Universidade de Santiago de Compostela

Grao en Intelixencia Artificial

Escola Técnica Superior de Enxeñería

Matemática Discreta

ÓSCAR RIVERO SALGADO

Santiago de Compostela, Xaneiro 2025

Índice xeral

Introdución **5**

1. Teoría de conxuntos **7**
1.1. Operacións con conxuntos 7
1.2. Aplicacións 10
1.3. Relacións de equivalencia 13

2. Indución matemática e demostracións **17**
2.1. Relacións de orde 17
2.2. O principio de indución 18
2.3. O teorema do binomio de Newton 21
2.4. Outros métodos de demostración 23

3. Aritmética **25**
3.1. Divisibilidade 25
3.2. Algoritmo de Euclides e identidade de Bézout 28
3.3. Congruencias 32
3.4. Resultados sobre congruencias 34
3.5. Raíces primitivas 39
3.6. A lei de reciprocidade cuadrática 43

4. Algoritmos **49**
4.1. Notación asintótica 49
4.2. Algoritmos 52
4.3. Criptografía e algoritmo RSA 57

5. Combinatoria **59**
5.1. Principios básicos de enumeración 59
5.2. Seleccións 62
5.3. Propiedades dos números binomiais e multinomiais 65
5.4. Principio de inclusión-exclusión 67
5.5. Particións dun conxunto 70
5.6. Números de Catalan 72

6. Recorrencias **75**
6.1. Sucesións recorrentes 75
6.2. Funcións xeradoras 77
6.3. Resolucións de recorrencias 83
6.4. Particións de enteiros 87

7. Teoría de grafos **89**
7.1. Definicións básicas 89
7.2. Conexión e distancia 95
7.3. Grafos eulerianos e hamiltonianos 100
7.4. Árbores 102
7.5. Planaridade 106
7.6. Coloración de grafos 107

8. Algoritmos en grafos **111**
8.1. Distancias en grafos: busca en anchura 111
8.2. Distancias en grafos ponderados: algoritmo de Dijkstra 112
8.3. Arbore xeradora mínima: algoritmo de Kruskal 113

9. Álxebras de Boole **117**
9.1. Álxebras de Boole: definicións 117
9.2. Funcións booleanas 118
9.3. Portas lóxicas 120
9.4. Minimización de circuítos 122

Introdución

Este libro está pensado para un primeiro curso de Matemática Discreta.
O texto adáptase ao temario da materia de *Matemática Discreta*, que se imparte na Escola Técnica Superior de Enxeñería da Universidade de Santiago de Compostela desde o curso 2022-2023

Contidos. O libro contén 9 capítulos, cada un deles correspondentes a un dos temas da materia.

- **Capítulo 1. Conxuntos e aplicacións.**
- **Capítulo 2. Indución matemática.**
- **Capítulo 3. Aritmética.**
- **Capítulo 4. Algoritmos.**
- **Capítulo 5. Combinatoria.**
- **Capítulo 6. Recorrencias.**
- **Capítulo 7. Teoría de grafos.**
- **Capítulo 8. Algoritmos en grafos.**
- **Capítulo 9. Álxebras de Boole.**

Tódolos capítulos se estruturan do mesmo xeito. Primeiro inclúense as diferentes seccións teóricas, nas que se presentan os resultados principais.

Libros e textos de referencias.

Agradecementos.

Capítulo 1

Teoría de conxuntos

O obxectivo deste tema é introducir as definicións básicas relativas á teoría de conxuntos e ás aplicacións entre eles, así como algunhas primeiras propiedades elementais. Na parte final, presentamos a noción de relación de equivalencia.

1.1. Operacións con conxuntos

Definición 1.1. Un *conxunto* está formado por *elementos*. Se A é un conxunto e a é un dos seus elementos, escríbese $a \in A$, e dise que a *pertence a* A. Se a non é un elemento de A, escríbese $a \notin A$. Para que un conxunto estea ben definido, o enunciado $a \in A$ ten que ser ou verdadeiro ou falso. Dous conxuntos son iguais cando teñen exactamente os mesmos elementos.

Hai dúas formas habituais de definir un conxunto. A primeira é dicindo cales son os seus elementos, que se escriben entre chaves. Por exemplo, $S = \{a, b, c, d\}$ é o conxunto que ten por elementos as catro letras a, b, c, d. A orde na que se escriben os elementos é irrelevante, de xeito que $\{a, b, c, d\} = \{b, a, c, d\}$; os conxuntos non teñen elementos repetidos, polo que tamén se cumpre que $\{a, b, c, d\} = \{a, b, b, c, d, c\}$. O segundo método consiste en dar unha propiedade que cumpren os elementos do conxunto, e unicamente eles. Por exemplo $P = \{n \colon n \text{ é un enteiro par}\}$ denota o conxunto dos enteiros pares. Existe un único conxunto sen ningún elemento, que se chama *conxunto baleiro* e que se denota por $\emptyset$.

Exemplo. Algúns exemplos importantes de conxuntos son os dos números enteiros, racionais e reais, que se denotan por $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$, respectivamente. Para evitar ambigüidades, nunca empregaremos a notación de números naturais ou $\mathbb{N}$, xa que, segundo a fonte consultada, pode denotar os enteiros positivos ou os non negativos. Escribiremos $\mathbb{Z}^{>0}$ para o conxunto dos enteiros positivos, $\{1, 2, 3, \ldots\}$, e $\mathbb{Z}^{\geq 0}$ para o conxunto dos enteiros non negativos, $\{0, 1, 2, 3, \ldots\}$.

Definición 1.2. Un conxunto A é *subconxunto* dun conxunto B se $a \in A$ implica $a \in B$ para todo B. Escríbese $A \subseteq B$.

As relacións de inclusión cumpren as seguintes propiedades:

(i) (Reflexiva) Se A é un conxunto, $A \subseteq A$.

(ii) (Antisimétrica) Se A e B son dous conxuntos e $A \subseteq B$ e $B \subseteq A$, entón $A = B$.

(iii) (Transitiva) Se A, B e C son conxuntos e $A \subseteq B$ e $B \subseteq C$, entón $A \subseteq C$.

Exemplo. Sexa $\mathbb{Z}$ o conxunto dos números enteiros. Dicimos que $4 \in \mathbb{Z}$, é dicir, o número 4 é un elemento do conxunto $\mathbb{Z}$. En cambio, non é correcto dicir que $4 \subseteq \mathbb{Z}$, porque o 4 é un elemento, non é un conxunto, e non ten sentido entón falar de inclusións. Si podemos dicir que $\{4\} \subseteq \mathbb{Z}$: o conxunto que só consta do elemento 4 é un subconxunto de $\mathbb{Z}$. Por este motivo, tampouco podemos escribir $\{4\} \in \mathbb{Z}$, dado que agora $\{4\}$

Definición 1.3. Se B é un conxunto, defínese o *conxunto das partes de* B como

$$\mathcal{P}(B) = \{A \colon A \subseteq B\}.$$

Exemplo. Se $B = \{1, 2, 3\}$, entón

$$\mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Tense entón que $\emptyset \in \mathcal{P}(B)$, porque, agora si, o conxunto baleiro é un subconxunto de $\mathcal{P}(B)$, que está formado unicamente por subconxuntos de B.

Definición 1.4. Sexa Ω un conxunto e A e B subconxuntos de Ω. A *unión* de A e B é o conxunto $A \cup B$ formado polos elementos que pertencen a A ou que pertencen a B. A *intersección* de A e B é o conxunto $A \cap B$ formado polos elementos que pertencen a ambos conxuntos ao mesmo tempo. Se $A \cap B = \emptyset$ dise que os conxuntos son *disxuntos*. A *diferenza* de A e B é o conxunto $A - B$ formado polos elementos de A que non pertencen a B. A diferenza $\Omega - A$ chámase *complementario de* A *respecto de* Ω e escríbese $\overline{A}$; outra notación habitual é A^c. Finalmente, a *diferenza simétrica* $A \triangle B$ é o conxunto formado polos elementos que pertencen exactamente a un dos conxuntos A ou B.

Tense que $A \triangle B = A \cup B - A \cap B$.

