leftrightarrow c\,g \mid f$, $\forall\, c \in K^\times$ (pues $f = q \cdot g \Leftrightarrow f = (c^{-1}q) \cdot (c\,g)$).
  De la misma manera $g \mid f \Leftrightarrow g \mid d\,f, \forall\, d \in K^\times$.
  Se concluye que si $f, g \in K[X]$ son no nulos,

$$g \mid f \iff c\,g \mid d\,f,\ \forall\, c, d \in K^\times \iff \frac{g}{\mathrm{cp}(g)} \mid \frac{f}{\mathrm{cp}(f)}.$$

Es decir la divisibilidad no depende de constantes no nulas (que son los elementos inversibles de K), y por lo tanto todo polinomio tiene infinitos divisores. Pero todo divisor g de f tiene un divisor mónico asociado, que es $g/\mathrm{cp}(g)$.

- Sean $f, g \in K[X]$ no nulos tales que $g \mid f$ y $\mathrm{gr}(g) = \mathrm{gr}(f)$. Entonces $g = c\,f$ para algún $c \in K^\times$ (pues $f = q\,g$ con $q \neq 0$ y $\mathrm{gr}(g) = \mathrm{gr}(f) \Rightarrow \mathrm{gr}(q) = 0$, i.e. $q = c \in K^\times$).

- $g \mid f$ y $f \mid g \Leftrightarrow f = c\,g$ para algún $c \in K^\times$ (pues tienen el mismo grado).

- Para todo $f \in K[X]$, $f \notin K$, se tiene $c \mid f$ y $c\,f \mid f$, $\forall\, c \in K^\times$.

  Así, todo f en esas condiciones tiene esas dos categorías distintas de divisores asegurados (los de grado 0 y los de su mismo grado que son de la forma $c\,f$, con $c \in K^\times$).

  Hay polinomios que tienen únicamente esos divisores, y otros que tienen más. Esto motiva la separación de los polinomios en $K[X]$ no constantes en dos categorías, la de polinomios *irreducibles* y la de los polinomios *reducibles* :

Definición 7.1.6. (Polinomios irreducibles y reducibles.)

Sea $f \in K[X]$.

- Se dice que f es *irreducible* en $K[X]$ cuando $f \notin K$ y los únicos divisores de f son de la forma $g = c$ o $g = c\,f$ para algún $c \in K^\times$. O sea f tiene únicamente dos divisores mónicos (distintos), que son 1 y $f/\mathrm{cp}(f)$.

- Se dice que f es *reducible* en $K[X]$ cuando $f \notin K$ y f tiene algún divisor $g \in K[X]$ con $g \neq c$ y $g \neq c\,f$, $\forall\, c \in K^\times$, es decir f tiene algún divisor $g \in K[X]$ (no nulo por definición) con $0 < \mathrm{gr}(g) < \mathrm{gr}(f)$.

En particular, todo polinomio de grado 1 en $K[X]$ es irreducible.

Pero no solo ellos, dependiendo del cuerpo K: por ejemplo el polinomio $X^2 + 1 \in \mathbb{R}[X]$ es irreducible en $\mathbb{R}[X]$, pues si fuera reducible, tendría un divisor mónico de grado 1 (grado intermedio), y luego se tendría $X^2 + 1 = (X + a)\,(X + b)$ con $a, b \in \mathbb{R}$, lo que implica $a + b = 0$, i.e. $b = -a$ y $a\,b = 1$, i.e. $-a^2 = 1$, lo que es imposible para $a \in \mathbb{R}$. Pero es reducible en $\mathbb{C}[X]$ ya que $X^2 + 1 = (x - i)(x + i)$, i.e. $X - i \mid X^2 + 1$ en $\mathbb{C}[X]$.

Y el polinomio $X^2 - 2 \in \mathbb{Q}[X]$ es irreducible en $\mathbb{Q}[X]$, pues si fuera reducible, tendría un divisor mónico de grado 1, y luego se tendría $X^2 - 2 =$

$(X+a)(X+b)$ con $a,b \in \mathbb{Q}$, lo que implica $a+b=0$, i.e. $b=-a$ y $a\,b=-2$, i.e. $a^2=2$, lo que es imposible para $a \in \mathbb{Q}$. Pero es reducible en $\mathbb{R}[X]$ y en $\mathbb{C}[X]$ ya que $X^2+2=(x-\sqrt{2})(x+\sqrt{2})$, i.e. $X-\sqrt{2} \mid X^2-2$ en $\mathbb{R}[X]$ y en $\mathbb{C}[X]$.

La divisibilidad de polinomios cumple exactamente las mismas propiedades que la divisibilidad de números enteros. Repasar esas propiedades.

Continuamos entonces el paralelismo con $\mathbb{Z}$ para $K[X]$:

Teorema 7.1.7. (Algoritmo de división.)

Dados $f, g \in K[X]$ no nulos, existen únicos $q, r \in K[X]$ que satisfacen

$$f = q \cdot g + r \quad \textit{con} \quad r = 0 \quad o \quad \mathrm{gr}(r) < \mathrm{gr}(g).$$

Se dice que q es el *cociente* y r es el *resto* de la división de f por g, que notaremos $r_g(f)$.

<u>*Ejemplo:*</u> Sean $f = X^5+X^4-3X^3+4X^2+2X$ y $g = X^4+3X^3-X^2-6X-2$, entonces

$$f = (X-2)g + r \quad \text{con } r = 4X^3+8X^2-8X-4.$$

Demostración. • *Existencia de q y r:*

La demostración es calcada del caso $\mathbb{Z}$. Dados $f, g \in K[X]$ no nulos, consideramos el conjunto

$$A = \{f - \tilde{q}\,g;\ \tilde{q} \in K[X]\} \ \subset\ K[X],$$

que es claramente un conjunto $\neq \emptyset$ pues por ejemplo $f \in A$ tomando $\tilde{q}=0$. Si $0 \notin A$, elijamos un polinomio $r \in A$ de grado mínimo, y si $0 \in A$, elijamos $r=0$. Es decir

$$\exists\, q \in K[X] \text{ tal que } \quad r = f - q\,g \quad \text{ y } \quad r=0 \text{ o } \mathrm{gr}(r) \le \mathrm{gr}(\tilde{r}),\ \forall\, \tilde{r} \in A.$$

Por lo tanto, $f = q\,g + r$ y se afirma que si $r \neq 0$, entonces $\mathrm{gr}(r) < \mathrm{gr}(g)$. Pues si fuera $\mathrm{gr}(r) \ge \mathrm{gr}(g)$, puedo considerar el polinomio

$$\begin{aligned}
\tilde{r} &= r - \frac{\mathrm{cp}(r)}{\mathrm{cp}(g)} X^{\mathrm{gr}(r)-\mathrm{gr}(g)}\, g \\
&= f - q\,g - \frac{\mathrm{cp}(r)}{\mathrm{cp}(g)} X^{\mathrm{gr}(r)-\mathrm{gr}(g)}\, g \\
&= f - \big(q + \frac{\mathrm{cp}(r)}{\mathrm{cp}(g)} X^{\mathrm{gr}(r)-\mathrm{gr}(g)}\big)\, g \ \in\ A.
\end{aligned}$$

Es fácil verificar que los dos sumandos tienen el mismo grado, y en esta resta, se cancela el coeficiente principal de r. Por lo tanto $\mathrm{gr}(\tilde{r}) < \mathrm{gr}(r)$, lo que contradice el hecho que r tenía grado mínimo en A.

- *Unicidad de q y r:*

  Supongamos que existen $q_1, r_1, q_2, r_2 \in K[X]$ con $r_1 = 0$ o $\mathrm{gr}(r_1) < \mathrm{gr}(g)$ y $r_2 = 0$ o $\mathrm{gr}(r_2) < \mathrm{gr}(g)$ tales que

  $$f = q_1\, g + r_1 = q_2\, g + r_2.$$

  Entonces $(q_1 - q_2)\, g = r_2 - r_1$ implica $g \mid r_2 - r_1$. Pero si $r_2 - r_1 \neq 0$, se tiene que $\mathrm{gr}(r_2 - r_1) \leq \max\{\mathrm{gr}(r_2), \mathrm{gr}(r_1)\} < \mathrm{gr}(g)$, luego no puede ser divisible por g. Por lo tanto $r_2 - r_1 = 0$, i.e. $r_1 = r_2$ de lo que se deduce que $q_1 = q_2$ pues $(q_1 - q_2)\, g = 0$ con $g \neq 0$ implica $q_1 - q_2 = 0$.

□

Observación 7.1.8. (Algoritmo de división en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.)

Una consecuencia tal vez impensada pero importante de la unicidad del cociente y el resto en el algoritmo de división es que si $f, g \in \mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X]$, entonces **el** cociente y **el** resto de dividir a f por g pertenecen a $\mathbb{Q}[X]$ independientemente de si miramos a los polinomios en $\mathbb{Q}[X]$, en $\mathbb{R}[X]$ o en $\mathbb{C}[X]$ (pues el cociente y el resto en $\mathbb{Q}[X]$ cumplen la propiedad de cociente y resto también en $\mathbb{R}[X]$ y en $\mathbb{C}[X]$). Y análogamente para $f, g \in \mathbb{R}[X] \subset \mathbb{C}[X]$.

Definición 7.1.9. (Máximo Común Divisor.)

Sean $f, g \in K[X]$ no ambos nulos. El *máximo común divisor* entre f y g, que se nota $(f : g)$, es el polinomio mónico de mayor grado que divide simultáneamente a f y a g.

Observación 7.1.10. No es obvio en este caso que este polinomio es único, de hecho es una consecuencia de las propiedades siguientes que se cumplen para un polinomio mónico de mayor grado que es divisor común de f y g, y de los resultados que se deducen de esas propiedades.

- $(f : 0) = f/\mathrm{cp}(f)$, $\forall\, f \in K[X]$ no nulo.
- Sean $f, g \in K[X]$ con g no nulo. Si $f = q \cdot g + r$ para $q, r \in K[X]$, entonces $(f : g) = (g : r)$.

<u>*Ejemplos:*</u> Sean $f, g \in K[X]$, $g \neq 0$. Entonces :

- Sea $c \in K^\times$, $(c : g) = 1$
- Si $g \mid f$, entonces $(f : g) = \frac{g}{\mathrm{cp}(g)}$.

A continuación deducimos el Algoritmo de Euclides, que al igual que en el caso $\mathbb{Z}$, permite calcular el máximo común divisor entre dos polinomios (y es de hecho la única forma de calcular el máximo común divisor de polinomios arbitrarios).

Teorema 7.1.11. (Algoritmo de Euclides.)

Sean $f, g \in K[X]$ no nulos. Entonces $(f : g)$ es el último resto r_k no nulo (dividido por su coeficiente principal para volverlo mónico) que aparece en la sucesión de divisiones siguiente:

$$\begin{array}{lcll} f & = & q_1\, g + r_1 & \textit{con} \quad r_1 \neq 0 \quad \textit{y} \quad \mathrm{gr}(r_1) < \mathrm{gr}(g), \\ g & = & q_2\, r_1 + r_2 & \textit{con} \quad r_2 \neq 0 \quad \textit{y} \quad \mathrm{gr}(r_2) < \mathrm{gr}(r_1), \\ r_1 & = & q_3\, r_2 + r_3 & \textit{con} \quad r_3 \neq 0 \quad \textit{y} \quad \mathrm{gr}(r_3) < \mathrm{gr}(r_2), \\ & \vdots & & \\ r_{k-2} & = & q_k\, r_{k-1} + r_k & \textit{con} \quad r_k \neq 0 \quad \textit{y} \quad \mathrm{gr}(r_k) < \mathrm{gr}(r_{k-1}), \\ r_{k-1} & = & q_{k+1}\, r_k & \end{array}$$

(pues resulta

$$(f : g) = (g : r_1) = (r_1 : r_2) = \cdots = (r_{k-2} : r_{k-1}) = (r_{k-1} : r_k) = \frac{r_k}{\mathrm{cp}(r_k)},$$

ya que $r_k \mid r_{k-1}$).

Observación 7.1.12. (Mcd en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.)

El hecho que el algoritmo de Euclides para calcular $(f : g)$ se basa en el algoritmo de división tiene una consecuencia no inmediata tal vez, pero fundamental, que es que si $f, g \in \mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X]$, entonces $(f : g) \in \mathbb{Q}[X]$ (y es siempre el mismo) independientemente de si miramos a $f, g \in \mathbb{Q}[X]$, en $\mathbb{R}[X]$ o en $\mathbb{C}[X]$. Y análogamente para $f, g \in \mathbb{R}[X] \subset \mathbb{C}[X]$.

Si despejamos en el algoritmo de Euclides para el cálculo del mcd el polinomio r_k de la anteúltima igualdad, y volviendo hacia arriba despejando paso a paso r_{k-1}, $r_{k-2}, \ldots$, r_2, r_1 en las igualdades anteriores, se logra escribir r_k en la forma $r_k = s'f + t'g$ (al igual que hicimos en el caso de $\mathbb{Z}$). Finalmente, dividiendo toda la expresión por la constante $\mathrm{cp}(r_k)$, se obtienen $s, t \in K[X]$ tales que $(f : g) = sf + tg$.