Exemplo. Sexa $\Omega = \{1, 2, 3, 4, 5, 6\}$, $A = \{1, 2, 3, 4\}$ e $B = \{3, 4, 5\}$. Entón,

$$A \cup B = \{1, 2, 3, 4, 5\}, \quad A \cap B = \{3, 4\}, \quad A \triangle B = \{1, 2, 5\}.$$

Por outra banda, $\overline{A} = \{5, 6\}$ e $\overline{B} = \{1, 2, 6\}$.

A modo de notación, escribiremos $[n]$ para referirnos ao conxunto formado polos n primeiros enteiros positivos:

$$[n] := \{1, 2, \ldots, n\}.$$

A proposición seguinte recolle as propiedades máis importantes da unión e da intersección de conxuntos. A comprobación de todas elas é rutineira e séguese a partir das definicións. En moitos casos, para entender mellor o significado, é útil realizar unha representación gráfica. É o que se coñece como *diagrama de Venn*, unha representación gráfica de conxuntos a través de liñas pechadas, de xeito que, por exemplo, a intersección correspóndese co recinto comprendido entre as liñas correspondentes a cada conxunto.

Proposición 1.1. Sexa Ω un conxunto. Para todo $A, B, C \in \mathcal{P}(\Omega)$ cúmprense as seguintes propiedades.

(a) (Idempotencia) $A \cup A = A$ e $A \cap A = A$.

(b) (Asociatividade) $(A \cup B) \cup C = A \cup (B \cup C)$ e $(A \cap B) \cap C = A \cap (B \cap C)$.

(c) (Conmutatividade) $A \cup B = B \cup A$ e $A \cap B = B \cap A$.

(d) (Absorción) $A \cap (A \cup B) = A$ e $A \cup (A \cap B) = A$.

(e) (Propiedade distributiva) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ e $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

(f) (Elemento absorbente) $A \cup \Omega = \Omega$ e $A \cap \emptyset = \emptyset$.

(g) (Elemento neutro) $A \cup \emptyset = A$ e $A \cap \Omega = A$.

(h) (Complementario) $A \cup \overline{A} = \Omega$ e $A \cap \overline{A} = \emptyset$.

(i) (Leis de Morgan) $\overline{A \cup B} = \overline{A} \cap \overline{B}$ e $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

(l) $\overline{\Omega} = \emptyset$ e $\overline{\emptyset} = \Omega$.

(m) $\overline{\overline{A}} = A$.

Para ilustrar o xeito de demostrar que estes resultados son certos, imos discutir a primeira parte da propiedade (i), isto é, que $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Demostración. Para demostrar unha igualdade de conxuntos é suficiente ver unha dobre inclusión, é dicir, que $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$ e $\overline{A \cup B} \supseteq \overline{A} \cap \overline{B}$.
Imos demostrar a primeira inclusión. Para iso, sexa $x \in \overline{A \cup B}$. Imos demostrar que $x \in \overline{A}$, sendo análoga a comprobación de que $x \in \overline{B}$. É equivalente ver que $x \in \overline{A}$ a ver que $x \notin A$. Agora ben, como $x \notin A \cup B$, en particular, $x \notin A$, como queriamos.
Pasamos á outra inclusión. Sexa $x \in \overline{A} \cap \overline{B}$, é dicir, $x \notin A$ e $x \notin B$. Hai que demostrar que $x \in \overline{A \cup B}$ ou, alternativamente, que $x \notin A \cup B$. Porén, isto último é equivalente a dicir que $x \notin A$ e $x \notin B$, que é obviamente certo pola condición de partida. □

Exemplo. Imos empregar as propiedades anteriores para demostrar que

$$A - (B \cap C) = (A - B) \cup (A - C).$$

Comezamos observando que, por definición, $A - (B \cap C) = A \cap \overline{B \cap C}$. Temos agora que

$$\begin{aligned} A \cap \overline{B \cap C} &= A \cap (\overline{B} \cup \overline{C}) \\ &= (A \cap \overline{B}) \cup (A \cap \overline{C}) \\ &= (A - B) \cup (A - C), \end{aligned}$$

onde na primeira igualdade empregamos as leis de Morgan e, na segunda, a propiedade distributiva.

Convén observar que é posible definir unións e interseccióńs arbitrarias, non necesariamente só de dous conxuntos. Sexa I un conxunto e supoñamos que, para $i \in I$, A_i é un subconxunto de Ω. Dise que $\{A_i \mid i \in I\}$ é unha *familia* de subconxuntos de Ω. A *unión* dos conxuntos A_i, $\bigcup_{i \in I} A_i$, é o conxunto formado polos elementos x de Ω de xeito que existe un $i \in I$ con $x \in A_i$. A *intersección* dos conxuntos A_i, denotada por $\bigcap_{i \in I} A_i$ é o conxunto formado polos x de Ω tales que $x \in A_i$ para todo $i \in I$.

Definición 1.5. Chámase *cardinal* dun conxunto ao número de elementos que ten. O cardinal dun conxunto A escríbese como $|A|$.

Por exemplo, cúmprese que, se A e B son conxuntos finitos, entón

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Definición 1.6. Sexan A e B dous conxuntos. O *produto cartesiano de A por B* é o conxunto $A \times B$ formado polas parellas ordenadas (a, b), con $a \in A$ e $b \in B$. O elemento a chámase *primeira compoñente ou coordenada* da parella e b é a *segunda compoñente ou coordenada*.

Se A e B son conxuntos finitos, cúmprese que $|A \times B| = |A| \cdot |B|$. Ademais, tense que $(a, b) = (c, d)$ se, e soamente se, $a = c$ e $b = d$. O produto cartesiano pódese definir tamén para n conxuntos do seguinte xeito. Sexan $A_1, \ldots, A_n$ conxuntos. O produto cartesiano é $A_1 \times \cdots \times A_n$, o conxunto das n tuplas $(a_1, \ldots, a_n)$, con $a_i \in A_i$. O produto cartesiano de n veces o mesmo conxunto A escríbese como A^n. No caso dos conxuntos finitos tense que $|A^n| = |A|^n$.

Exemplo. Se $A = \{1, 2, 3\}$ e $B = \{1, 2\}$, entón

$$A \times B = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 2)\}.$$

Por outra banda,

$$B^2 = B \times B = \{(1, 1), (1, 2), (2, 1), (2, 2)\}.$$

1.2. Aplicacións

A modo de notación, cando A e B son dous conxuntos, dicimos que unha *correspondencia* entre A e B é un subconxunto non baleiro $C \subseteq A \times B$.

Definición 1.7. Sexan A e B dous conxuntos. Unha *aplicación* de A en B é unha correspondencia $f \subseteq A \times B$ de xeito que para cada $a \in A$ existe un único $b \in B$ de xeito que $(a, b) \in f$. O conxunto A chámase *dominio* ou *conxunto inicial* e o conxunto B *imaxe* ou *conxunto final* da aplicación. Dado $a \in A$, o único elemento $b \in B$ tal que $(a, b) \in f$ chámase *imaxe* de a e denótase como $f(A)$. O elemento a é unha *preimaxe* de B.

Definición 1.8. Sexan $f\colon A \to B$ e $g\colon B \to C$ dúas aplicacións. A aplicación $g \circ f\colon A \to C$ definida por $(g \circ f)(a) = g(f(a))$ para todo $a \in A$ chámase *composición* de f e g.

A composición de dúas aplicacións non é necesariamente conmutativa.

Definición 1.9. A aplicación $\mathrm{Id}_A\colon A \to A$ definida por $\mathrm{Id}_A(a) = a$ para todo $a \in A$ chámase *aplicación identidade* de A.

Se $f\colon A \to B$ é unha aplicación arbitraria, tense que $f \circ \mathrm{Id}_A = f = \mathrm{Id}_B \circ f$.

Definición 1.10. Unha aplicación $f\colon A \to B$ é *inxectiva* se elementos diferentes de A teñen imaxes diferentes. A aplicación dise que é *sobrexectiva* se todo elemento de B ten, polo menos, unha preimaxe. Finalmente, dise que é *bixectiva* se é inxectiva e sobrexectiva.

Exemplo. Sexa $A = \{1, 2, 3\}$ e $B = \{1, 2, 3, 4\}$. A aplicación $\alpha\colon A \to B$ definida por $\alpha(1) = \alpha(2) = 2$ e $\alpha(3) = 1$ non é nin inxectiva nin sobrexectiva. Os elementos 1 e 2 teñen a mesma imaxe, e o 3 non ten ningunha preimaxe.
A aplicación β definida por $\beta\colon A \to A$ definida por $\alpha(1) = 2$, $\alpha(2) = 3$ e $\alpha(3) = 1$ é inxectiva e sobrexectiva (e, polo tanto, bixectiva).
A aplicación $\gamma\colon A \to B$ que cumpre $f(x) = x$ para todo $x \in A$ é inxectiva, pero non sobrexectiva; non hai dous elementos coa mesma imaxe, e o 4 non ten ningunha preimaxe.

A aplicación $\delta\colon B \to A$ dada por $\delta(1) = \delta(2) = 1$, $\delta(3) = 2$ e $\delta(4) = 3$ é sobrexectiva, pero non inxectiva.

Exemplo. A función $f\colon \mathbb{R} \to \mathbb{R}$ dada por $x \mapsto x^2$ non é inxectiva nin sobrexectiva: tense que $f(1) = f(-1)$, polo que non é inxectiva; e o -1 non ten ningunha preimaxe, polo que non é tampouco sobrexectiva.
A función $g\colon \mathbb{R} \to \mathbb{R}$ dada por $x \mapsto x + 1$ é bixectiva: se $g(x) = g(y)$, temos que $x + 1 = y + 1$, o que automaticamente implica que $x = y$, polo que g é inxectiva; por outra banda, dado $y \in \mathbb{R}$, tense que $g(y - 1) = y$, polo que a función é sobrexectiva.
A función $h\colon \mathbb{R} \to \mathbb{R}$ dada por e^x é inxectiva, pero non sobrexectiva. É inxectiva porque calquera función de variable real estritamente crecente é inxectiva, e non é sobrexectiva porque a exponencial non toma valores non negativos.
Por último, a función $j\colon \mathbb{R} - \{0\} \to \mathbb{R}$ dada por

$$j(x) = \begin{cases} \log(x) & \text{se } x > 0 \\ \log(-x) & \text{se } x < 0 \end{cases}$$

é sobrexectiva, pero non inxectiva. É sobrexectiva porque o logaritmo toma calquera valor no intervalo $(0, +\infty)$, ao ser unha función continua e estritamente crecente que ten límite $-\infty$ en $x = 0$ e $+\infty$ cando x tende a infinito; porén, non é inxectiva xa que $j(x) = j(-x)$.

Proposición 1.2. Sexa $f\colon A \to B$ e $g\colon B \to C$ dúas aplicacións.

(a) Se f e g son inxectivas, entón $g \circ f$ é inxectiva.

(b) Se f e g son sobrexectivas, entón $g \circ f$ é sobrexectiva.

(c) Se f e g son bixectivas, entón $g \circ f$ é bixectiva.

Demostración. (a) Sexan $a_1, a_2 \in A$ e supoñamos que $(g \circ f)(a_1) = (g \circ f)(a_2)$. Como $g(f(a_1)) = g(f(a_2))$ e g é inxectiva, temos que $f(a_1) = f(a_2)$. Finalmente, como f é inxectiva, $a_1 = a_2$, como queriamos.

(b) Sexa $c \in C$. Como g é sobrexectiva, existe $b \in B$ de xeito que $g(b) = c$; e como f é sobrexectiva, existe $a \in A$ con $f(a) = b$. Polo tanto, $g(f(a)) = c$.

(c) Como f e g son inxectivas, a composición tamén o é; como ambas son sobrexectivas, a composición tamén. Polo tanto, a composición é bixectiva.

□

Unha aplicación $f\colon A \to B$ induce unha aplicación

$$f_*\colon \mathcal{P}(A) \to \mathcal{P}(B), \quad X \mapsto f_*(X) = \{f(x) \mid x \in X\}$$

e unha aplicación

$$f^*\colon \mathcal{P}(B) \to \mathcal{P}(A), \quad Y \mapsto f^*(Y) = \{x \in A \mid f(x) \in Y\}.$$

A aplicación f_* adoita chamarse *imaxe directa* e a aplicación f^*, *imaxe recíproca*.

Exemplo. Sexa $f\colon \{1,2,3,4\} \to \{1,2,3\}$ dada por $f(1) = f(2) = f(4) = 1$ e $f(3) = 2$. Entón, $f_*\colon \mathcal{P}(A) = \mathcal{P}(B)$ cumpre que $f_*(\emptyset) = \emptyset$, $f_*(\{1\}) = \{1\}$, $f_*(\{1,3\}) = \{1,2\}$, $f_*(\{1,3,4\}) = \{1,2\}$ ou $f_*(\{1,2,3,4\}) = \{1,2\}$; de xeito similar pódese calcular a imaxe do resto de subconxuntos de A (hai 16 en total).
Por outra banda, a imaxe recíproca cumpre que $f^*(\emptyset) = \emptyset$, $f^*(\{3\}) = \emptyset$, $f^*(\{1,3\}) = \{1,2,4\}$ e $f^*(\{1,2,3\}) = \{1,2,3,4\}$.

Se a aplicación $f\colon A \to B$ é inxectiva ou sobrexectiva, as aplicacións f_* e f^* tamén cumpren propiedades relacionadas.

Proposición 1.3. Sexa $f\colon A \to B$ unha aplicación.

(a) Se f é inxectiva, $f_*\colon \mathcal{P}(A) \to \mathcal{P}(B)$ é inxectiva, mentres que $f^*\colon \mathcal{P}(B) \to \mathcal{P}(A)$ é sobrexectiva.

(b) Se f é sobrexectiva, $f_*\colon \mathcal{P}(A) \to \mathcal{P}(B)$ é sobrexectiva, mentres que $f^*\colon \mathcal{P}(B) \to \mathcal{P}(A)$ é inxectiva.

Demostración. Trátase dunha comprobación rutineira empregando as definicións. □

A seguinte proposición resume outras propiedades relevantes da imaxe directa e da imaxe recíproca.

Proposición 1.4. Se $f\colon A \to B$, entón as aplicación $f_*\colon \mathcal{P}(A) \to \mathcal{P}(B)$ e $f^*\colon \mathcal{P}(B) \to \mathcal{P}(A)$ cumpren as seguintes propiedades. En tódolos casos, $A_1, A_2 \subseteq A$ e $B_1, B_2 \subseteq B$ son conxuntos arbitrarios.

(a) Se $A_1 \subseteq A_2$, entón $f_*(A_1) \subseteq f_*(A_2)$.

(b) Se $B_1 \subseteq B_2$, entón $f^*(B_1) \subseteq f^*(B_2)$.

(c) $A_1 \subseteq f^*(f_*(A_1))$.

(d) $f_*(f^*(B_1)) \subseteq B_1$.

(e) $f_*(A_1 \cup A_2) = f_*(A_1) \cup f_*(A_2)$.

(f) $f^*(B_1 \cup B_2) = f^*(B_1) \cup f^*(B_2)$.

(g) $f_*(A_1 \cap A_2) \subseteq f_*(A_1) \cap f_*(A_2)$.

(h) $f^*(B_1 \cap B_2) = f^*(B_1) \cap f^*(B_2)$.

(i) $f^*(B - B_1) = A - f^*(B_1)$.

Para ilustrar o xeito de demostrar que estas propiedades son certas, imos discutir a demostración das propiedades (f) e (g).

Demostración. (f) Como é habitual, imos comprobar a dobre inclusión. Sexa $x \in f^*(B_1 \cup B_2)$. Isto quere dicir que existe $y \in B_1 \cup B_2$ de xeito que $f(x) = y$. En particular, $y \in B_1$ ou $y \in B_2$; supoñamos, sen perder xeneralidade, que $y \in B_1$. Como $f(x) = y$, para $y \in B_1$, tense que $x \in f^*(B_1)$, como queriamos ver. Sexa agora $x \in f^*(B_1) \cup f^*(B_2)$. En particular, $x \in f^*(B_1)$ ou $x \in f^*(B_2)$; imos supor que estamos no primeiro caso, xa que o segundo é análogo. Nese caso, existe $y \in B_1$ de xeito que $f(x) = y$. Como se cumpre tamén que $y \in B_1 \cup B_2$, necesariamente sucede que $x \in f^*(B_1 \cup B_2)$.

(g) Sexa $y \in f_*(A_1 \cap A_2)$. Entón, existe $x \in A_1 \cap A_2$ de xeito que $f(x) = y$. Sucede entón que $y \in f_*(A_1)$, xa que $f(x) = y$ e $x \in A_1$; de xeito análogo, $y \in f_*(A_2)$.