<u>*Ejemplo:*</u> Sean $f = X^5+X^4-3X^3+4X^2+2X$ y $g = X^4+3X^3-X^2-6X-2$. Se tiene :

$$\begin{array}{lcll} f & = & (X-2)g + r_1 & \text{con} \quad r_1 = 4X^3 + 8X^2 - 8X - 4 \\ g & = & (\frac{1}{4}X + \frac{1}{4})r_1 + r_2 & \text{con} \quad r_2 = -X^2 - 3X - 1 \\ r_1 & = & (-4X + 4)r_2 & \end{array}$$

Luego $(f:g) = \frac{r_2}{\mathrm{cp}(r_2)} = X^2 + 3X + 1$ y

$$\begin{aligned} r_2 &= g - (\tfrac{1}{4}X + \tfrac{1}{4})r_1 \\ &= g - (\tfrac{1}{4}X + \tfrac{1}{4})(f - (X-2)g) \\ &= -(\tfrac{1}{4}X + \tfrac{1}{4})f + [1 + (\tfrac{1}{4}X + \tfrac{1}{4})(X-2)]g \\ &= -(\tfrac{1}{4}X + \tfrac{1}{4})f + (\tfrac{1}{4}X^2 - \tfrac{1}{4}X + \tfrac{1}{2})g \end{aligned}$$

Así : $(f:g) = -r_2 = (\tfrac{1}{4}X + \tfrac{1}{4})f - (\tfrac{1}{4}X^2 - \tfrac{1}{4}X + \tfrac{1}{2})g$.

Corolario 7.1.13. (Mcd y combinación polinomial.)

Sean $f, g \in K[X]$ no ambos nulos. El máximo común divisor entre f y g es el (único) polinomio mónico $h \in K[X]$ que satisface simultáneamente las dos condiciones siguientes :

- $h \mid f$ *y* $h \mid g$,
- *Existen* $s, t \in K[X]$ *tales que* $h = sf + tg$.

También se puede deducir, como en el caso de los enteros, la propiedad siguiente que relaciona el máximo común divisor con los divisores comunes mediante divisibilidad.

Corolario 7.1.14. (Mcd y divisores comunes.)

Sean $f, g \in K[X]$ no ambos nulos. El máximo común divisor entre f y g es el (único) polinomio mónico $h \in K[X]$ que satisface simultáneamente las dos condiciones siguientes :

- $h \mid f$ *y* $h \mid g$,
- *Si* $\tilde{h} \in K[X]$ *satisface que* $\tilde{h} \mid f$ *y* $\tilde{h} \mid g$, *entonces* $\tilde{h} \mid h$.

Definición 7.1.15. (Polinomios coprimos)

Sean $f, g \in K[X]$ no ambos nulos. Se dice que son *coprimos* si satisfacen

$$(f:g) = 1.$$

Es decir si ningún polinomio de grado ≥ 1 divide simultáneamente a f y a g . O equivalentemente si existen polinomios $s, t \in K[X]$ tales que

$$1 = sf + tg.$$

Proposición 7.1.16. (Divisibilidad con coprimalidad.)

Sean f, g, $h \in K[X]$, entonces:

1. *Si g y h son* coprimos, *entonces* $g \mid f$ *y* $h \mid f \iff gh \mid f$

2. Si g *y* h *son* coprimos, *entonces* $g \mid h\,f \iff g \mid f$.

Demostración. $(g : h) = 1 \Longrightarrow \exists\, s, t \in K[X]$ tales que $1 = sg + th$. Luego

$$f = sgf + thf. \tag{7.1}$$

1. ($\Leftarrow$) vale siempre.

   ($\Rightarrow$) $g\,h$ divide al primer sumando a la derecha en (7.1) pues $h \mid f$ por hipótesis, y $g\,h$ divide también al segundo sumando pues $g \mid f$ por hipótesis. Por lo tanto $g\,h$ divide a la suma que es igual a f.

2. ($\Leftarrow$) vale siempre.

   ($\Rightarrow$) g divide claramente al primer sumando a la derecha en (7.1), y también divide al segundo sumando pues $g \mid hf$ por hipótesis. Por lo tanto g divide a la suma que es igual a f. divide a f.

□

7.1.3 El Teorema Fundamental de la Aritmética para Polinomios.

Observación 7.1.17. (Primalidad de los polinomios irreducibles.)

Sea f un polinomio *irreducible* en $K[X]$. Entonces

- Para todo $g \in K[X]$, $(f : g) = \frac{f}{\mathrm{cp}(f)}$ si $f \mid g$ y $(f : g) = 1$ si $f \nmid g$.
- Para todo $g, h \in K[X]$, $f \mid g\,h \implies f \mid g$ o $f \mid h$.

Teorema 7.1.18. (Teorema Fundamental de la Aritmética para polinomios.)

Sea K *un cuerpo, y sea* $f \in K[X]$ *un polinomio no constante. Entonces* existen únicos polinomios irreducibles mónicos distintos $g_1, \ldots, g_r$ *en* $K[X]$ *tales que*

$$f = c\,{g_1}^{m_1} \ldots {g_r}^{m_r} \quad \text{donde} \quad c \in K \setminus \{0\} \text{ y } m_1, \ldots, m_r \in \mathbb{N}$$

(La unicidad de los factores irreducibles g_i *es salvo el orden de los factores.) La constante* c *resulta ser el coeficiente principal de* f.

<u>*Ejemplo:*</u> El polinomio $(X^2+1)(X^2-2)$ está factorizado en factores irreducibles en $\mathbb{Q}[X]$ (pues ambos factores son irreducibles) pero su factorización en $\mathbb{R}[X]$ es $(X^2+1)(X-\sqrt{2})(X+\sqrt{2})$ y su factorización en $\mathbb{C}[X]$ es $(X-i)(X+i)(X-\sqrt{2})(X+\sqrt{2})$. Notemos que en $\mathbb{Q}[X]$ el polinomio

$(X^2+1)(X^2-2)$ es **reducible** en $\mathbb{Q}[X]$, pues $X^2+1 \mid f$ en $\mathbb{Q}[X]$ pero sin embargo **no tiene raíces** en $\mathbb{Q}$. Pero de todos modos como veremos en lo que sigue la búsqueda de raíces de f, si tenemos la suerte de encontrar, ayuda para la factorización.

7.2 Evaluación y Raíces.

Sea $f = a_n X^n + \cdots + a_1 X + a_0 \in K[X]$ un polinomio, entonces f define en forma natural una función

$$f : K \to K, \quad f(x) = a_n x^n + \cdots + a_1 x + a_0 \quad \forall\, x \in K$$

que se llama la función *evaluación*.

Esta función evaluación cumple las dos propiedades siguientes para todo $f, g \in K[X]$:

$$\big(f+g\big)(x) = f(x) + g(x) \quad \text{y} \quad \big(f \cdot g\big)(x) = f(x) \cdot g(x), \quad \forall\, x \in K.$$

En particular, si $f = q\,g + r$ con $q, r \in K[X]$, entonces

$$f(x) = q(x)\,g(x) + r(x), \ \forall\, x \in K.$$

<u>*Ejemplos:*</u>

- Sea $f = X^2 + X - 2 \in \mathbb{Q}[X]$. Entonces $f(3) = 3^2 + 3 - 2 = 10$, $f(0) = -2$ y $f(1) = 1^2 + 1 - 2 = 0$.
- Sea $f = \sum_{i=0}^{n} a_i X^i \in K[X]$. Entonces $f(0) = a_0$ y $f(1) = \sum_{i=0}^{n} a_i$.
- Sea $f = c$ un polinomio constante en $K[X]$. Entonces $f(x) = c$, $\forall\, x \in K$.
- Determinar todos los polinomios $f \in \mathbb{R}[X]$ de grado ≤ 2 (o nulo) tales que $f(0) = 1$ y $f(1) = f(2)$:

  El polinomio f es de la forma $f = aX^2 + bX + c \in \mathbb{R}[X]$. Se tiene $f(0) = 1 \ \Leftrightarrow \ c = 1$ y $f(1) = f(2) \ \Leftrightarrow \ a + b + c = 4a + 2b + c$, es decir $3a + b = 0$. En definitiva, $b = -3a$ y $c = 1$, lo que implica que $f = aX^2 - 3aX + 1$, $a \in \mathbb{R}$.
- Sea $f \in \mathbb{Q}[X]$ tal que $f(0) = 1$ y $f(1) = f(2) = 3$. Calcular el resto de dividir f por $X(X-1)(X-2)$:

  El polinomio f se escribe por el Algoritmo de División como

  $$f = q \cdot X(X-1)(X-2) + r \ \text{ con } \ r = 0 \ \text{ o } \ \operatorname{gr}(r) < 3,$$

o sea $r = aX^2 + bX + c \in \mathbb{Q}[X]$. Por lo tanto, dado que el polinomio $X(X-1)(X-2)$ se anula en 0, 1 y 2, si evaluamos en $x = 0$, $x = 1$ y $x = 2$ obtenemos $f(0) = r(0)$, $f(1) = r(1)$ y $f(2) = r(2)$. O sea $r(0) = 1$, $r(1) = r(2) = 3$. Por el inciso anterior, $r = aX^2 - 3aX + 1$, con $r(1) = a - 3a + 1 = 3$, es decir $-2a = 2$, o sea $a = -1$. Se concluye $r = -X^2 + 3X + 1$.

Definición 7.2.1. (Raíz de un polinomio.)

Sean $f \in K[X]$ un polinomio y $x \in K$. Si $f(x) = 0$, se dice que x es una *raíz* de f (en K).

Proposición 7.2.2. (Equivalencias de raíz.)

$$\begin{aligned} x \in K \text{ es raíz de } f &\iff f(x) = 0 \\ &\iff X - x \mid f \\ &\iff f = q \cdot (X - x) \text{ para algún } q \in K[X]. \end{aligned}$$

Es decir, si $f \neq 0$, $X - x$ es un factor irreducible (mónico) en la descomposición en irreducibles de $f \in K[X]$.

Demostración. Las equivalencia $X - x \mid f \iff f = q\,(X - x)$ para algún $q \in K[X]$ es simplemente por la definición de divisibilidad. Probemos la equivalencia $f(x) = 0 \iff f = q \cdot (X - x)$ para algún $q \in K[X]$:
Por el algoritmo de división, $f = q \cdot (X - x) + r$ donde o bien $r = 0$ o bien $\mathrm{gr}(r) < \mathrm{gr}(X - x) = 1$, es decir $r = 0$ o $\mathrm{gr}(r) = 0$. Así, en todo caso, $r \in K$: r es un polinomio constante. Y por lo tanto cuando evaluamos la expresión en $X = x$ obtenemos

$$f(x) = q(x) \cdot (x - x) + r(x) = q(x) \cdot 0 + r = r$$

ya que $x - x = 0$ y el polinomio constante r evaluado en x da r.
Por lo tanto $f(x) = 0 \iff r = 0$, es decir $f(x) = 0 \iff f = q\,(X - x)$ como se quería probar. □

El razonamiento que acabamos de hacer muestra también el resultado un poco más general siguiente.

Proposición 7.2.3. (Teorema del resto.)

Dados $f \in K[X]$ y $x \in K$, se tiene que $r_{X-x}(f) = f(x)$.

Demostración. Si dividimos al polinomio f por el polinomio $X - x \in K[X]$, obtenemos

$$f = q \cdot (X - x) + r \quad \text{con} \quad r = 0 \text{ o } \mathrm{gr}(r) = 0,$$

o sea $r \in K$ es un polinomio constante. Evaluando como arriba la expresión en $x \in K$ se obtiene $f(x) = r$, y por lo tanto $f = q \cdot (X - x) + f(x)$. Es decir $r_{X-x}(f) = f(x)$. □

Observación 7.2.4. Sean $f, g \in K[X]$ con $g \neq 0$ tal que $g \mid f$ en $K[X]$. Sea $x \in K$. Si x es raíz de g, entonces x es raíz de f también. (Pues $g \mid f$ implica existe $q \in K[X]$ tal que $f = q\,g$ y por lo tanto $f(x) = q(x)\,g(x) = q(x) \cdot 0 = 0$.)

Ejemplos:

- 1 es raíz del polinomio $X^2 + X - 2 \in \mathbb{Q}[X]$.
- 0 es raíz de $f \in K[X]$ si y solo si el coeficiente constante de f es igual a 0.
- f constante: $f = c$ con $c \in K$.

  Entonces, o bien $c = 0$ y todo $x \in K$ es raíz de f, ó bien $c \neq 0$ y f no tiene ninguna raíz en K.
- f de grado 1: $f = aX + b$ con $a, b \in K$, $a \neq 0$. Entonces $x = -\frac{b}{a}$ es raíz de f y $f = a\big(X - (-\frac{b}{a})\big) = a(X - x)$ es la factorización del polinomio irreducible f en $K[X]$.

El resultado siguiente puede ser útil a la hora de buscar raíces si se tiene alguna información adicional sobre el polinomio.

Proposición 7.2.5. (Raíz común y Mcd.)

Sean $f, g \in K[X]$ no ambos nulos y sea $x \in K$. Entonces

$$f(x) = 0 \;\; y \;\; g(x) = 0 \iff (f : g)(x) = 0.$$

Demostración.

- ($\Rightarrow$) Se sabe que existen $s, t \in K[X]$ tales que $(f : g) = s\,f + t\,g$. Por lo tanto $(f : g)(x) = s(x)f(x) + t(x)g(x) = 0$ si $f(x) = g(x) = 0$.
- ($\Leftarrow$) Como $(f : g) \mid f$ y $(f : g) \mid g$ en $K[X]$, si $(f : g)(x) = 0$, entonces $f(x) = 0$ y $g(x) = 0$.

□

7.2.1 Multiplicidad de las raíces.

Vimos en los ejemplos anteriores que a veces una raíz puede aparecer "repetida". Por ejemplo si consideramos el polinomio

$$f = 10(X - 1)^2(X + 1)(X - 2)^3$$

tenemos que la raíz 1 "aparece" dos veces, la raíz -1 una sola, y la raíz 2 tres veces. Esto sugiere la noción de multiplicidad de una raíz de un polinomio.