□

Convén observar que mentres a unión se comporta ben tanto por f_* como por f^*, non sucede o mesmo para a intersección. Consideremos para ilustralo o caso no que $A = \{1, 2, 3\}$ e $B = \{1, 2\}$. Sexa $f\colon A \to B$ dada por $f(1) = f(3) = 1$ e $f(2) = 2$. Tomamos agora $A_1 = \{1, 2\}$ e $A_2 = \{2, 3\}$. Entón,

$$f_*(A_1 \cap A_2) = f_*(\{2\}) = \{2\},$$

mentres que

$$f_*(A_1) \cap f_*(A_2) = \{1, 2\} \cap \{1, 2\} = \{1, 2\}.$$

As propiedades (c) e (d) pódense converter en igualdades cando as aplicacións correspondentes son inxectivas ou sobrexectivas.

Proposición 1.5. Se $f\colon A \to B$, entón as aplicación $f_*\colon \mathcal{P}(A) \to \mathcal{P}(B)$ e $f^*\colon \mathcal{P}(B) \to \mathcal{P}(A)$ cumpren as seguintes propiedades. Sexa $A_1 \subseteq A$ e $B_1 \subseteq B$.

(a) Se f é inxectiva $A_1 = f^*(f_*(A_1))$.

(b) Se f é sobrexectiva, $f_*(f^*(B_1)) = B_1$.

Demostración. (a) Do resultado anterior sabemos que $A_1 \subseteq f^*(f_*(A_1))$. Se non fosen iguais, existiría un elemento $x' \in f^*(f_*(A_1))$ de xeito que $x' \notin A_1$. Como $x' \in f^*(f_*(A_1))$, temos que $f(x') \in f_*(A_1)$, polo que existe $x \in A_1$ de xeito que $f(x) = f(x')$. Por ser f inxectiva, a última igualdade implica que $x = x'$, o que é unha contradición, xa que $x \in A_1$ e $x' \notin A_1$.

(b) Sabemos que $f_*(f^*(B_1)) \subseteq B_1$. Sexa $y \in B_1$; imos comprobar que $y \in f_*(f^*(B_1))$. Como f é sobrexectiva, sabemos que existe $x \in A$ de xeito que $f(x) = y$. Polo tanto, $y \in f_*(\{x\})$; porén, temos que $\{x\} \subseteq f^*(B_1)$ xa que, por definición, x é unha preimaxe dun elemento de B_1. Polo tanto, $y \in f_*(\{x\}) \subseteq f_*(f^*(B_1))$.

□

É frecuente cometer o abuso de notación de escribir f en vez de f_* e f^{-1} en lugar de f^*. Por outro lado, se $y \in B$, é normal escribir $f^{-1}(b)$ e non $f^*(\{b\})$, que sería o correcto conforme á notación que se introduciu.

1.3. Relacións de equivalencia

Definición 1.11. Unha partición dun conxunto A é un conxunto P de subconxuntos non baleiros de A disxuntos dous a dous e de xeito que a unión de todos eles é A. Máis concretamente, é un conxunto $P \subseteq \mathcal{P}(A)$ de xeito que:

(i) O conxunto baleiro non está en P.

(ii) $P_1 \cap P_2 = \emptyset$ para todo $P_1, P_2 \in P$, con $P_1 \neq P_2$.

(iii) $A = \cup_{P_i \in P} P_i$.

Definición 1.12. Unha relación R definida nun conxunto A é de *equivalencia* se, para todo $a, b, c \in A$, se cumpren as seguintes propiedades:

(i) (Reflexiva) aRa;

(ii) (Simétrica) aRb implica bRa;

(iii) (Transitiva) aRb e bRc implica aRc.

A seguinte proposición, cuxa demostración é inmediata, asegura que unha partición produce automaticamente unha relación de equivalencia.

Proposición 1.6. Se $\mathcal{P}$ é unha partición dun conxunto A, entón a relación definida en A por *aRb se, e soamente se, existe un $P \in \mathcal{P}$ tal que $a, b \in \mathcal{P}$* é de equivalencia.

Se R é unha relación de equivalencia nun conxunto A, o conxunto

$$\bar{a} = \{x \in A \mid xRa\}$$

chámase *clase de equivalencia do elemento a*. O conxunto de clases de equivalencia denótase por A/R e chámase *conxunto cociente* de A pola relación R.

Proposición 1.7. Se R é unha relación de equivalencia definida nun conxunto A, entón o conxunto de clases de equivalencia A/R é unha partición de A.

Demostración. A propiedade reflexiva implica que $a \in \bar{a}$ para todo $a \in A$. Iso quere dicir que unha clase de equivalencia $\bar{a}$ é un conxunto non baleiro porque $a \in \bar{a}$, e tamén a unión de tódalas clases é A, xa que todo elemento pertence á súa propia clase. Falta por ver que dúas clases son disxuntas. Supoñamos que $x \in \bar{a}$ e $x \in \bar{b}$, isto é, xRa e xRb. Pola propiedade simétrica, aRx; pola transitiva, aRb, de onde se ten que $\bar{a} \subseteq \bar{b}$. Un argumento similar dános que $\bar{b} \subseteq \bar{a}$, polo que $\bar{a} = \bar{b}$. □

Exemplo. Sexa P o conxunto das 50 provincias españolas. En P definimos a relación de equivalencia pola cal xRy se, e soamente se, x e y están na mesma comunidade autónoma.

- (Reflexiva) Temos que toda provincia está na mesma comunidade autónoma que ela mesma.
- (Simétrica) Se a provincia P_1 está na mesma comunidade que P_2, entón P_2 está na mesma que P_1.
- (Transitiva) Se P_1 está na mesma comunidades autónoma que P_2, e P_2 na mesma que P_3, entón P_1 está na mesma comunidade autónoma que P_3.

O conxunto cociente P/R está formado polas clases de equivalencia de provincias, isto é, unha por cada comunidade autónoma. Por exemplo, a clase de equivalencia da provincia Ourense contén os elementos A Coruña, Lugo, Ourense e Pontevedra; observamos que a clase de equivalencia da provincia Ourense é, polo tanto, a mesma que a clase de equivalencia da provincia Lugo.

Exemplo. No conxunto $\mathbb{Z}^{\geq 0} \times \mathbb{Z}^{\geq 0}$ dos enteiros non negativos, a relación dada por $(a, b)R(c, d)$ se, e soamente se, $a + d = b + c$, é de equivalencia.

- (Reflexiva) Temos que $(a, b)R(a, b)$ xa que $a + b = b + a$.
- (Simétrica) $(a, b)R(c, d)$ quere dicir que $a + d = b + c$, e $(c, d)R(a, b)$, que $c + b = d + a$. Polo tanto, as dúas condicións son equivalentes.

- (Transitiva) Se $(a,b)R(c,d)$ e $(c,d)R(e,f)$, entón $a+d=b+c$ e $c+f=d+e$. De aquí dedúcese que $a+f=b+e$, polo que $(a,b)R(e,f)$.

Dado un elemento $\alpha=(a,b)$, a súa clase de equivalencia $\bar{\alpha}$ está formada por tódolos elementos (a',b') tales que $b'-a'=b-a$. Polo tanto, o conxunto cociente identifícase cos enteiros.

Exemplo. No conxunto $A=\{(a,b) \mid a,b\in\mathbb{Z},\ b\neq 0\}$, dicimos que $(a,b)R(c,d)$ se, e soamente se, $ad=bc$. Trátase dunha relación de equivalencia, xa que cumpre as tres propiedades.

- (Reflexiva) Temos que $(a,b)R(a,b)$ xa que $ab=ba$.

- (Simétrica) $(a,b)R(c,d)$ quere dicir que $ad=bc$, e $(c,d)R(a,b)$, que $cb=da$. Polo tanto, as dúas condicións son equivalentes.

- (Transitiva) Se $(a,b)R(c,d)$ e $(c,d)R(e,f)$, entón $ad=bc$ e $cf=de$. Se $c=0$, entón $a=e=0$ e o resultado é certo. Senón, $af=\frac{ad}{c}\cdot e=be$, polo que, en calquera caso, $(a,b)R(e,f)$.

Dado un elemento $\alpha=(a,b)$, con $a\neq b$, a súa clase de equivalencia $\bar{\alpha}$ está formada por tódolos elementos (a',b') tales que $a/b=a'/b'$. Polo tanto, o conxunto cociente identifícase cos racionais.

Proposición 1.8 (Descomposición canónica dunha aplicación)**.** Sexa $f\colon A\to B$ unha aplicación. Entón:

(a) A relación definida en A por aRb se, e soamente se, $f(a)=f(b)$ é unha relación de equivalencia.

(b) A aplicación $\pi\colon A\to A/R$ que envía cada elemento á súa clase de equivalencia $\pi(a)=\bar{a}$ é unha aplicación sobrexectiva.

(c) A aplicación $\hat{f}\colon A/R\to f(A)$ que envía cada clase $\bar{a}$ ao elemento $\hat{f}(\bar{a})=f(a)$ está ben definida e é bixectiva.

(d) A aplicación $j\colon f(A)\to B$ definida por $j(b)=b$ é inxectiva.

(e) Tense que $f=j\circ\hat{f}\circ\pi$.

Demostración. (a) Trátase dunha comprobación rutineira.

(b) O cociente A/R é o conxunto das clases de equivalencia, de xeito que cada clase $c\in A/R$ éo dalgún elemento $c=\bar{a}$. Entón, $\pi(a)=c$, polo que π é sobrexectiva.

(c) Sexa $c\in A/R$. A súa imaxe $\hat{f}(c)$ está definida como segue: cóllese a de xeito que $c=\bar{a}$ e ponse $\hat{f}(c)=f(a)$. Se $c=\bar{b}$, entón $f(a)=f(b)$, polo que a aplicación está ben definida e unicamente depende de c. Para ver que é inxectiva, observamos que se $\hat{f}(\bar{a})=\hat{f}(\bar{b})$, entón $f(a)=f(b)$, polo que $\bar{a}=\bar{b}$. Finalmente, para ver que é sobrexectiva, temos que todo elemento de $f(A)$ é da forma $f(a)$, para algún $a\in A$. Temos entón que $\bar{a}$ é unha preimaxe de $f(a)$ por $\hat{f}$.

(d) É unha comprobación inmediata.

(e) Sexa $a \in A$. Entón,

$$(j \circ \hat{f} \circ \pi)(a) = j(\hat{f}(\pi(a))) = j(\hat{f}(\bar{a})) = j(f(a)) = f(a),$$

de onde se segue que $j \circ \hat{f} \circ \pi = f$.

□

Exemplo. Consideramos a aplicación $f\colon [4] \to [6]$ dada por $f(1) = f(2) = 1$, $f(3) = f(4) = 2$. Consideramos polo tanto a relación de equivalencia R na que unha das clases contén os elementos 1 e 2 e outra o 3 o 4. Sexa C o conxunto cociente e sexa $\pi\colon [4] \to C$ a aplicación que envía cada elemento á súa clase. A continua, como a imaxe de f é o conxunto $\{1, 2\}$, consideramos a aplicación $\hat{f}\colon C \to \{1, 2\}$ que envía a clase do 1 a 1 e a clase de 3 a 2. Finalmente, sexa $j\colon \{1, 2\} \to [6]$ a aplicación que envía cada número a el mesmo. Cúmprese polo tanto que $f = j \circ \hat{f} \circ \pi$.

Exemplo. Consideramos a aplicación $f\colon \mathbb{R}^2 \to \mathbb{R}$ dada por $f(x, y) = \sqrt{x^2 + y^2}$. Temos que dous elementos teñen a mesma imaxe se, e soamente se, están á mesma distancia da orixe; iso permite definir unha relación de equivalencia:

$$(x_1, y_1)E(x_2, y_2) \quad \text{se, e soamente, se} \quad x_1^2 + y_1^2 = x_2^2 + y_2^2.$$

Polo tanto, a relación de equivalencia $C = \mathbb{R}^2/E$ é o conxunto de circunferencias centradas en $(0, 0)$. A aplicación $\pi\colon \mathbb{R}^2 \to \mathbb{C}$ envía cada $x \in \mathbb{R}^2$ á circunferencia centrada en $(0, 0)$ que pasa por x. A imaxe de f é o conxunto dos números reais non negativos, polo que $\tilde{f}\colon C \to \mathbb{R}^{\geq 0}$ faille corresponder a cada circunferencia o seu radio. Finalmente, j envía cada radio r a el mesmo en $\mathbb{R}$.

Capítulo 2

Indución matemática e demostracións

O obxectivo deste tema é discutir algunhas técnicas de demostración frecuentes en matemáticas. A principal delas, a indución, require introducir as relacións de orde e o concepto de *conxunto ben ordenado*. Como aplicación destacada, presentamos o teorema do binomio de Newton.

2.1. Relacións de orde

Definición 2.1. Unha relación R definida nun conxunto E é unha relación de orde se, para todo $a, b, c \in E$, cúmprense as tres propiedades seguintes:

(i) (Reflexiva) aRa;

(ii) (Antisimétrica) se aRb e bRa, entón $a = b$.

(iii) (Transitiva) se aRb e bRc, entón aRc.

Un *conxunto ordenado* é unha parella (E, R), onde E é un conxunto e R é unha relación de orde en E. Se E é un conxunto ordenado e $\emptyset \neq A \subseteq E$, dicimos que un elemento $a \in A$ é un *mínimo* ou *primeiro elemento* de A se $a \leq x$ para todo $x \in A$. Escribimos $a = \min A$. De xeito similar, dise que un elemento $b \in A$ é un *máximo* se $x \leq b$ para todo $x \in A$, e pomos $b = \max A$.
Un elemento c de E dise que é unha *cota inferior* de A se $c \leq x$ para todo $x \in A$, e unha *cota superior* se $c \geq x$ para todo $x \in A$. Se o conxunto de cotas inferiores ten máximo, entón a este máximo chámaselle *ínfimo* de A; se o conxunto de cotas superiores ten mínimo, chámaselle *supremo* de A.

Exemplo. Os enteiros positivos, coa relación de orde dada pola divisibilidade, son unha relación de orde. É dicir, pomos aRb se, e soamente se, $a \mid b$.

Porén, nas relacións de orde non esiximos que dous elementos calquera se poidan comparar.

Exemplo. No conxunto dos enteiros positivos, $\mathbb{Z}^{\geq 1}$, consideramos a relación de orde dada pola divisibilidade, é dicir, aRb se, e soamente se, $a \mid b$. Imos verificar que se cumpren as tres propiedades.

- (Reflexiva) Para calquera $a \in \mathbb{Z}^{\geq 1}$ cúmprese que $a \mid a$.

- (Antisimétrica) Se $a \mid b$ e $b \mid a$ tense que $b \geq a$ e $a \geq b$, polo que, en particular, $a = b$.

- (Transitiva) Se $a \mid b$ e $b \mid c$, entón $b = ka$ e $c = k'b$, para algúns $k, k' \in \mathbb{Z}^{\geq 1}$. Polo tanto, $c = k'b = k'ka$, polo que $a \mid c$.

2.2. O principio de indución

Definición 2.2. Unha relación de orde $\leq$ definida nun conxunto E é unha *boa orde* se todo subconxunto non baleiro de E ten un mínimo. Un *conxunto ben ordenado* é unha parella $(E, \leq)$ formada por un conxunto E e unha boa orde definida en E.

Unha propiedade importante dos conxuntos ben ordenados é o principio de indución.

Proposición 2.1. Sexa E un conxunto non baleiro e ben ordenado, e A un subconxunto de E que cumpre a seguinte propiedade: para cada $b \in E$, se $x \in A$ para todo $x < b$, entón $b \in A$. Nese caso, $A = E$.

Demostración. Supoñamos que $A \neq E$. Entón o conxunto $E - A$ é non baleiro. Como E ten unha boa orde, o conxunto $E - A$ ten un primeiro elemento, ao que podemos chamar p. Claramente $p \notin A$. Como p é o mínimo de $E - A$, para todo $x < p$ temos que $x \in A$. Pola primeira propiedade do enunciado, resulta que $p \in A$, o que é contraditorio. □

Proposición 2.2. Sexa n_0 un enteiro e $E = \{n \in \mathbb{Z} \mid n \geq n_0\}$. Sexa A un subconxunto de E que cumpre que $n_0 \in A$ e que, para todo $n > n_0$, se $n - 1 \in A$, entón $n \in A$. Neste caso, $A = E$.