Definición 7.2.6. (Multiplicidad de una raíz).

Sea $f \in K[X]$ *no nulo.*

- Sea $m \in \mathbb{N}_0$. Se dice que $x \in K$ es una *raíz de multiplicidad* m *de* f si $(X-x)^m \mid f$ y $(X-x)^{m+1} \nmid f$, o lo que equivalente, existe $q \in K[X]$ tal que

  $$f = (X-x)^m\, q \quad \text{con} \quad q(x) \neq 0.$$

  Notamos aquí $\text{mult}(x; f) = m$.

- Se dice que $x \in K$ es una *raíz simple de* f cuando $\text{mult}(x; f) = 1$, es decir $X-x \mid f$ pero $(X-x)^2 \nmid f$, o lo que es equivalente $f = (X-x)\, q$ con $q(x) \neq 0$.

- Se dice que $x \in K$ es una *raíz múltiple de* f cuando $\text{mult}(x; f) > 1$, es decir $(X-x)^2 \mid f$.

- Se dice que $x \in K$ es una *raíz doble de* f cuando $\text{mult}(x; f) = 2$ y que es una *raíz triple de* f cuando $\text{mult}(x; f) = 3$.

Está claro de la definición que dado un polinomio $f \in K[X]$ *no nulo* y $x \in K$ una raíz de f, su multiplicidad m siempre está acotada por el grado del polinomio: $\text{mult}(x; f) \leq \text{gr}(f)$.

Ejemplos:

- En el ejemplo $f = 10(X-1)^2(X+1)(X-2)^3$, 1 es raíz doble de f, -1 es simple y 2 es triple.

- $\text{mult}(x; f) = 0$ si y solo si x no es raíz de f.

Proposición 7.2.7. (Multiplicidad en suma y producto.)

Sea K un cuerpo y sean $f, g \in K[X]$ no nulos. Sea $x \in K$. Entonces

1. *Si* $\text{mult}(x; f) \neq \text{mult}(x; g)$, *entonces* $\text{mult}(x; f+g) = \min\{\text{mult}(x; f), \text{mult}(x; g)\}$.
2. $\text{mult}(x; fg) = \text{mult}(x; f) + \text{mult}(x; g)$.

Demostración. Pongamos $m_1 := \text{mult}(x; f)$ y $m_2 = \text{mult}(x; g)$ donde $m_1, m_2 \in \mathbb{N}_0$, o sea $f = (X-x)^{m_1} q_1$ con $q_1(x) \neq 0$ y $g = (X-x)^{m_2} q_2$ con $q_2(x) \neq 0$.

1. Supongamos sin pérdida de generalidad que $m_1 < m_2$. Entonces

   $$f+g = (X-x)^{m_1}\big(q_1 + (X-x)^{m_2-m_1} q_2\big) \quad \text{donde} \quad \big(q_1 + (X-x)^{m_2-m_1} q_2\big)(x) \neq 0$$

pues $\big(q_1 + (X-x)^{m_2-m_1}q_2\big)(x) = q_1(x) \neq 0$ al ser $m_2 - m_1 \geq 1$, y por lo tanto $\text{mult}(x; f+g) = m_1$.

Notar que si $\text{mult}(x; f) = \text{mult}(x; g)$ puede pasar cualquier cosa. Por ejemplo $\text{mult}(0; 1) = 0 = \text{mult}(0; X^n - 1)$ pero

$$\text{mult}(0; 1 + (X^n - 1)) = \text{mult}(0; X^n) = n.$$

2. Se tiene

$$f\,g = (X-x)^{m_1+m_2}q_1q_2 \quad \text{donde} \quad (q_1q_2)(x) \neq 0$$

pues $(q_1q_2)(x) = q_1(x)q_2(x) \neq 0$ al ser $q_1(x) \neq 0$ y $q_2(x) \neq 0$, y por lo tanto $\text{mult}(x; fg) = m_1 + m_2$.

□

Se recuerda que si $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$ entonces

$$f' = n\,a_nX^{n-1} + (n-1)\,a_{n-1}X^{n-2} + \cdots + a_1 \in K[X]$$

es la *derivada* de f, que satisface:

- $(f+g)' = f' + g'$ y $(fg)' = f'g + fg'$, $\forall\, f, g \in K[X]$.
- $(g \circ f)' = g'(f)f'$, $\forall\, f, g \in K[X]$.
  En particular $\big((X-x)^k\big)' = k(X-x)^{k-1}$.
- $f'' = (f')'$ y en general $f^{(m)} = (f')^{(m-1)}$, $\forall\, m \in \mathbb{N}$.

Observemos que si x es una raíz múltiple de f, es decir $f = (X-x)^2q$ para algún $q \in K[X]$, entonces

$$f' = 2(X-x)q + (X-x)^2q' = (X-x)\big(2\,q + (X-x)\,q'\big).$$

Por lo tanto $f'(x) = 0$ también. O sea no sólo vale que $f(x) = 0$ pero también $f'(x) = 0$. Esto es la base de la siguiente proposición que relaciona la multiplicidad con las derivadas de f.

Proposición 7.2.8. (Raíz múltiple y derivada.)

Sea $f \in K[X]$ y sea $x \in K$. Entonces

- *x es raíz múltiple de f si y solo si $f(x) = 0$ y $f'(x) = 0$.*
- *x es raíz simple de f si y solo si $f(x) = 0$ y $f'(x) \neq 0$.*

Demostración. Alcanza con probar el primer inciso, ya que el segundo es decir que x es raíz de f pero no múltiple.

Sabemos que $x \in K$ es raíz de f si y solo si $f = (X - x)\, q$ para algún $q \in K[X]$. Derivando, $f' = q + (X - x)q'$ satisface $f'(x) = q(x)$. En particular $f'(x) = 0 \Leftrightarrow q(x) = 0$.

Por lo tanto,

$$f(x) = 0 \text{ y } f'(x) = 0 \implies (X - x)^2 \mid f.$$

La recíproca fue observada antes de enunciar la proposición: si $(X-x)^2 \mid f$, entonces $f(x) = f'(x) = 0$. □

Ejemplos:

- Probar que el polinomio $2X^{15}+7X^7+2X^3+1$ no tiene raíces múltiples reales.

  Supongamos que sí: Sea $x \in \mathbb{R}$ tal que $f(x) = f'(x) = 0$. En particular, dado que $f' = 30X^{14}+49X^6+6X^2$, se tendría $0 = f'(x) = 30x^{14} + 49x^6 + 6x^2$. Lo que implica que $x = 0$ dado que todos los exponentes en f' son pares (luego $\forall\, x \in \mathbb{R}$, $f'(x) \geq 0$ y $f'(x) = 0 \Leftrightarrow x = 0$.) Pero claramente $f(0) = 1 \neq 0$.

- Hallar para qué valores de $a \in \mathbb{C}$ el polinomio $f = X^8 - 2X^4 + a$ tiene raíces múltiples en $\mathbb{C}$.

  Sea $x \in \mathbb{C}$ una raíz múltiple. Equivalentemente, $f(x) = f'(x) = 0$. Es decir, dado que $f' = 8X^7 - 8X^3$, $8x^7 - 8x^3 = 8x^3(x^4 - 1) = 0$. O sea $x = 0$ o $x^4 = 1$.

  - $f(0) = 0 \Leftrightarrow a = 0$: en ese caso $f = X^8 - 2X^4 = X^4(X^4 - 2)$, o sea f tiene la raíz 0 con multiplicidad 4.
  - Si $x^4 = 1$, entonces

    $$f(x) = x^8 - 2x^4 + a = (x^4)^2 - 2x^4 + a = 1 - 2 \cdot 1 + a = -1 + a$$

    implica que $f(x) = 0 \Leftrightarrow a = 1$. Por lo tanto $f = X^8-2X^4+1 = (X^4 - 1)^2$ tiene claramente la raíz 1 que es múltiple.

Se puede ser más explícito cuando se trabaja sobre $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$ (pero atención, el argumento no es válido para los cuerpos finitos $\mathbb{Z}/p\mathbb{Z}$).

Proposición 7.2.9. (Multiplicidad en f y multiplicidad en f'.)
Sea $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$, sea $x \in K$ y sea $m \in \mathbb{N}$. Entonces

$$\text{mult}(x; f) = m \quad \Longleftrightarrow \quad f(x) = 0 \;\; y \;\; \text{mult}(x; f') = m - 1.$$

Demostración.

($\Rightarrow$)

$$\begin{aligned}
\text{mult}(x;f) = m \iff & \exists\, q \in K[X] \text{ tal que } f = (X-x)^m\, q \text{ con } q(x) \neq 0 \\
\implies & f' = m(X-x)^{m-1}q + (X-x)^m q' \\
& = (X-x)^{m-1}\big(m\,q + (X-x)\,q'\big) \\
\implies & f' = (X-x)^{m-1}h, \\
& \text{donde } h = m\,q + (X-x)\,q' \in K[X] \text{ es tal que} \\
& h(x) = m\,q(x) \neq 0 \text{ pues } q(x) \neq 0.
\end{aligned}$$

Por lo tanto, $f(x) = 0$ y $\text{mult}(x;f') = m-1$.

(Este argumento no es válido en un cuerpo finito $\mathbb{Z}/p\mathbb{Z}$ si $p \mid m$ pues en ese caso $h(x) = 0$.)

($\Leftarrow$) Queremos probar que si $f(x) = 0$ y $\text{mult}(x;f') = m-1$, entonces $\text{mult}(x;f) = m$. Como $f(x) = 0$, x es raíz de f con cierta multiplicidad $k \geq 1$ (y queremos probar que en realidad $k = m$). Por lo tanto por la implicación que acabamos de probar, $\text{mult}(x;f') = k-1$. Pero por hipótesis, $\text{mult}(x;f') = m-1$, de lo cual se deduce $k-1 = m-1$ y por lo tanto $k = m$ como se quería probar. □

Se obtiene el corolario siguiente en términos del máximo común divisor entre f y f'.

Corolario 7.2.10. (Multiplicidad en f y multiplicidad en $(f : f')$.)

Sea $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$, sea $x \in K$ y sea $m \geq 2$. Entonces

$$\text{mult}(x;f) = m \quad \iff \quad \text{mult}(x;(f:f')) = m-1.$$

Demostración.

($\Rightarrow$) Tenemos que probar que $(X-x)^{m-1} \mid (f:f')$ pero $(X-x)^m \nmid (f:f')$. Como $\text{mult}(x;f) = m$, entonces $\text{mult}(x;f') = m-1$ por la proposición anterior, y por lo tanto $(X-x)^{m-1} \mid f'$. Por otro lado $(X-x)^{m-1} \mid f$ también pues $(X-x)^m \mid f$, con lo cual $(X-x)^{m-1} \mid (f:f')$. Pero $(X-x)^m \nmid (f:f')$ pues si $(X-x)^m$ dividiera a $(f:f')$, dividiría en particular a f', lo que contradice que $\text{mult}(x;f') = m-1$.

($\Leftarrow$) $\text{mult}(x;(f:f')) = m-1$ implica en particular que $(X-x)^{m-1} \mid f$, y como $m \geq 2$ entonces $m-1 \geq 1$, lo que implica $f(x) = 0$. Por otro lado $(X-x)^{m-1} \mid f'$ y por lo tanto $\text{mult}(x;f') = k \geq m-1$. Estos dos hechos implican por la proposición anterior que $\text{mult}(x;f) = k+1 \geq m$. Ahora bien, por ($\Rightarrow$), $\text{mult}(x;f) = k+1 \geq m \geq 2$ implica $\text{mult}(x;(f:f')) = k$. Pero por hipótesis $\text{mult}(x;(f:f')) = m-1$, o sea $k = m-1$ y por lo tanto $k+1 = m$, es decir $\text{mult}(x;f) = m$ como se quería probar. □

Finalmente podemos presentar también la importante caracterización de la multiplicidad en términos de la derivadas.

Proposición 7.2.11. (Raíz de multiplicidad m y derivadas hasta orden m.)

Sea $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$, sea $x \in K$ y sea $m \in \mathbb{N}$. Entonces

$$\text{mult}(x; f) = m \iff \begin{cases} f(x) = 0 \\ f'(x) = 0 \\ \vdots \\ f^{(m-1)}(x) = 0 \\ f^{(m)}(x) \neq 0. \end{cases}$$

Demostración. Por inducción en $m \in \mathbb{N}$:

$p(m)$: Dado $g \in K[X]$,

$$x \in K \text{ es t.q. } \text{mult}(x; g) = m \iff \begin{cases} g(x) = 0 \\ g'(x) = 0 \\ \vdots \\ g^{(m-1)}(x) = 0 \\ g^{(m)}(x) \neq 0. \end{cases}$$

- Caso base, $m = 1$: $p(1)$ es V? Sí pues $\text{mult}(x; g) = 1 \Leftrightarrow g(x) = 0$ y $g'(x) \neq 0$ por la Proposicíón 7.2.8.

- Paso inductivo, $p(k)$ V $\rightarrow$ $p(k+1)$ V:

  Por la Proposición 7.2.9,

  $$\text{mult}(x, f) = k + 1 \Leftrightarrow f(x) = 0 \text{ y } \text{mult}(x, f') = k.$$

  Por HI, para $g = f'$ se tiene que

  $$f'(x) = 0, (f')'(x) = 0, \ldots, (f')^{(k-1)}(x) = 0 \text{ y } (f')^{(k)}(x) \neq 0,$$

  es decir

  $$f'(x) = 0, f''(x) = 0, \ldots, f^{(k)}(x) = 0 \text{ y } f^{(k+1)}(x) \neq 0.$$

  Así concluimos

  $$\text{mult}(x, f) = k + 1 \Leftrightarrow f(x) = 0, f'(x) = 0, \ldots, f^{(k)}(x) = 0 \text{ y } f^{(k+1)}(x) \neq 0.$$

  Hemos probado el paso inductivo.

Por lo tanto $p(m)$ es Verdadera para todo $m \in \mathbb{N}$. □

7.2.2 Cantidad de raíces en K.

Vamos a probar ahora que un polinomio $f \in K[X]$ no nulo no puede tener más raíces en el cuerpo K, aún contadas con su multiplicidad, que su grado.

Proposición 7.2.12. (Raíces de f y factores.)

Sea $f \in K[X]$ no nulo.

- *Sean $x_1, x_2 \in K$ raíces* distintas *de f tales que* $\text{mult}(x_1; f) = m_1$ *y* $\text{mult}(x_2; f) = m_2$. *Entonces* $(X - x_1)^{m_1}(X - x_2)^{m_2} \mid f$.
- *Sean $x_1, \ldots, x_r \in K$ raíces* distintas *de f tales que*

$$\text{mult}(x_1; f) = m_1, \ldots, \text{mult}(x_r; f) = m_r.$$

Entonces

$$(X - x_1)^{m_1} \cdots (X - x_r)^{m_r} \mid f.$$

Demostración. • Esto es porque $(X - x_1)^{m_1}$ y $(X - x_2)^{m_2}$ son polinomios coprimos al ser potencias de polinomios irreducibles distintos. Luego,

$$(X - x_1)^{m_1} \mid f \text{ y } (X - x_2)^{m_2} \mid f \implies (X - x_1)^{m_1}(X - x_2)^{m_2} \mid f.$$

- Por inducción en la cantidad de raíces distintas.

□

En esas condiciones se tiene que si $f \neq 0$, $\text{gr}\left((X - x_1)^{m_1} \cdots (X - x_r)^{m_r}\right) \leq \text{gr}(f)$, es decir $m_1 + \cdots + m_r \leq \text{gr}(f)$. Se obtuvo:

Proposición 7.2.13. (Cantidad de raíces en K.)

Sea K un cuerpo y sea $f \in K[X]$ un polinomio no nulo *de grado n. Entonces f tiene a lo sumo n raíces en K contadas con multiplicidad.*

Esto implica que sobre un cuerpo *infinito* K, dos polinomios son iguales si y sólo si coinciden como función de K en K.

Corolario 7.2.14. (Igualdad de polinomios.)

1. *Sea $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$, y sean $f, g \in K[X]$. Entonces*

$$f = g \text{ en } K[X] \iff f(x) = g(x), \ \forall\, x \in K.$$

2. *¡Ojo que no esto no es cierto en $\mathbb{Z}/p\mathbb{Z}[X]$! Por ejemplo el polinomio $X^p - X$ coincide con el polinomio 0 en todos los elementos de $\mathbb{Z}/p\mathbb{Z}$ (verificarlo) pero sin embargo no son el mismo polinomio...*

Demostración. Probamos solo (i), y alcanza con probar la vuelta, ya que si dos polinomios son iguales, tienen los mismos coeficientes y por lo tanto coinciden en todos los valores de K.
Supongamos entonces que $f, g \in K[X]$ satisfacen $f(x) = g(x)$, $\forall\, x \in K$, y definamos el polinomio $h := f - g \in K[X]$. Por lo tanto,

$$h(x) = f(x) - g(x) = 0, \ \forall\, x \in K.$$

O sea ¡todos los elementos de K (que es infinito al ser $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$) son raíces de h! Pero esto es imposible si $h \neq 0$ pues h no puede tener más raíces que su grado.... Por lo tanto $h = 0$ en $K[X]$, es decir, $f = g$ en $K[X]$. □

7.2.3 Cálculo de raíces en $\mathbb{Q}$ de polinomios en $\mathbb{Q}[X]$.

Un hecho notorio es que se pueden encontrar todas las raíces racionales de un polinomio $f \in \mathbb{Q}[X]$ por medio de un algoritmo. Este hecho es una consecuencia de que todo número entero $a \in \mathbb{Z} \setminus \{0\}$ tiene un número finito de divisores posibles, que se pueden calcular.

Sea $f = a_n X_n + \cdots + a_0 \in \mathbb{Q}[X]$. Entonces existe $c \in \mathbb{Z} \setminus \{0\}$ tal que $g = c\, f \in \mathbb{Z}[X]$, es decir g tiene todos sus coeficientes enteros (por ejemplo, eligiendo c como el mínimo común múltiplo de los denominadores de los coeficientes de f), y además las raíces de f claramente coinciden con las de g.

Por ejemplo, $f = \frac{3}{2}X^5 - \frac{1}{3}X^4 + X^2 - \frac{5}{4} \in \mathbb{Q}[X]$ y $g = 12\, f = 18X^5 - 4X^4 + 12X^2 - 15 \in \mathbb{Z}[X]$ tienen exactamente las mismas raíces.

Por consiguiente para encontrar las raíces racionales de un polinomio en $\mathbb{Q}[X]$, nos podemos restringir a estudiar cómo encontrar las raíces racionales de un polinomio en $\mathbb{Z}[X]$.

Lema 7.2.15. (Lema de Gauss.)

Sea $f = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ con $a_n,\ a_0 \neq 0$. Si $\frac{\alpha}{\beta} \in \mathbb{Q}$ es una raíz racional de f, con α y $\beta \in \mathbb{Z}$ coprimos, *entonces $\alpha \,|\, a_0$ y $\beta \,|\, a_n$.*

Demostración.

$$\begin{aligned} f\left(\frac{\alpha}{\beta}\right) = 0 \quad &\iff \quad a_n \left(\frac{\alpha}{\beta}\right)^n + a_{n-1}\left(\frac{\alpha}{\beta}\right)^{n-1} + \cdots + a_1\left(\frac{\alpha}{\beta}\right) + a_0 = 0 \\ &\iff \quad \frac{a_n\alpha^n + a_{n-1}\alpha^{n-1}\beta + \cdots + a_1\alpha\beta^{n-1} + a_0\beta^n}{\beta^n} = 0 \\ &\iff \quad a_n\alpha^n + a_{n-1}\alpha^{n-1}\beta + \cdots + a_1\alpha\beta^{n-1} + a_0\beta^n = 0. \end{aligned}$$

Por lo tanto, $\alpha\left(a_n\alpha^{n-1}+\cdots+a_1\beta^{n-1}\right)=-a_0\beta^n$.

Esto implica $\alpha\,|\,-a_0\beta^n$ en $\mathbb{Z}$. Pero al ser α y β enteros coprimos, α es coprimo con β^n también, y por lo tanto $\alpha\,|\,a_0$.

De la misma manera, $\beta\left(a_{n-1}\alpha^{n-1}+\cdots+a_0\beta^{n-1}\right)=-a_n\alpha^n$ implica que $\beta\,|\,-a_n\alpha^n$ pero al ser coprimo con α, resulta $\beta\,|\,a_n$. □

Observación 7.2.16. (Algoritmo para calcular las raíces en $\mathbb{Q}$ de $f\in\mathbb{Z}[X]$.)

En las condiciones del teorema anterior, el Lema de Gauss implica que si se construye el conjunto (finito) $\mathcal{N}$ (por numerador) de los divisores positivos y negativos de a_0 y el conjunto $\mathcal{D}$ (por denominador) de los de a_n, las raíces del polinomio f se encuentran en el conjunto de todas las fracciones coprimas $\frac{\alpha}{\beta}$, eligiendo α en $\mathcal{N}$ y β en $\mathcal{D}$. Chequeando para cada fracción $\frac{\alpha}{\beta}$ así construída si $f(\frac{\alpha}{\beta})=0$, se obtienen todas las raíces racionales de f.

Simplemente hay que tener un poco de cuidado en que este procedimiento no aclara la multiplicidad de cada raíz.

Ejemplo: Hallar las raíces racionales del polinomio racional

$$f=X^8+\frac{8}{3}X^7+\frac{1}{3}X^6-\frac{14}{3}X^5-\frac{14}{3}X^4-\frac{4}{3}X^3.$$

Limpiando los denominadores de f se obtiene el polinomio entero g con las mismas raíces:

$$g=3X^8+8X^7+X^6-14X^5-14X^4-4X^3=X^3(3X^5+8X^4+X^3-14X^2-14X-4).$$

Claramente, $\mathrm{mult}(0;g)=3$ (y por lo tanto $\mathrm{mult}(0;f)=3$ también pues $g=3\,f$), y las restantes raíces racionales de g (o f) son las de

$$h=3X^5+8X^4+X^3-14X^2-14X-4.$$

Aquí, $a_0=-4$ y $a_n=3$.

Los divisores de a_0 son $\pm1,\pm2,\pm4$ y los divisores de a_n son $\pm1,\pm3$, luego las raíces racionales se buscan en el conjunto :

$$\{\,\pm1,\pm2,\pm4,\pm\frac{1}{3},\pm\frac{2}{3},\pm\frac{4}{3}\,\}$$

Chequeando se obtiene que $h(-1)=0$ y $h(-2/3)=0$, y éstas son las únicas raíces racionales (distintas) de h.

Para conocer con qué multiplicidad son éstas raíces de h, se puede o bien dividir h por $(X+1)(X+\frac{2}{3})$ y volver a evaluar el cociente en -1 y $-2/3$, o bien también se puede derivar h:

$h' = 15X^4 + 32X^3 + 3X^2 - 28X - 14$ y se tiene que $h'(-1) = 0$ mientras que $h'(-2/3) \neq 0$.

O sea -1 es raíz de multiplicidad ≥ 2 y $-2/3$ es raíz simple.

Volviendo a derivar h: $h'' = 60X^3 + 96X + 6X - 28$ y $h''(-1) \neq 0$.

Se concluye que -1 es raíz doble de h.

Finalmente la factorización de h en $\mathbb{Q}[X]$ es:

$$h = 3(X+1)^2(X+\frac{2}{3})(X^2-2)$$

ya que $X^2 - 2$ es irreducible en $\mathbb{Q}[X]$.

Y dado que $f = \frac{1}{3}X^3\, h$, obtenemos la siguiente factorización de f en $\mathbb{Q}[X]$:

$$f = X^3(X+1)^2(X+\frac{2}{3})(X^2-2).$$

Observación 7.2.17. El Lema de Gauss provee un algoritmo para calcular todas las raíces racionales de un polinomio racional, pero se ve claramente que éste es extremadamente costoso, pues hay que evaluar el polinomio de entrada en un gran número de fracciones $\dfrac{\alpha}{\beta}$ (la cantidad de fracciones está relacionada con la cantidad de divisores de a_0 y a_n).

7.3 Factorización en $K[X]$.

Como ya se mencionó, todo polinomio no constante en $K[X]$ se factoriza en forma única como producto de polinomios irreducibles mónicos en $K[X]$, multiplicados por su coeficiente principal en $K^\times$. Estudiaremos en lo que sigue más en detalle como puede ser esa factorización según quién es el cuerpo K.

7.3.1 Polinomios cuadráticos en $K[X]$.

Sea $f = aX^2 + bX + c$ con $a, b, c \in K$, $a \neq 0$.

Como f tiene grado 2, es reducible si y solo si tiene un factor en $K[X]$ de grado 1, que podemos asumir mónico de la forma $X - x$ con $x \in K$. Así que en este caso f es reducible en $K[X]$ si y solo si f tiene una raíz $x \in K$.

Asumimos en lo que sigue que $1 + 1 \neq 0$ en K, es decir $2 \neq 0 \in K$ (por ejemplo $K \neq \mathbb{Z}/2\mathbb{Z}$) para que tenga sentido dividir por 2 en la cuenta que hacemos a continuación.

Luego

$$\begin{aligned} f &= a\left(X^2 + \frac{b}{a}X + \frac{c}{a}\right) \\ &= a\left(\left(X + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right) \\ &= a\left(\left(X + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}\right). \end{aligned}$$

Se define el *discriminante* de f como $\Delta = \Delta(f) := b^2 - 4ac \in K$.

Si existe $\omega \in K$ tal que $\omega^2 = \Delta$, o sea tal que $\left(\frac{w}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}$, se tiene que :

$$f = a\left(\left(X + \frac{b}{2a}\right)^2 - \left(\frac{\omega}{2a}\right)^2\right) = a\left(X + \frac{b}{2a} - \frac{\omega}{2a}\right)\left(X + \frac{b}{2a} + \frac{\omega}{2a}\right)$$

por diferencia de cuadrados. Por lo tanto

$$f = a\left(X - \frac{-b + \omega}{2a}\right)\left(X - \frac{-b - \omega}{2a}\right),$$

lo que implica, dado que K es un cuerpo, $f(x) = 0 \Leftrightarrow x - \frac{-b + \omega}{2a} = 0$ o $x - \frac{-b - \omega}{2a} = 0$. Es decir, se obtienen las 2 raíces (a lo mejor la misma repetida si $\omega = 0$):

$$x_\pm = \frac{-b \pm \omega}{2a}.$$

Lo que probamos hasta ahora es que si $\Delta \in K$ es un cuadrado en K, entonces el polinomio cuadrático $f = aX^2 + bX + c$ tiene (al menos) una raíz en K. Podemos probar la recíproca también: que si f tiene una raíz en K, entonces Δ es un cuadrado en K:

En efecto, si $f = aX^2 + bX + c$ tiene una raíz $x_1 \in K$, $X - x_1 \mid f$ y el cociente, que tiene grado 1, se puede escribir en la forma $a(X - x_2)$. Por lo tanto

$$f = a(X - x_1)(X - x_2) = aX^2 - a(x_1 + x_2)X + ax_1x_2.$$

Igualando coeficiente a coeficiente, resulta que $b = -a(x_1 + x_2)$ y $c = ax_1x_2$. Por lo tanto,

$$\begin{aligned} \Delta = b^2 - 4ac &= a^2(x_1 + x_2)^2 - 4a^2x_1x_2 \\ &= a^2(x_1^2 + x_2^2 - 2x_1x_2) = \big(a(x_1 - x_2)\big)^2 = \omega^2 \end{aligned}$$

donde $\omega = a(x_1 - x_2) \in K$: Δ resulta ser un cuadrado en K!