Demostración. Supoñamos que $A \neq E$. O conxunto $E - A$ non é baleiro e, polo tanto, ten un primeiro elemento p, que cumpre $p \notin A$. Como $n_0 \in A$, tense que $p > n_0$. Entón, $p - 1 \in E$, e como p é o primeiro elemento de $E - A$, cúmprese que $p - 1 \in A$. Pero, polas condicións do enunciado, cúmprese entón que $p \in A$, o cal é unha contradición. □

O método de indución consiste en demostrar a veracidade dun enunciado comprobándoo para un caso base n_0 e demostrando logo que se se cumpre para $n \geq n_0$, tamén se cumpre para $n + 1$. Coñécese como *método de indución forte* ao mesmo procedemento, pero no que se supón que o enunciado se cumpre non só para n, senón para calquera enteiro entre n_0 e n. A demostración deste resultado é similar á do caso anterior.

Proposición 2.3 (Principio de indución forte)**.** Sexa n_0 un enteiro e $E = \{n \in \mathbb{Z} \mid n \geq n_0\}$. Sexa A un subconxunto de E que cumpre que $n_0 \in A$ e que, para todo $n > n_0$, se $a \in A$ para todo $n_0 \leq a \leq n - 1$, entón $n \in A$. Neste caso, $A = E$.

Demostración. Sexa B o subconxunto de E formado polos elementos n que cumpren que para todo $n_0 \leq k \leq n$ se ten que $n \in A$. Claramente temos que $B \subseteq A \subseteq E$, polo que se demostramos que $B = E$, automaticamente concluímos que $A = E$.
Imos demostrar que $B = E$ por indución. Temos que n_0 pertence a A por definición, polo que $n_0 \in B$. Supoñamos agora que se cumpre que $n \in B$. Polo tanto, tense que tódolos k con $n_0 \leq k \leq n$ están en A. Iso quere dicir, pola condición do enunciado, que $n + 1 \in A$. Polo tanto, tense que k pertence a A para todo $n_0 \leq k \leq n + 1$, polo que $n + 1 \in B$. Polo principio de indución, $B = E$, o que é suficiente para concluír. □

A continuación imos traballar diferentes exemplos de demostracións por indución. En todas elas se segue o seguinte esquema.

(a) Comprobación do caso base.

(b) Formulación da hipótese de indución.

(c) Paso indutivo: empregando a hipótese de indución, é dicir, que o resultado é certo para n, demostrar que o resultado é certo para $n+1$.

Exemplo. Sexa n un enteiro positivo. Demostrar que

$$1+2+\ldots+n=\frac{n(n+1)}{2}.$$

(a) O resultado é certo para $n=1$, xa que $1=\frac{1\cdot 2}{2}$.

(b) Hipótese de indución. Supoñamos certo o resultado para n, é dicir, que

$$1+2+\ldots+n=\frac{n(n+1)}{2}.$$

(c) Para demostrar o resultado para $n+1$, observamos que

$$\begin{aligned}1+2+\ldots+n+(n+1) &= (1+2+\ldots+n)+(n+1)\\ &= \frac{n(n+1)}{2}+(n+1)\\ &= \frac{(n+1)(n+2)}{2},\end{aligned}$$

onde a segunda igualdade é consecuencia da hipótese de indución.

Exemplo. Sexa n un enteiro positivo. Demostrar que

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}\ldots+\frac{1}{n\cdot(n+1)}=\frac{n}{n+1}.$$

(a) O resultado é certo para $n=1$, xa que $\frac{1}{1\cdot 2}=\frac{1}{1+1}$.

(b) Hipótese de indución. Supoñamos que o resultado é certo para n, é dicir, que

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}\ldots+\frac{1}{n\cdot(n+1)}=\frac{n}{n+1}.$$

(c) Para demostrar o resultado para $n+1$, observamos que

$$\begin{aligned}\frac{1}{1\cdot 2}+\ldots+\frac{1}{n\cdot(n+1)}+\frac{1}{(n+1)(n+2)} &= \frac{n}{n+1}+\frac{1}{(n+1)(n+2)}\\ &= \frac{n(n+2)+1}{(n+1)(n+2)}\\ &= \frac{(n+1)^2}{(n+1)(n+2)}\\ &= \frac{n+1}{n+2},\end{aligned}$$

onde na primeira igualdade se empregou a hipótese de indución.

Imos agora tratar un par de exemplos diferentes, no que se demostra unha desigualdade.

Exemplo. Sexa $n \geq 4$ un enteiro positivo. Demostrar por indución que $n! > 2^n$.

(a) Comezamos observando que para $n = 4$ o resultado é certo, xa que $24 = 4! > 2^4 = 16$.

(b) Hipótese de indución. Supomos certo o resultado para n, isto é, $n! > 2^n$.

(c) Imos demostrar agora que $(n+1)! > 2^{n+1}$. Para iso, temos que

$$(n+1)! = (n+1)n! > (n+1)2^n > 2 \cdot 2^n = 2^{n+1},$$

onde a hipótese de indución se empregou na primeira desigualdade.

Exemplo. Sexa $n \geq 4$ un enteiro positivo. Imos demostrar por indución que $2^n \geq n^2$.

(a) Comezamos observando que para $n = 4$ o resultado é certo, xa que $16 = 2^4 > 4^2 = 16$.

(b) Supomos agora certo o resultado para n, isto é, $2^n > n^2$.

(c) Imos demostrar agora que $2^{n+1} > (n+1)^2$. Para iso, temos que

$$2^{n+1} = 2 \cdot 2^n \geq 2n^2 = n^2 + n^2 \geq n^2 + 2n + 1,$$

onde a hipótese de indución se empregou na primeira desigualdade e a segunda séguese de observar que $n^2 > 2n$, xa que $n \geq 2$ e, polo tanto, $n^2 \geq 2n + 1$.

Exemplo. Sexa $n \geq 0$ un número enteiro. Demostrar que $n^3 + 2n$ sempre é múltiplo de 3.

(a) Comezamos comprobando que o enunciado se cumpre no caso base $n = 0$, xa que $0^3 + 2 \cdot 0 = 0$ é un múltiplo de 3.

(b) Supoñamos certa a afirmación para n, é dicir, poñamos $n^3 + 2n = 3k$, onde $k \in \mathbb{Z}$.

(c) Imos comprobar agora o resultado para $n + 1$. Entón:

$$\begin{aligned}(n+1)^3 + 2(n+1) &= n^3 + 3n^2 + 3n + 1 + 2n + 2 \\ &= n^3 + 2n + +3n^2 + 3n + 3 \\ &= 3k + 3n^2 + 3n + 3 \\ &= 3(k + n^2 + n + 1),\end{aligned}$$

que é un múltiplo de 3. Observamos que no terceiro paso aplicamos a hipótese de indución.

Convén ter presente que nas demostracións por indución hai que tratar sempre o caso base e asegurarse de que a hipótese de indución non precisa de ningunha condición extra no valor de n. A modo de exemplo, imos discutir a seguinte demostración falsa.

Exemplo. Vaise demostrar por indución que tódolos cabalos son da mesma cor. *Para $n = 1$, o resultado é trivialmente certo. Supoñamos agora que o resultado se cumpre para n, polo que calquera grupo de n cabalos é da mesma cor. Consideremos entón un grupo de $n + 1$ cabalos. Excluímos un dos cabalos e miramos aos outros n que, por hipótese de indución, son da mesma cor. De xeito similar, se excluímos un cabalo diferente, temos que o grupo de n teñen a mesma cor. Polo tanto, o primeiro cabalo que*

foi excluído é da mesma cor que os que non excluímos que, á súa vez, son da mesma cor que o último que se excluíu. Polo tanto, se n cabalos teñen a mesma cor, $n+1$ tamén.
O erro no argumento é supor que o conxunto de $n+1$ cabalos ten tamaño polo menos 3, de xeito que dous conxuntos de n elementos sempre comparten polo menos un argumento. Iso, por suposto, non é certo cando $n+1=2$.

Imos rematar a sección dando un exemplo no que se emprega a indución forte.