Hemos probado el siguiente resultado:

Proposición 7.3.1. (Polinomios cuadráticos en $K[X]$.)

Sea K un cuerpo y sea $f = aX^2+bX+c \in K[X]$, con $a \neq 0$, un polinomio cuadrático. Entonces f es reducible en $K[X]$ si y solo si f tiene una raíz en K.

Si $2 \neq 0$ en K, f es reducible en $K[X]$ (o equivalentemente tiene raíz en K) si y solo si $\Delta = b^2 - 4ac$ es un cuadrado en K. En ese caso, sea $\omega \in K$ tal que $\omega^2 = \Delta$. Entonces las raíces de f en K son

$$x_\pm = \frac{-b \pm \omega}{2a}$$

(donde si $\Delta = 0$, $x_+ = x_-$), y $f = a(X - x_+)(X - x_-)$ es la factorización de f en $K[X]$.

<u>*Ejemplos:*</u> Sea $f = aX^2 + bX + c \in K[X]$, con $a \neq 0$, un polinomio cuadrático.

- Cuando $K = \mathbb{C}$, sabemos que siempre existe $\omega \in \mathbb{C}$ tal que $\omega^2 = \Delta \in \mathbb{C}$ (pues todo número complejo tiene raíz cuadrada), luego todo polinomio de grado 2 es reducible en $\mathbb{C}[X]$, o equivalentemente tiene dos raíces en $\mathbb{C}$ (que pueden ser distintas o la misma repetida dos veces cuando $\Delta = 0$).

  Por ejemplo si $f = X^2 - iX + (-1 + i)$, entonces $\Delta = 3 - 4i = \omega^2$ con $\omega = 2 - i$. Se obtiene

  $$x_+ = \frac{i + (2 - i)}{2} = 1 \quad \text{y} \quad x_- = \frac{i - (2 - i)}{2} = -1 + i.$$

  La factorización de f en polinomios irreducibles en $\mathbb{C}[X]$ es

  $$f = (X - x_+)(X - x_-) = (X - 1)(X - (-1 + i)).$$

- Cuando $K = \mathbb{R}$, existe $\omega \in \mathbb{R}$ tal que $\omega^2 = \Delta$ si y sólo si $\Delta \geq 0$. Por lo tanto, f es reducible en $\mathbb{R}[X]$ si y solo si $\Delta \geq 0$. Los polinomios cuadráticos tales que $\Delta < 0$ son irreducibles en $\mathbb{R}[X]$, como por ejemplo los polinomios de la forma $X^2 + c$ con $c \in \mathbb{R}$ positivo, y los que son tales que $\Delta \geq 0$ son reducibles en $\mathbb{R}[X]$, o equivalentemente en este caso tienen dos raíces reales contadas con multiplicidad.

- Cuando $K = \mathbb{Q}$, f es reducible en $\mathbb{Q}[X]$ (o tiene raíz en $\mathbb{Q}$) si y solo si Δ es un cuadrado en $\mathbb{Q}$. Existen luego polinomios de grado 2 irreducibles en $\mathbb{Q}[X]$ (o equivalentemente en este caso sin raíces racionales), como por ejemplo los polinomios de la forma $X^2 + c$ con $c > 0$, o también $X^2 - 2$.

- Cuando $K = \mathbb{Z}/p\mathbb{Z}$ con p primo $\neq 2$, f puede ser reducible o no según si Δ es un cuadrado o no en $\mathbb{Z}/p\mathbb{Z}$. Por ejemplo el polinomio $f = X^2 + \overline{2}X + \overline{5}$ es irreducible en $\mathbb{Z}/7\mathbb{Z}$ pues $\Delta = \overline{2}^2 - 4 \cdot \overline{5} = \overline{4 - 20} = \overline{-16} = \overline{5}$ no es un cuadrado en $\mathbb{Z}/7\mathbb{Z}$, mientras que el polinomio $X^2 + X + \overline{1}$ es reducible pues $\Delta = \overline{1}^2 - 4 \cdot \overline{1} = \overline{-3} = \overline{4} = \overline{2}^2$ es un cuadrado en $\mathbb{Z}/7\mathbb{Z}$ (aquí $\omega = \overline{2}$): se tiene

$$x_+ = \frac{-\overline{1} + \overline{2}}{2} = \frac{\overline{1}}{2} = \overline{4} \quad \text{y} \quad x_- = \frac{-\overline{1} - \overline{2}}{2} = \frac{\overline{-3}}{2} = \frac{\overline{4}}{2} = \overline{2},$$

y por lo tanto $f = (X - x_+)(X - x_-) = (X - \overline{4})(X - \overline{2})$ es la factorización de f en $\mathbb{Z}/7\mathbb{Z}$.

- Cuando $K = \mathbb{Z}/2\mathbb{Z}$, hay pocos polinomios de grado 2. Estos son $f_1 = X^2$, $f_2 = X^2 + \overline{1}$, $f_3 = X^2 + X$ y $f_4 = X^2 + X + \overline{1}$. Se puede ver que los tres primeros son reducibles (por ejemplo $f_2 = (X - \overline{1})^2$) mientras que el último no lo es, pues ni $\overline{0}$ ni $\overline{1}$ son raíces de f_4. (Sin embargo $\Delta = \overline{1} - 4 \cdot \overline{1} = \overline{1}$ es un cuadrado en $\mathbb{Z}/2\mathbb{Z}$.)

7.3.2 Polinomios en $\mathbb{C}[X]$ y el Teorema Fundamental del Álgebra.

Acabamos de ver que todo polinomio cuadrático $f = aX^2 + bX + c \in \mathbb{C}[X]$, con $a \neq 0$, tiene exactamente 2 raíces en $\mathbb{C}$ (contadas con multiplicidad), que son

$$z_\pm = \frac{-b \pm \omega}{2a} \quad \text{donde } \omega \in \mathbb{C} \text{ es tal que } \omega^2 = b^2 - 4ac,$$

y por lo tanto el polinomio f se factoriza en $\mathbb{C}[X]$ en la forma

$$f = (X - z_+)(X - z_-).$$

También podemos deducir inmediatamente de nuestro estudio sobre las raíces n-ésimas de números complejos en el capítulo anterior que todo polinomio de la forma $X^n - z$ en $\mathbb{C}[X]$ tiene exactamente n raíces en $\mathbb{C}$ (contadas con multiplicidad):

- Si $z = 0$, el polinomio es X^n que tiene la raíz 0 con multiplicidad n.
- Si $z \neq 0$, determinar las raíces de $X^n - z$ equivale a hallar los $\omega \in \mathbb{C}$ tales que $\omega^n - z = 0$, es decir hallar los $\omega \in \mathbb{C}$ tales que $\omega^n = z$, o sea determinar las raíces n-ésimas de z. Sabemos que $z \neq 0$ tiene n raíces n-ésimas distintas en $\mathbb{C}$, que son $\omega_0, \omega_1, \ldots, \omega_{n-1}$ descritas en el capítulo anterior. Por lo tanto estas n raíces son simples (ya que el

polinomio tiene a lo sumo n raíces contadas con multiplicidad), y el polinomio $X^n - z$ se factoriza en $\mathbb{C}[X]$ en la forma

$$X^n - z = (X - \omega_0) \cdots (X - \omega_{n-1}).$$

De hecho vale un resultado general al respecto, conocido como el Teorema Fundamental del Álgebra: todo polinomio no constante en $\mathbb{C}[X]$ tiene (al menos) una raíz en $\mathbb{C}$, o, lo que es equivalente aplicando divisiones sucesivas, todo polinomio de grado $n \geq 1$ en $\mathbb{C}[X]$ tiene exactamente n raíces contadas con multiplicidad! (Se dice que $\mathbb{C}$ es *algebraicamente cerrado*.)

Teorema 7.3.2. (Teorema Fundamental del Álgebra.)

Sea $f \in \mathbb{C}[X]$ un polinomio no constante. Entonces existe $z \in \mathbb{C}$ tal que $f(z) = 0$.

Equivalentemente, todo polinomio no constante en $\mathbb{C}[X]$ de grado n tiene exactamente n raíces contadas con multiplicidad en $\mathbb{C}$.

El Teorema Fundamental del Álgebra es equivalente a que los únicos polinomios irreducibles en $\mathbb{C}[X]$ son los de grado 1, de lo cual se deduce la factorización de polinomios en $\mathbb{C}[X]$.

Teorema 7.3.3. (Irreducibles y factorización en $\mathbb{C}[X]$.)

- *Sea $f \in \mathbb{C}[X]$. Entonces f es irreducible en $\mathbb{C}[X]$ si y solo si $\operatorname{gr}(f) = 1$, es decir $f = aX + b \in \mathbb{C}[X]$ con $a \neq 0$.*
- *Sea $f \in \mathbb{C}[X] - \mathbb{C}$. Entonces la factorización en irreducibles de f en $\mathbb{C}[X]$ es de la forma*

  $$f = c\,(X - z_1)^{m_1} \cdots (X - z_r)^{m_r}$$

  donde $z_1, \ldots, z_r \in \mathbb{C}$ son distintos, $m_1, \ldots, m_r \in \mathbb{N}$ y $c \in \mathbb{C}^\times$.

El Teorema Fundamental del Álgebra, que enunciamos en este curso sin demostración (se ven varias demostraciones en nuestra licenciatura en Matemática, pero hacen falta más herramientas que las que disponemos a este nivel) fue enunciado y demostrado en varias etapas a lo largo del tiempo, empezando con el matemático francés Albert Girard quién lo enunció en alguna forma en 1629. Una primera demostración, incompleta, fue esbozada por Jean le Rond D'Alembert en 1746. Aparecieron luego muchas demostraciones entre 1749 y 1795, pero con "agujeros" (argumentos no claros, que necesitan una demostración en sí mismo) ya que todas asumían que las raíces existen en "algún lado". Gauss también presentó una demostración con un agujero en 1799. En 1814, el librero y matemático amateur de origen suizo Jean-Robert Argand publicó la primera demostración completa, y

luego Gauss presentó otra en 1816. Existen hoy en día numerosas demostraciones distintas de este teorema, aunque todas ellas usan algún ingrediente indispensable de la rama de la matemática que se suele llamar *Análisis*, la completitud de los números reales en una u otra forma (como por ejemplo el Teorema de Bolzano, que establece que toda función continua en $\mathbb{R}$ que toma un valor positivo y un valor negativo obligatoriamente toma el valor 0).

Ejemplos: (para información nomás)

- f de grado 3: (Scipione del Ferro 1515?, Tartaglia 1535, Cardano 1545.)

$$f = aX^3 + bX^2 + cX + d \ \in \mathbb{C}[X], \quad a \neq 0.$$

Haciendo el cambio de variables $Y = X - \dfrac{b}{3a}$, el problema se traduce en buscar las raíces del polinomio :

$$g = Y^3 + pY + q.$$

Buscando las soluciones de la forma $y = u + v$, con $u^3 + v^3 = -q$ y $u^3v^3 = -\dfrac{p^3}{27}$, se observa que u^3 y v^3 son las raíces del polinomio (*resolvente*):

$$Z^2 + qZ - \frac{p^3}{27}.$$

Por lo tanto hay 3 posibilidades para u y 3 posibilidades para v, o sea 6 posibilidades para $y = u + v$: las 3 raíces y del polinomio son 3 de entre esas 6 posibilidades, las 3 que son dadas por las elecciones de u y v que satisfacen $u\,v = -p/3$.

Pero puede ocurrir que calcular las raíces de un polinomio de esa forma puede dar una expresión muy engorrosa para algo mucho más sencillo! Por ejemplo la raíz $x = 1$ del polinomio X^3+X-2 aparece expresada en la forma

$$1 = \sqrt[3]{1 + \frac{2}{9}\sqrt{21}} + \sqrt[3]{1 - \frac{2}{9}\sqrt{21}}.$$

- f de grado 4: (Ludovico Ferrari, 1540?)

$$f = X^4 + pX^2 + qX + r.$$

Las 4 raíces son del tipo $\alpha = \frac{1}{2}(\pm u \pm v \pm \omega)$, donde $-u^2$, $-v^2$, $-\omega^2$ son las tres raíces del polinomio *resolvente*:

$$Z^3 - 2pZ^2 + (p^2 - 4r)Z + q^2.$$

La condición aquí para determinar las 4 raíces complejas entre las 8 posibles expresiones es $(\pm u)(\pm v)(\pm \omega) = -q$.

Hasta ahora se obtuvieron las raíces complejas de polinomios $f \in \mathbb{C}[X]$ de grado ≤ 4, por medio de fórmulas que se obtienen a partir de los coeficientes del polinomio f mediante las operaciones $+$, $-$, $\cdot$, $/$ y extracción de raíces cuadradas y cúbicas.

La pregunta natural es entonces : ¿Existirá para cada polinomio f de grado arbitrario una fórmula para las raíces que involucre los coeficientes de f y las operaciones $+$, $-$, $\cdot$, $/$ y extracción de raíces n-ésimas para algunos n adecuados?

Durante más de 200 años, muchos matemáticos buscaron esas fórmulas. Pero a principios del S. XIX el joven matemático noruego Niels Abel, 1802-1829, probó que sorprendentemente la respuesta es NO:

Teorema 7.3.4. (Abel, 1824?)

No existe ninguna fórmula que describa las raíces (complejas) de un polinomio general cualquiera $f \in \mathbb{C}[X]$ de grado ≥ 5 a partir de sus coeficientes y de las operaciones elementales $+$, $-$, $\cdot$, $/$ y extracciones de raíces n-ésimas.

El aún más joven matemático francés Evariste Galois, 1811-1832, caracterizó en 1832, la noche antes de morir, al batirse en duelo, cuáles son los polinomios de grado ≥ 5 para los cuales existe tal fórmula (aunque no es fácilmente deducible de los coeficientes del polinomio, sino que tiene que ver con cierto grupo asociado a él).

Esto es parte de la hoy llamada Teoría de Galois, que además de su importancia en matemática, constituye también la base del funcionamiento de sistemas de navegación satelital como el GPS por ejemplo. Sus resultados fueron entendidos recién en 1846 por el matemático francés Joseph Liouville, 1809-1882.

Tanto Abel como Galois fueron los iniciadores de la Teoría de Grupos.

7.3.3 Polinomios en $\mathbb{R}[X]$.

Sabemos que un polinomio en $\mathbb{R}[X]$ de grado $n \geq 1$ tiene a lo sumo n raíces contadas con multiplicidad. También sabemos que si $f \in \mathbb{R}[X]$ tiene grado

≥ 2 y tiene una raíz $x \in \mathbb{R}$, entonces f es reducible en $\mathbb{R}[X]$ pues $X-x \mid f$ ($X-x$ es un factor no trivial de f en $\mathbb{R}[X]$). Pero ser reducible en $\mathbb{R}[X]$ no implica tener raíz en $\mathbb{R}$: existen polinomios reducibles en $\mathbb{R}[X]$ de cualquier grado (par) que no tienen raíces reales, como por ejemplo el polinomio $(X^2+1)^n$, $\forall\, n \geq 2$. Sin embargo no existen polinomios irreducibles en $\mathbb{R}[X]$ de cualquier grado. Es lo que estudiaremos a continuación, gracias al estudio ya realizado de los polinomios en $\mathbb{C}[X]$.

Primeramente volvamos a mencionar la consecuencia siguiente del famoso Teorema de Bolzano, probado en 1817 por el matemático bohemio Bernard Bolzano, 1781-1848.

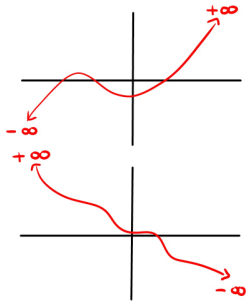
Proposición 7.3.5. (Polinomios reales de grado impar.)

Sea $f \in \mathbb{R}[X]$ de grado impar. *Entonces f tiene al menos una raíz en $\mathbb{R}$.*

Demostración. Sea $f = a^n X^n + \cdots + a_0 \in \mathbb{R}[X]$, con n impar.

Si $a_n > 0$, entonces :

$$\lim_{x\to+\infty} f(x) = +\infty \quad \text{y} \quad \lim_{x\to-\infty} f(x) = -\infty :$$



Y si $a_n < 0$ se tiene :

$$\lim_{x\to+\infty} f(x) = -\infty \quad \text{y} \quad \lim_{x\to-\infty} f(x) = +\infty :$$

En ambos casos los signos son opuestos, y por lo tanto, por el Teorema de Bolzano (y dado que $f : \mathbb{R} \to \mathbb{R}$ define una función continua), debe existir $x \in \mathbb{R}$ tal que $f(x) = 0$. □

Pero se puede ser más explícito y precisar un poco más cuántas raíces reales puede tener f.

Proposición 7.3.6. (Raíces complejas conjugadas de polinomios reales.)

Sea $f \in \mathbb{R}[X]$, y sea $z \in \mathbb{C} - \mathbb{R}$ un número complejo no real. Entonces

1. $f(z) = 0 \iff f(\overline{z}) = 0$.
2. *Para todo* $m \in \mathbb{N}$, $\text{mult}(z; f) = m \iff \text{mult}(\overline{z}; f) = m$.
3. $(X - z)(X - \overline{z})$ *es un polinomio irreducible de* $\mathbb{R}[X]$.
4. $f(z) = 0 \implies (X - z)(X - \overline{z}) \mid f$ *en* $\mathbb{R}[X]$.

5. $\text{mult}(z;f) = m \implies \big((X-z)(X-\overline{z})\big)^m \mid f$ *en* $\mathbb{R}[X]$.

Demostración. 1. Sea $f = a_nX^n + \cdots + a_0 \in \mathbb{R}[X]$. Entonces

$$\begin{aligned} f(z) = 0 &\iff a_nz^n + \cdots + a_1z + a_0 = 0 \\ &\iff \overline{a_nz^n + \cdots + a_1z + a_0} = 0 \\ &\iff \overline{a_n}\,\overline{z}^n + \cdots + \overline{a_1}\,\overline{z} + \overline{a_0} = 0 \\ &\iff a_n\overline{z}^n + \cdots + a_1\overline{z} + a_0 = 0 \quad \text{pues } a_0,\ldots,a_n \in \mathbb{R} \\ &\iff f(\overline{z}) = 0 \end{aligned}$$

2. Por la Proposición 7.2.11,

$$\text{mult}(z;f) = m \iff f(z) = f'(z) = \cdots = f^{(m-1)}(z) = 0, f^{(m)}(z) \neq 0.$$

Pero $f', \ldots, f^{(m-1)}$, $f^{(m)}$ también son polinomios en $\mathbb{R}[X]$. Por lo tanto, por (1):

$$\begin{aligned} f(z) = \cdots = f^{(m-1)}(z) = 0, f^{(m)}(z) \neq 0 &\iff f(\overline{z}) = \cdots = f^{(m-1)}(\overline{z}) = 0, f^{(m)}(\overline{z}) \neq 0 \\ &\iff \text{mult}(\overline{z};f) = m. \end{aligned}$$

3. $(X-z)(X-\overline{z}) = X^2 - 2\,\Re e(z) + |z|^2 \in \mathbb{R}[X]$ pues sus coeficientes pertenecen a $\mathbb{R}$, y es irreducible por ser de grado 2 y no tener raíces reales.

4. $f(z) = 0 \Rightarrow f(\overline{z}) = 0$, por lo tanto $X - z \mid f$ y $X - \overline{z} \mid f$ en $\mathbb{C}[X]$. Luego, como son polinomios coprimos, su producto $(X-z)(X-\overline{z}) \mid f$ en $\mathbb{C}[X]$. Pero al ser $f \in \mathbb{R}[X]$ y $(X-z)(X-\overline{z}) \in \mathbb{R}[X]$, se concluye que $(X-z)(X-\overline{z}) \mid f$ en $\mathbb{R}[X]$.

5. Por inducción en $m \geq 1$. El caso base es el inciso anterior. Sea entonces $m > 1$ y sea $z \in \mathbb{C} - \mathbb{R}$ raíz de f de multiplicidad m. Entonces $(X-z)(X-\overline{z}) \mid f \in \mathbb{R}[X]$ y consideremos el cociente $q := \dfrac{f}{(X-z)(X-\overline{z})} \in \mathbb{R}[X]$. Se tiene que $\text{mult}(z;q) = m-1$ y por lo tanto, por hipótesis inductiva, $\big((X-z)(X-\overline{z})\big)^{m-1} \mid q$ en $\mathbb{R}[X]$. Es decir, $\big((X-z)(X-\overline{z})\big)^m \mid f$ en $\mathbb{R}[X]$.

□

La proposición anterior significa que las raíces complejas no reales de un polinomio real f vienen de a pares de complejos conjugados, o sea que un

polinomio real f de grado n, que tiene exactamente n raíces complejas contadas con multiplicidad, tiene un número par de ellas que son complejas no reales, y las restantes automáticamente tienen que ser reales. Por ejemplo, un polinomio real de grado impar tiene un número impar de raíces reales. Más aún, existen algoritmos que calculan la cantidad exacta de raíces reales que tiene un polinomio en $\mathbb{R}[X]$ (como por ejemplo el Algoritmo de Sturm), pero no los vamos a ver aquí. A continuación caracterizamos los polinomios irreducibles de $\mathbb{R}[X]$ y como es la factorización de polinomios en $\mathbb{R}[X]$.

Proposición 7.3.7. (Polinomios irreducibles en $\mathbb{R}[X]$.)

Los polinomios irreducibles en $\mathbb{R}[X]$ son exactamente los siguientes:

- *Los de grado 1, o sea de la forma $aX + b \in \mathbb{R}[X]$ con $a \neq 0$.*
- *Los de grado 2 con discriminante negativo, o sea de la forma*

$$aX^2 + bX + c \in \mathbb{R}[X] \quad con \quad a \neq 0 \quad y \quad \Delta := b^2 - 4ac < 0.$$

Demostración. Claramente los polinomios de grado 1 y los de grado 2 con discriminante negativo son irreducibles. Probemos que son los únicos.

- Si f tiene grado impar > 1, entonces tiene por lo menos una raíz real y por lo tanto es reducible.
- Si f es de grado 2, sabemos que es reducible si y solo si tiene discriminante ≥ 0.
- Si f tiene grado par ≥ 4, o bien tiene alguna raíz real, y en tal caso es reducible, o bien todas sus raíces son complejas no reales y vienen de a pares conjugados. Por lo tanto si z es una de esas raíces, el polinomio real $(X - z)(X - \overline{z})$ divide a f en $\mathbb{R}[X]$, y f resulta ser reducible.

□

Teorema 7.3.8. (Factorización en $\mathbb{R}[X]$.)

Sea $f \in \mathbb{R}[X] - \mathbb{R}$. Entonces la factorización en irreducibles de f en $\mathbb{R}[X]$ es de la forma

$$f = c\,(X - x_1)^{m_1} \dots (X - x_r)^{m_r} (X^2 + b_1 X + c_1)^{n_1} \dots (X^2 + b_s X + c_s)^{n_s}$$

donde $c \in \mathbb{R}^\times$, $r, s \in \mathbb{N}_0$, $m_i, n_j \in \mathbb{N}$ para $1 \leq i \leq r, 1 \leq j \leq s$, $x_1, \dots, x_r \in \mathbb{R}$, $b_1, c_1, \dots, b_s, c_s \in \mathbb{R}$ y $\Delta_j := {b_j}^2 - 4c_j < 0$.

Ejemplo: Factorizar en $\mathbb{R}[X]$ y $\mathbb{C}[X]$ el polinomio $f = X^4 - 2X^3 + X^2 - 4X - 2$ sabiendo que $\sqrt{2}\,i$ es raíz de f:

Como $f \in \mathbb{R}[X]$, por la Proposición 7.3.6, se tiene que $f(\sqrt{2}\,i) = 0 \Leftrightarrow f(-\sqrt{2}\,i) = 0$. Por lo tanto $(X - \sqrt{2}\,i)(X + \sqrt{2}\,i) = X^2 + 2 \mid f$. En efecto, $f = (X^2+2)(X^2 - 2X - 1)$. Las raíces de $X^2 - 2X - 1$ son reales: $1 + \sqrt{2}$ y $1 - \sqrt{2}$. Por lo tanto,

- $f = (X - \sqrt{2}\,i)(X + \sqrt{2}\,i)(X - (1+\sqrt{2}))(X - (1-\sqrt{2}))$ es la factorización de f en $\mathbb{C}[X]$

- $f = (X^2 + 2)(X - (1 + \sqrt{2}))(X - (1 - \sqrt{2}))$ es la factorización de f en $\mathbb{R}[X]$.

7.3.4 Polinomios en $\mathbb{Q}[X]$.

Sabemos que un polinomio en $\mathbb{Q}[X]$ de grado $n \geq 1$ tiene a lo sumo n raíces contadas con multiplicidad. También sabemos que si $f \in \mathbb{Q}[X]$ tiene grado ≥ 2 y tiene una raíz $x \in \mathbb{Q}$, entonces f es reducible en $\mathbb{Q}[X]$ pues $X - x \mid f$ (lo que implica $X - x$ es un factor no trivial de f en $\mathbb{Q}[X]$). Pero ser reducible en $\mathbb{Q}[X]$ no implica tener raíz en $\mathbb{Q}$: existen polinomios reducibles en $\mathbb{Q}[X]$ de cualquier grado que no tienen raíces racionales, como por ejemplo los polinomios $(X^2 - 2)^n$, $\forall\, n \geq 2$ y $(X^2 - 2)(X^3 - 2)$.

Sin embargo la situación no es como en $\mathbb{R}[X]$ donde no existen polinomios irreducibles de grado impar: en $\mathbb{Q}[X]$ se puede probar que existen polinomios irreducibles de cualquier grado, como por ejemplo el polinomio $X^n - 2$, $\forall\, n \in \mathbb{N}$: no sólo el polinomio $X^n - 2$ no tiene raíces en $\mathbb{Q}$ para todo $n \geq 2$, pero más aún no tiene ningún factor en $\mathbb{Q}[X]$ de cualquier grado d, $1 \leq d \leq n - 1$. También se puede probar que para p primo, el polinomio $X^{p-1} + \cdots + X + 1$ es irreducible en $\mathbb{Q}[X]$.