Exemplo. Defínese a sucesión dada por $a_0 = 1$, $a_1 = 3$ e $a_n = 2a_{n-1} - a_{n-2}$ para $n \geq 2$. Imos demostrar por indución que $a_n = 2n+1$. Para $n = 0, 1$ o resultado é certo. Supoñamos que o resultado é certo ata un número n e ímolo probar para $n+1$. En particular, temos que $a_n = 2n+1$ e $a_{n-1} = 2n-1$. Polo tanto,

$$a_{n+1} = 2a_n - a_{n-1} = 4n + 2 - (2n-1) = 2n+3;$$

observamos que aquí é preciso comprobar os casos a_0 e a_1, dado que empregamos como hipótese de indución os dous valores anteriores.

2.3. O teorema do binomio de Newton

Definición 2.3. Sexa n un enteiro positivo. Defínese o *factorial* de n como

$$n! = n(n-1)\cdots 2 \cdot 1.$$

Por convención, consideraremos que $0! = 1$.
Se $n \geq k \geq 0$ definimos *o número combinatorio ou binomial n sobre k*, $\binom{n}{k}$, como

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Os números combinatorios cumpren diferentes relacións entre eles. Por exemplo, se $n \geq k \geq 1$,

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Estes números tamén aparecen ao desenvolver potencias de certas sumas. Por exemplo:

$$\begin{aligned}(a+b)^2 &= a^2 + 2ab + b^2\\ (a+b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3\\ (a+b)^4 &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.\end{aligned}$$

Máis en xeral, tense o seguinte resultado, cuxa demostración se realiza por indución.

Proposición 2.4. Sexan $a, b \in \mathbb{R}$ e $n \geq 1$. Entón,

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.$$

Antes de realizar a demostración, imos ilustrar como realizar o paso indutivo para pasar de $n = 3$ a $n+1 = 4$. Supoñamos que sabemos xa que

$$(a+b)^3 = \binom{3}{0}a^3 + \binom{3}{1}a^2b + \binom{3}{2}ab^2 + \binom{3}{3}b^3.$$

Entón,

$$\begin{aligned}(a+b)^4 &= (a+b)^3(a+b)\\ &= \Big(\binom{3}{0}a^3 + \binom{3}{1}a^2b + \binom{3}{2}ab^2 + \binom{3}{3}b^3\Big)(a+b)\\ &= \binom{3}{0}a^4 + \binom{3}{1}a^3b + \binom{3}{2}a^2b^2 + \binom{3}{3}ab^3\\ &+ \binom{3}{0}a^3b + \binom{3}{1}a^2b^2 + \binom{3}{2}ab^3 + \binom{3}{3}b^4\\ &= \binom{4}{0}a^4 + \binom{4}{1}a^3b + \binom{4}{2}a^2b^2 + \binom{4}{3}ab^3 + \binom{4}{4}b^4.\end{aligned}$$

No último paso empregamos dous feitos: por un lado, que $\binom{3}{0} = \binom{4}{0} = 1$, e que $\binom{3}{3} = \binom{4}{4} = 1$; por outro, que $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$, o que nos permite dicir que $\binom{3}{1} + \binom{3}{0} = \binom{4}{1}$, $\binom{3}{2} + \binom{3}{1} = \binom{4}{2}$ e $\binom{3}{3} + \binom{3}{2} = \binom{4}{3}$.

Demostración. Para $n = 1$ o resultado é inmediato, xa que

$$(a+b)^1 = \binom{1}{0}a + \binom{1}{1}b.$$

Supoñámolo certo para n, isto é, a igualdade

$$(a+b)^n = \sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i$$

será a hipótese de indución. Demostrémolo agora para $n+1$:

$$\begin{aligned}(a+b)^{n+1} &= (a+b)(a+b)^n\\ &= (a+b)\Big(\sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i\Big)\\ &= a^{n+1} + b^{n+1} + \sum_{i=1}^{n}\Big(\binom{n}{i} + \binom{n}{i-1}\Big)a^{n+1-i}b^i\\ &= \sum_{i=0}^{n+1}\binom{n+1}{i}a^{n+1-i}b^i,\end{aligned}$$

onde despois da segunda igualdade separamos os termos a^{n+1} e b^{n+1}; na terceira igualdade agrupamos os termos que acompañan a $a^{n+1-i}b^i$; e na cuarta empregamos que $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. □

Os números binomiais adoitan representarse no chamado *triángulo de Tartaglia* ou *triángulo de Pascal*.

$$\begin{array}{ccccccccccc}
 & & & & \binom{0}{0} & & & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
 & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5}
\end{array}$$

Cambiando os binomiais por números, temos o seguinte:

$$\begin{array}{ccccccccccc}
 & & & & 1 & & & & & & \\
 & & & 1 & & 1 & & & & & \\
 & & 1 & & 2 & & 1 & & & & \\
 & 1 & & 3 & & 3 & & 1 & & & \\
1 & & 4 & & 6 & & 4 & & 1 & & \\
1 & & 5 & & 10 & & 5 & & 1 & & 1
\end{array}$$

2.4. Outros métodos de demostración

Coñécese como *redución ao absurdo* (*reductio ad absurdum*) o método de demostración que se basea en demostrar que unha proposición é verdadeira, probando que se non o fose conduciría a unha contradición, polo que debe ser certa.

Exemplo. Sexa p un número primo. Entón, $\sqrt{p}$ é un número irracional. Procedemos por redución ao absurdo e supomos que $\sqrt{p} = \frac{a}{b}$ é racional, onde $a, b \in \mathbb{Z}$. Polo tanto, $\sqrt{p}b = a$; elevando ao cadrado, $pb^2 = a^2$. Consideramos a factorización de a e b en factores primos, e illamos o primo p:

$$a = p^{\alpha} p_1^{a_1} \cdots p_m^{a_m}, \quad b = p^{\beta} q_1^{b_1} \cdots q_m^{b_m},$$

onde os p_i e os q_i son distintos de p. Entón,

$$p^{2\beta+1} q_1^{b_1} \cdots q_m^{b_m} = p^{2\alpha} p_1^{a_1} \cdots p_m^{a_m},$$

e igualando os expoñentes de p, quédanos que $2\beta + 1 = 2\alpha$, o cal é unha contradición. No caso concreto no que $p = 2$, a factorización que estamos considerando para a e b e simplemente escribir $a = 2^{\alpha} r$ e $b = 2^{\beta} s$, con r e s impares; isto é, cada número estámolo separando na súa parte par e na súa parte impar, e tratando cada unha delas de xeito independente.

Coñécese como *demostración por contrarrecíproco* a demostrar que A implica B establecendo que se B é falso, entón A necesariamente tamén.

Exemplo. Sexa n un número enteiro. Se $5n + 3$ é par, entón n é impar. Procedemos por contrarrecíproco. Se n é par, $n = 2k$, entón

$$5n + 3 = 5(2k) + 3 = 10k + 3 = 2(5k + 1) + 1,$$

polo cal $5n + 3$ é impar.

En xeral, existen moitos outros métodos de demostración, que iremos traballando en próximos temas.

Capítulo 3

Aritmética

A aritmética, tamén coñecida como teoría de números, é unha das áreas da matemática con máis tradición histórica. Desde a Antiga Grecia, as cuestións relativas aos números primos ou ás chamadas ecuacións diofantianas ocuparon un lugar destacado no estudo das ciencias. O obxectivo deste tema é presentar as cuestións básicas de divisibilidade e congruencias, ata chegar a outras cuestión máis avanzadas relativas ás raíces primitivas ou aos restos cuadráticos.

3.1. Divisibilidade

Imos comezar establecendo o resultado que garante que dados dous números enteiros a, b, con $b \neq 0$, sempre podemos dividir a por b obtendo un resto que sexa menor que b en valor absoluto.