La situación parece desesperada. Pero al menos en $\mathbb{Q}$ existen algoritmos para encontrar (en forma exacta) todas las raíces racionales, como por ejemplo el algoritmo de Gauss, y más aún, también para decidir si el polinomio es irreducible o no en $\mathbb{Q}[X]$, y en caso de ser reducible, determinar su factorización en irreducibles de $\mathbb{Q}[X]$!

Una herramienta que puede ser útil si se tiene más información sobre el polinomio es la proposición siguiente que ayuda a determinar factores irreducibles cuadráticos de un polinomio cuando tiene una raíz real de la forma $a + b\sqrt{d}$ con $d \in \mathbb{Q}$ tal que $\sqrt{d} \notin \mathbb{Q}$:

Proposición 7.3.9. (Raíces de la forma $a + b\sqrt{d}$ de polinomios racionales.)

Sea $d \in \mathbb{Q}$ tal que $\sqrt{d} \notin \mathbb{Q}$, y sean $a, b \in \mathbb{Q}$ con $b \neq 0$. Sea $f \in \mathbb{Q}[X]$. Entonces

1. $g := \big(X - (a + b\sqrt{d})\big)\big(X - (a - b\sqrt{d})\big)$ *es un polinomio irreducible de* $\mathbb{Q}[X]$,
2. $f(a + b\sqrt{d}) = 0 \implies g \mid f$ *en* $\mathbb{Q}[X]$,
3. $f(a + b\sqrt{d}) = 0 \iff f(a - b\sqrt{d}) = 0$,
4. *Para todo* $m \in \mathbb{N}$, $\text{mult}(a + b\sqrt{d}; f) = m \Leftrightarrow \text{mult}(a - b\sqrt{d}; f) = m$.

Demostración. 1. Haciendo la cuenta,

$$g := \big(X - (a + b\sqrt{d})\big)\big(X - (a - b\sqrt{d})\big) = X^2 - 2aX + a^2 - b^2 d \in \mathbb{Q}[X]$$

porque todos sus coeficientes pertenecen a $\mathbb{Q}$, y es irreducible por ser de grado 2 y no tener raíz en $\mathbb{Q}$.

2. Dividamos a $f \in \mathbb{Q}[X]$ por el polinomio $g \in \mathbb{Q}[X]$:

$$g = q\,g + r \quad \text{con} \quad r = 0 \quad \text{o} \quad \text{gr}(r) < 2.$$

En todo caso se puede escribir en la forma $r = cX + e$ con $c, e \in \mathbb{Q}$. Ahora bien, como $a + b\sqrt{d}$ es raíz de f y de g, se obtiene que $a + b\sqrt{d}$ es raíz de r también. Es decir

$$\begin{aligned} 0 &= r(a + b\sqrt{d}) = c(a + b\sqrt{d}) + e = ca + e + cb\sqrt{d} \\ &\implies ca + e = -cb\sqrt{d}. \end{aligned}$$

Si fuera $c \neq 0$, como $b \neq 0$ se obtendría $\sqrt{d} = \dfrac{ca + e}{-cb} \in \mathbb{Q}$ lo que contradice la hipótesis $\sqrt{d} \notin \mathbb{Q}$. Por lo tanto $c = 0$, lo que implica también de la igualdad $0 = c(a + b\sqrt{d}) + e$ que $e = 0$. Se concluye que $r = cX + e$ es el polinomio nulo, y por lo tanto $g \mid f \in \mathbb{Q}[X]$.

3. Es una consecuencia directa del inciso anterior, ya que si $f(a + b\sqrt{d}) = 0$, entonces $g \mid f$ y por lo tanto $f(a - b\sqrt{d}) = 0$ también. La recíproca es análoga.

4. La misma multiplicidad se obtiene por inducción, aplicando la hipótesis inductiva al polinomio $f/g \in \mathbb{Q}[X]$ cuando $a + b\sqrt{d}$ es raíz de f.

□

Ejemplo: Factorizar en $\mathbb{C}[X]$, $\mathbb{R}[X]$ y $\mathbb{Q}[X]$ el polinomio $f = X^4 - X^3 - 2X^2 - 3X - 1$ sabiendo que tiene a $1 - \sqrt{2}$ como raíz.

Como $f \in \mathbb{Q}[X]$ y $1 - \sqrt{2}$ es raíz, también lo es $1 + \sqrt{2}$ y f es divisible por el polinomio $g = \big(X - (1 - \sqrt{2})\big)\big(X - (1 + \sqrt{2})\big) = X^2 - 2X - 1$. En efecto, al hacer la división se obtiene

$$f = (X^2 - 2X - 1)(X^2 + X + 1).$$

Ahora bien, las raíces de $X^2 + X + 1$ son las raíces cúbicas primitivas de la unidad, $\dfrac{-1 \pm \sqrt{3}i}{2}$, por lo tanto la factorización de f en $\mathbb{C}[X]$ es

$$f = \big(X - (1 - \sqrt{2})\big)\big(X - (1 + \sqrt{2})\big)\big(X - (\frac{-1 + \sqrt{3}}{2})\big)\big(X - (\frac{-1 - \sqrt{3}}{2})\big).$$

El polinomio X^2+X+1 es irreducible tanto en $\mathbb{R}[X]$ como en $\mathbb{Q}[X]$ al tener grado 2 y no tener raíces allí, y el polinomio $X^2 - 2X - 1$ es irreducible en $\mathbb{Q}[X]$ al tener grado 2 y no tener raíces en $\mathbb{Q}$. Por lo tanto la factorización de f en $\mathbb{R}[X]$ es

$$f = \big(X - (1 - \sqrt{2})\big)\big(X - (1 + \sqrt{2})\big)\big(X^2 + X + 1\big)$$

y la factorización de f en $\mathbb{Q}[X]$ es

$$\big(X^2 - 2X - 1\big)\big(X^2 + X + 1\big).$$

Con respecto a la factorización en general, en el caso de $\mathbb{Q}[X]$ no se puede decir nada más preciso que lo que ya dice el Teorema Fundamental de la Aritmética para polinomios:

Teorema 7.3.10. (Factorización en $\mathbb{Q}[X]$.)

Sea $f \in \mathbb{Q}[X] - \mathbb{Q}$. Entonces la factorización en irreducibles de f en $\mathbb{Q}[X]$ es de la forma

$$f = c\, g_1^{m_1} \dots g_r^{m_r}$$

donde $c \in \mathbb{Q}^\times$, $g_1, \dots, g_r$ son polinomios mónicos irreducibles distintos en $\mathbb{Q}[X]$ y $m_1, \dots, m_r \in \mathbb{N}$.

Notemos que cada factor irreducible $g_i \in \mathbb{Q}[X]$ cuando lo miremos como polinomio en $\mathbb{R}[X]$ o en $\mathbb{C}[X]$ va probablemente a dejar de ser irreducible para factorizarse como polinomios de grado 1 o 2 en el caso de $\mathbb{R}$, o todos de grado 1 en el caso de $\mathbb{C}$. En ese sentido la factorización de f en $\mathbb{R}[X]$ "refina" la factorización de f en $\mathbb{Q}[X]$, y la de f en $\mathbb{C}[X]$ la refina aún más.

Zassenhaus

Berlekamp

A. Lenstra

H. Lenstra

Lovasz

Por ejemplo el polinomio $f = X^4 - 2X^3 + X^2 - 4X - 2 \in \mathbb{Q}[X]$ que consideramos arriba se factoriza en $\mathbb{Q}[X]$ en la forma

$$f = (X^2 + 2)(X^2 - 2X - 1),$$

ya que ambos factores son irreducibles en $\mathbb{Q}[X]$ al no tener raíces en $\mathbb{Q}$ (por ser de grado 2).

Si bien no se sabe nada a priori sobre los factores irreducibles en $\mathbb{Q}[X]$ de un polinomio, en este caso existen algoritmos de factorización (exacta), contrariamente a lo que pasa en $\mathbb{C}[X]$ o $\mathbb{R}[X]$.

La historia de los algoritmos de factorización de polinomios en $\mathbb{Q}[X]$ comenzó con el astrónomo alemán Friedrich von Schubert en 1793, que presentó un algoritmo luego redescubierto por Leopold Kronecker en 1882 y y que se conoce hoy como el *Algoritmo de Kronecker*.

Para factorizar un polinomio en $\mathbb{Q}[X]$, dado que las constantes no influyen, alcanza con considerar el polinomio en $\mathbb{Z}[X]$ obtenido limpiando los denominadores comunes. Y en realidad se puede probar más: se puede probar que el problema de la factorización en $\mathbb{Q}[X]$ se reduce a encontrar factores con coeficientes enteros.

El algoritmo de Kronecker se basa en ese hecho, y en evaluación e interpolación de polinomios. Es muy sencillo teóricamente, aunque terriblemente costoso de implementar computacionalmente. Pero tiene la importante característica de indicar que existen algoritmos, y por lo tanto se pueden buscar algoritmos que funcionen mejor... Hubo posteriormente grandes mejoras en cuanto a la velocidad de los algoritmos de factorización en $\mathbb{Q}[X]$.

El primero de ellos, debido a Hans Zassenhaus, en 1969, se basa esencialmente en un algoritmo de Elwyn Berlekamp para factorizar rápidamente polinomios en cuerpos finitos, 1967. El algoritmo requiere en promedio un número de operaciones del orden de $\mathrm{gr}(f)^c$, donde c es una constante calculada, aunque en el peor de los casos puede necesitar un número exponencial en $\mathrm{gr}(f)$ operaciones como en el algoritmo de Kronecker mencionado más arriba.

El primer algoritmo polinomial para factorizar polinomios en $\mathbb{Q}[X]$, conoci-

do como algoritmo L^3, es debido a los hermanos holandeses Arjen Lenstra y Hendrik Lenstra y al húngaro László Lovász, en 1982. Establece exactamente lo siguiente :

Teorema 7.3.11. **(L^3.)**

Sea $f = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ un polinomio que satisface que sus coeficientes (enteros) no tienen ningún factor común no trivial en $\mathbb{Z}$. Sea H una cota superior para los módulos de los coeficientes $a_i \in \mathbb{Z}$. Entonces, se puede factorizar f en $\mathbb{Q}[X]$ realizando del orden de $n^{12} + n^9(\log_2 H)^3$ operaciones "bit" (es decir los números se representan en base 2, y se cuenta una operación cada vez que se suma, resta, multiplica o divide un bit "0" ó "1").

Este es el primer algoritmo *polinomial* que existe para factorizar en $\mathbb{Q}[X]$ polinomios racionales, donde polinomial significa que si el polinomio de entrada se mide a través de su grado n y del tamaño de sus coeficientes en representación binaria $\log_2 H$, la cantidad total de operaciones binarias que realiza el algoritmo está acotado por $(n \cdot \log_2 H)^c$ para algún $c \in \mathbb{N}$ calculado, y no del tipo 2^n como lo era hasta entonces.

El algoritmo utilizado hoy en día por la mayoría de los sistemas de álgebra computacional es un algoritmo más moderno, debido principalmente a Mark van Hoeij (que trabaja en él desde el 2002, y logró varias mejoras teóricas y prácticas): tiene la ventaja de ser polinomial en teoría y también eficiente en la práctica.

La descripción y la demostración de los algoritmos de Zassenhaus-Berlekamp, L^3 y van Hoeij quedan fuera de nuestro alcance, y utilizan fundamentalmente en el primer caso la reducción a factorizar polinomios módulo p para p primo, en el segundo caso la teoría de látices o reticulados en $\mathbb{Z}^n$, y en el último una combinación de ambos.

7.4 Ejercicios.

Generalidades.

1. Calcular el grado y el coeficiente principal de los siguientes polinomios

   i) $(4X^6 - 2X^5 + 3X^2 - 2X + 7)^{77}$,

   ii) $(-3X^7 + 5X^3 + X^2 - X + 5)^4 - (6X^4 + 2X^3 + X - 2)^7$,

   iii) $(-3X^5 + X^4 - X + 5)^4 - 81X^{20} + 19X^{19}$.

2. Calcular el coeficiente de X^{20} de los siguientes polinomios

   i) $(X^{18}+X^{16}+1)(X^5+X^4+X^3+X^2+X+1)$ en $\mathbb{Q}[X]$ y en $(\mathbb{Z}/2\mathbb{Z})[X]$,

   ii) $(X-3\,i)^{133}$ en $\mathbb{C}[X]$,

   iii) $(X-1)^4(X+5)^{19}+X^{33}-5X^{20}+7$ en $\mathbb{Q}[X]$,

   iv) $f=X^{10}(X^5+4)^7$ en $(\mathbb{Z}/5\mathbb{Z})[X]$.

3. Hallar, cuando existan, todos los $f\in\mathbb{C}[X]$ tales que

   i) $f^2=Xf+X+1$

   ii) $f^2-Xf=-X^2+1$

   iii) $(X+1)f^2=X^6+Xf$

   iv) $f\neq 0$ y $f^3=\mathrm{gr}(f)\cdot X^2 f$

4. Hallar el cociente y el resto de la división de f por g en los casos

   i) $f=5X^4+2X^3-X+4$, $g=X^2+2$ en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$,

   ii) $f=4X^4+X^3-4$, $g=2X^2+1$ en $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ y $(\mathbb{Z}/7\mathbb{Z})[X]$,

   iii) $f=X^n-1$, $g=X-1$ en $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ y $(\mathbb{Z}/p\mathbb{Z})[X]$.

5. Determinar todos los $a\in\mathbb{C}$ tales que

   (a) X^3+2X^2+2X+1 sea divisible por X^2+aX+1,

   (b) $X^4-aX^3+2X^2+X+1$ sea divisible por X^2+X+1,

   (c) El resto de la división de $X^5-3X^3-X^2-2X+1$ por X^2+aX+1 sea $-8X+4$.

6. *Definición:* Sea K un cuerpo y sea $h\in K[X]$ un polinomio no nulo. Dados $f,g\in K[X]$, se dice que f es congruente a g módulo h si $h\mid f-g$. En tal caso se escribe $f\equiv g \pmod h$.

   i) Probar que $\equiv \pmod h$ es una relación de equivalencia en $K[X]$.

   ii) Probar que si $f_1\equiv g_1 \pmod h$ y $f_2\equiv g_2 \pmod h$ entonces $f_1+f_2\equiv g_1+g_2 \pmod h$ y $f_1\cdot f_2\equiv g_1\cdot g_2 \pmod h$.

   iii) Probar que si $f\equiv g \pmod h$ entonces $f^n\equiv g^n \pmod h$ para todo $n\in\mathbb{N}$.

   iv) Probar que r es el resto de la división de f por h si y sólo si $f\equiv r \pmod h$ y $r=0$ ó $\mathrm{gr}(r)<\mathrm{gr}(h)$.

7. Hallar el resto de la división de f por g para

   i) $f=X^{353}-X-1$ y $g=X^{31}-2$ en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$,

   ii) $f=X^{1000}+X^{40}+X^{20}+1$, $g=X^6+1$ en $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ y $(\mathbb{Z}/p\mathbb{Z})[X]$,

iii) $f = X^{200} - 3X^{101} + 2\,, \quad g = X^{100} - X + 1$ en $\mathbb{Q}[X]\,,\ \mathbb{R}[X]$ y $\mathbb{C}[X]\,.$

iv) $f = X^{3016} + 2X^{1833} - X^{174} + X^{137} + 2X^4 - X^3 + 1\,, \quad g = X^4 + X^3 + X^2 + X + 1$ en $\mathbb{Q}[X]\,,\ \mathbb{R}[X]$ y $\mathbb{C}[X]\,.$ (Sug: ver Ej. 4)iii)).

8. Sea K un cuerpo. Sea $n \in \mathbb{N}$, sea $a \in K\,.$

i) Probar que $X - a \mid X^n - a^n$ en $K[X]\,.$

ii) Probar que si n es impar entonces $X + a \mid X^n + a^n$ en $K[X]\,.$

iii) Probar que si n par entonces $X + a \mid X^n - a^n$ en $K[X]\,.$

Calcular los cocientes en cada caso.

9. Calcular el máximo común divisor entre f y g y escribirlo como combinación lineal de f y g siendo

i) $f = X^5 + X^3 - 6X^2 + 2X + 2\,, \quad g = X^4 - X^3 - X^2 + 1\,,$

ii) $f = X^6 + X^4 + X^2 + 1\,, \quad g = X^3 + X\,,$

iii) $f = X^5 + X^4 - X^3 + 2X - 3\,, \quad g = X^4 + 2X + 1\,.$

¿Cambia algo si se consideran los polinomios en $\mathbb{R}[X]$ o $\mathbb{C}[X]$?

Evaluación y raíces.

10. Sea $f \in \mathbb{Q}[X]$ tal que $f(1) = -2\,,\ f(2) = 1$ y $f(-1) = 0\,.$ Hallar el resto de la división de f por $X^3 - 2X^2 - X + 2\,.$

11. Sea $n \in \mathbb{N}\,,\ n \geq 3\,.$ Hallar el resto de la división de $X^{2n} + 3X^{n+1} + 3X^n - 5X^2 + 2X + 1$ por $X^3 - X$ en $\mathbb{Q}[X]\,.$

12. Hallar la forma binomial de cada una de las raíces complejas del polinomio $X^6 + X^3 - 2\,.$

13. Sea $\omega = e^{\frac{2\pi}{7}i}\,.$ Probar que $\omega + \omega^2 + \omega^4$ es raíz del polinomio $X^2 + X + 2\,.$

14. i) Probar que si $\omega = e^{\frac{2\pi}{5}i} \in G_5\,,$ entonces

$$X^2 + X - 1 = \big(X - (\omega + \omega^{-1})\big)\,\big(X - (\omega^2 + \omega^{-2})\big).$$

ii) Calcular, justificando cuidadosamente, el valor exacto de $\cos\left(\frac{2\pi}{5}\right)\,.$

15. i) Sean $f, g \in \mathbb{C}[X]$ y sea $a \in \mathbb{C}\,.$ Probar que a es raíz de f y de g si y sólo si a es raíz de $(f : g)\,.$

ii) Hallar todas las raíces complejas de $X^4 + 3X - 2$ sabiendo que tiene una raíz común con $X^4 + 3X^3 - 3X + 1\,.$

16. Determinar la multiplicidad de a como raíz de f en los casos

    i) $f = X^5 - 2X^3 + X\,, \quad a = 1\,,$

    ii) $f = X^6 - 3X^4 + 4\,, \quad a = i\,,$

    iii) $f = (X-2)^2(X^2-4) + (X-2)^3(X-1)\,, \quad a = 2\,,$

    iv) $f = (X-2)^2(X^2-4) - 4(X-2)^3\,, \quad a = 2\,.$

17. Sea $n \in \mathbb{N}$. Determinar todos los $a \in \mathbb{C}$ tales que $f = nX^{n+1} - (n+1)X^n + a$ tiene sólo raíces simples en $\mathbb{C}$.

18. Determinar todos los $a \in \mathbb{R}$ para los cuales $f = X^{2n+1} - (2n+1)X + a$ tiene al menos una raíz múltiple en $\mathbb{C}$.

19. Sea $f = X^{20} + 8X^{10} + 2a$. Determinar todos los valores de $a \in \mathbb{C}$ para los cuales f admite una raíz múltiple en $\mathbb{C}$. Para cada valor hallado determinar cuántas raíces distintas tiene f y la multiplicidad de cada una de ellas.

20. Sea $f = X^{68} - 17X^4 - 16 \in \mathbb{C}[X]$. Determinar la forma binomial de cada raíz *múltiple* de f en $\mathbb{C}$ y la multiplicidad de cada una de ellas.

21. i) Probar que para todo $a \in \mathbb{C}$, el polinomio $f = X^6 - 2X^5 + (1+a)X^4 - 2aX^3 + (1+a)X^2 - 2X + 1$ es divisible por $(X-1)^2$.

    ii) Determinar todos los $a \in \mathbb{C}$ para los cuales f es divisible por $(X-1)^3$.

22. Determinar todos los $a \in \mathbb{C}$ tales que 1 sea raíz *doble* de $X^4 - aX^3 - 3X^2 + (2+3a)X - 2a$.

23. Sea $n \in \mathbb{N}$. Probar que $\displaystyle\sum_{k=0}^{n} \frac{X^k}{k!}$ tiene todas sus raíces (complejas) simples.

24. Sea $(f_n)_{n\in\mathbb{N}}$ la sucesión de polinomios definida por

$$f_1 = X^4 + 2X^2 + 1 \quad \text{y} \quad f_{n+1} = (X-i)(f_n + f_n'),\ \forall\, n \in \mathbb{N}.$$

    Probar que i es raíz *doble* de f_n para todo $n \in \mathbb{N}$.

25. Sea $(f_n)_{n\in\mathbb{N}}$ la sucesión de polinomios definida por

$$f_1 = X^3 + 2X - 1 \quad \text{y} \quad f_{n+1} = Xf_n^2 + X^2 f_n',\ \forall\, n \in \mathbb{N}.$$

    Probar que $\operatorname{gr}(f_n) = 2^{n+1} - 1$ para todo $n \in \mathbb{N}$.

26. Sea $\alpha \in \mathbb{C}$ raíz de multiplicidad 3 de $f \in \mathbb{C}[X]$. Probar que el resto de dividir a f' por $(X-\alpha)^3$ es $a(X-\alpha)^2$, con $a \in \mathbb{C}$, $a \neq 0$.

27. i) Hallar todas las raíces racionales de
    (a) $2X^5 + 3X^4 + 2X^3 - X$,
    (b) $X^5 - \frac{1}{2}X^4 - 2X^3 + \frac{1}{2}X^2 - \frac{7}{2}X - 3$,
    ii) Probar que $X^4 + 2X^3 - 3X^2 - 2$ no tiene raíces racionales.

Factorización.

28. Factorizar en $\mathbb{C}[X]$, $\mathbb{R}[X]$, $\mathbb{Q}[X]$ y en $(\mathbb{Z}/7\mathbb{Z})[X]$ los polinomios cuadráticos

    i) $X^2 + 6X - 2$, ii) $X^2 + X - 6$, iii) $X^2 - 2X + 10$.

29. Factorizar en $\mathbb{C}[X]$ los polinomios

    i) $X^2 + (1 + 2\,i)\,X + 2\,i$,
    ii) $X^8 - 1$,
    iii) $X^6 - (2 - 2i)^{12}$.

30. Factorizar en $\mathbb{C}[X]$, $\mathbb{R}[X]$ y $\mathbb{Q}[X]$ los polinomios

    i) $X^6 - 9$,
    ii) $X^4 + 3$,
    iii) $X^4 - X^3 + X^2 - 3X - 6$.

31. Factorizar los polinomios

    i) $X^4 - 1$ en $(\mathbb{Z}/5\mathbb{Z})[X]$ y $(\mathbb{Z}/7\mathbb{Z})[X]$,
    ii) $X^4 + 3$ en $(\mathbb{Z}/7\mathbb{Z})[X]$,
    iii) $X^4 + X^3 + X^2$ en $(\mathbb{Z}/7\mathbb{Z})[X]$,
    iv) $X^7 - X$ en $(\mathbb{Z}/7\mathbb{Z})[X]$.

32. Sea $n \in \mathbb{N}$. Probar que $\displaystyle\sum_{k=0}^{n} X^k \in \mathbb{C}[X]$ tiene todas sus raíces complejas simples.

33. Factorizar los siguientes polinomios en $\mathbb{C}[X]$, $\mathbb{R}[X]$ y $\mathbb{Q}[X]$

    i) $X^5 - 4X^4 - X^3 + 9X^2 - 6X + 1$ sabiendo que $2 - \sqrt{3}$ es raíz.
    ii) $X^5 - X^3 + 17X^2 - 16X + 15$ sabiendo que $1 + 2\,i$ es raíz.
    iii) $X^6 + X^5 + 5X^4 + 4X^3 + 8X^2 + 4X + 4$ sabiendo que $\sqrt{2}\,i$ es raíz múltiple.

iv) $X^4+2X^3+3X^2+10X-10$ sabiendo que tiene una raíz imaginaria pura.

v) $X^5-3X^4-2X^3+13X^2-15X+10$ sabiendo que tiene alguna raíz en común con X^3+1.

vi) $f=X^4-6X^3+11X^2-2X-10$, sabiendo que tiene alguna raíz en común con el polinomio $g=X^4-5X^3+7X^2-6$.

34. Hallar todos los $a\in\mathbb{Q}$ tales que $f=X^4-(a+4)X^3+(4a+5)X^2-(5a+2)X+2a$ tenga a a como raíz *doble*. Para cada valor de a hallado, factorizar f en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.

35. Hallar todos los $a\in\mathbb{C}$ para los cuales al menos una de las raíces de

$$f=X^6+X^5-3X^4+2X^3+X^2-3X+a$$

es una raíz sexta de la unidad que no es una raíz cúbica de la unidad.

Para cada valor de $a\in\mathbb{Q}$ hallado, factorizar f en $\mathbb{Q}[X]$, $\mathbb{R}[X]$ y $\mathbb{C}[X]$.

36. i) En cada caso, hallar un polinomio $f\in\mathbb{Q}[X]$ de grado mínimo tal que:
   (a) $X^2(X^2+1)\mid(f:f')$.
   (b) $(f:f')=X^5-5X^4+\frac{25}{4}X^3$ y $f(1)=3$.
   (c) $X+2\mid f$, $(f:(X-\sqrt{2})^2)=X-\sqrt{2}$ y f mónico.

   ii) Determinar todos los $f\in\mathbb{Q}[X]$ mónicos de grado 5 que satisfacen simultáneamente que $(f:f')$ tiene grado 2, $1+2\,i$ es raíz de f y $f(1)=\frac{1}{2}$.

37. Sean $a,b,c\in\mathbb{C}$ las raíces de $2X^3-3X^2+4X+1$. Determinar

   i) $a+b+c$, ii) $ab+ac+bc$, iii) abc.

38. i) Hallar todas las raíces en $\mathbb{C}$ del polinomio $f=X^4-(i+4)X^3+(8+4i)X^2-(2i+24)X+12$ sabiendo que tiene al menos una raíz real.

   ii) Hallar todas las raíces en $\mathbb{C}$ del polinomio $f=X^6-3X^4-(2+8\,i)X^3+24\,iX+16\,i$, sabiendo que tiene al menos una raíz entera.

39. i) ¿Cuántos polinomios mónicos de grado 2 hay en $(\mathbb{Z}/7\mathbb{Z})[X]$? ¿Cuántos de ellos son reducibles y cuántos irreducibles?

   ii) Sea p un número primo. ¿Cuántos polinomios mónicos de grado 2 hay en $(\mathbb{Z}/p\mathbb{Z})[X]$? ¿Cuántos de ellos son reducibles y cuántos irreducibles?