Proposición 3.1 (Algoritmo da división euclidiana)**.** Sexan $a, b \in \mathbb{Z}$, con $b \neq 0$. Existen enteiros q e r únicos de xeito que

$$a = bq + r, \quad 0 \leq r < |b|.$$

Demostración. Imos comezar vendo a existencia, supondo en primeiro lugar que $b > 0$. Consideramos os conxuntos

$$S = \{a - bx \mid x \in \mathbb{Z}\}, \quad S_0 = \{n \in S \mid n \geq 0\}.$$

Imos demostrar que S_0 é non baleiro. Se $a \geq 0$, entón, como $a = a - b \cdot 0 \in S$, temos que $a \in S_0$. Se $a < 0$, como $b > 0$, temos que $b \geq 1$ e, polo tanto, $1 - b \leq 0$; como $a - ba = a(1 - b) \geq 0$, temos que $a - ba \in S_0$. Como o conxunto é non baleiro, ten mínimo; podemos chamarlle $r \geq 0$, e sexa q de xeito que $a = bq + r$. É suficiente con ver que $r < b$. Se $r \geq b$, entón $0 \leq r - b < r$ e

$$r - b = a - bq - q = a - b(q + 1) \in S,$$

polo que $r - b$ é un elemento de S_0 menor que r, o que é unha contradición coa definición de r. Polo tanto, $0 \leq r < b = |b|$.
Se $b < 0$, entón $-b > 0$. Polo caso anterior, existen q e r con $a = (-b)q + r = b(-q) + r$ e $0 \leq r < |b|$. Neste caso, $-q$ e r cumpren as propiedades.
Finalmente, para ver a unicidade, se

$$a = bq_1 + r_1 = bq_2 + r_2,$$

podemos supor que $0 \leq r_1 \leq r_2 < |b|$. Temos que $b(q_1 - q_2) = r_2 - r_1 < |b|$. Como $0 \leq r_2 - r_1 = b(q_1 - q_2)$, entón $q_1 = q_2$. De aquí é inmediato que $r_2 - r_1 = 0$. □

Exemplo. Se $a = 22$ e $b = 5$, temos que $22 = 5 \cdot 4 + 2$. Se $a = 22$ e $b = -5$, temos que $22 = (-5)(-4) + 2$. Se $a = -22$ e $b = 5$, entón

$$-22 = 5(-4) - 2 = 5(-4) - 2 + 5 - 5 = 5(-5) + 3.$$

O seguinte resultado é unha aplicación do algoritmo da división euclidiana, que afirma que cada número admite unha representación única nunha certa base $b \geq 2$.

Proposición 3.2. Sexa $b \geq 2$ un enteiro. Para todo enteiro $n \geq 0$ existen enteiros $a_0, \ldots, a_k$ únicos de xeito que

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0, \quad 0 \leq a_0, \ldots, a_k < b, \quad a_k \neq 0.$$

Demostración. Para demostrar a existencia, procedemos por indución sobre n. Se $n < b$, collemos $k = 0$ e $a_0 = n$. Se $n \geq b$, sexan q_0 e a_0 o cociente e o resto de dividir n por b, respectivamente, de xeito que $n = bq_0 + a_0$, con $a_0 < b$ e $q_0 < n$. Por hipótese de indución $q_0 = a_k b^{k-1} + \ldots + a_1$. Polo tanto,

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0.$$

Para ver a unicidade, temos que a_0 é o resto de dividir n por b e que o cociente é $q_0 = a_k b^{k-1} + \ldots + a_1$; deste xeito a_1 é o resto de dividir q_0 por b é o cociente é $q_1 = a_k b^{k-1} + \ldots + a_2$. En xeral, $q_i = a_k b^{k-i} + \ldots + a_i$ é o cociente e a_{i-1} é o resto de dividir q_{i+1} por b. □

Este resultado permite traballar en diferentes bases. En casos de ambigüidade, empregamos un subíndice para indicar a base.

Exemplo. O número 13 exprésase como $(1101)_2$ en base 2, xa que $13 = 2^3 + 2^2 + 2^0$. En base 3 escríbese como $(111)_3$, xa que $13 = 3^2 + 3^1 + 3^0$. En base 4 escríbese como $(31)_4$, xa que $13 = 3 \cdot 4 + 1$.

Por comodidade, cando traballamos en bases superiores a 10 e precisamos máis díxitos, adoitamos empregar as letras do alfabeto. Deste xeito, o número 10 escríbese como A en base 11, ou o número 12 correspóndese coa C en base 16. A base 16, tamén chamada *hexadecimal*, é moi frecuente en sistemas de numeración relacionados coa informática, e involucra ás letras A, B, C, D, E e F. Por exemplo, o número $(EAB)_{16}$ correspóndese co $14 \cdot 16^2 + 10 \cdot 16 + 11 = 3755$.

Exemplo. O número $(1010111101)_2$ correspóndese co

$$(1 \cdot 2) \cdot (2^4)^2 + (1 \cdot 2^3 + 1 \cdot 2 + 1) \cdot 2^4 + (1 \cdot 2^3 + 1 \cdot 2^2 + 1) = 2 \cdot 16^2 + 11 \cdot 16 + 13,$$

polo que en base 16 é $(1BD)_{16}$. De xeito similar, o número $(C91)_{16}$ correspóndese co $(110010010001)_2$ en base 2. É dicir, como $16 = 2^4$, pasar de base 2 a 16, e viceversa, e especialmente sinxelo.

Unha noción central no estudo da aritmética é a de número primo.

Definición 3.1. Un enteiro p dise que é *primo* se $p > 1$ e, para todo $a, b \in \mathbb{Z}$, se $p \mid (ab)$ e $p \nmid a$, entón $p \mid b$.

A seguinte proposición dá unha caracterización alternativa do que é ser un número primo; é o que xeralmente se coñece como *irredutible*, pero que no contexto dos números enteiro son equivalentes.

Proposición 3.3. Un enteiro $p > 1$ é primo se, e soamente se, os únicos divisores positivos de p son el mesmo e o 1.

Demostración. Supoñamos que p é primo e sexa d un divisor de p, de xeito que $p = dd'$, con $d, d' \in \mathbb{Z}$ maiores que 0; en particular, $d, d' \leq p$. Neste caso, $p \mid dd'$, polo que, ou $p \mid d$ ou $p \mid d'$. Se $p \mid d$, entón $p \leq d$; e, en caso contrario, $p \leq d'$. Cúmprese entón que $p = d$ ou que $p = d'$, polo que o outro é 1.
Supoñamos agora que os únicos divisores son o 1 e p. Entón, se $p \mid ab$ e $p \nmid a$, necesariamente sucede que $\gcd(p, a) = 1$. Como $p \mid (ab)$ e $\gcd(p, a) = 1$, tense que cumprir que $p \mid b$. □

De aquí observamos que todo enteiro $n \geq 2$ ten un divisor primo. Isto vese por indución: $n = 2$ ten o divisor primo 2. Se $n > 2$ é primo acabamos; senón, ten un divisor positivo d con $1 < d < n$. Por hipótese de indución d ten un divisor primo, que tamén é entón un divisor de n.

Proposición 3.4. Existen infinitos números primos.

Demostración. Imos proceder por redución ao absurdo. Supoñamos que só hai un número finito, $p_1, \ldots, p_k$. Sexa

$$N = p_1 \cdots p_k + 1.$$

O número N non pode ser divisible por ningún dos p_i xa que, como $1 = N - p_1 \cdots p_k$, se dividise a N tamén dividiría á diferenza e polo tanto a 1, que non é posible. Polo tanto, temos un número maior que 1 que non ten ningún factor primo, o cal é unha contradición. □

O seguinte resultado, que se coñece como *teorema fundamental da aritmética*, establece que todo número descompón de xeito único como produto de factores primos.

Proposición 3.5 (Teorema fundamental da aritmética)**.** Se $n \neq 0, 1$ é un enteiro, existen $u \in \{\pm 1\}$, enteiros primos $p_1 < \ldots < p_k$ e enteiros positivos $\alpha_1, \ldots, \alpha_k$ únicos de xeito que

$$n = u p_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$

Demostración. Comezamos coa situación na que n é un enteiro positivo. Para establecer a existencia, chega con ver que todo enteiro $n \geq 2$ é produto de primos, o que se pode ver por indución. Se $n = 2$ é obvio. Se $n > 2$ e n é primo, tamén é obvio. Senón, n ten un divisor primo p e, por indución, sabemos que n/p é produto de primo. Polo tanto, $n = p(n/p)$ é produto de primos.
Para ver a unicidade, sexa $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = q_1^{\beta_1} \cdots q_s^{\beta_s}$, onde os p_i e os q_j son primos con $p_1 < \cdots < p_r$ e $q_1 < \cdots < q_s$. Procedemos de novo por indución sobre n, sendo obvio para $n = 2$. Como $q_1 \mid p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, sabemos que $q_1 \mid p_i$ para algún i. Como q_1 e p_i son primos, temos que $q_1 = p_i$. Do mesmo xeito, existe j de xeito que $p_1 = q_j$. Polo tanto, $q_1 = p_i \geq p_1 = q_j \geq q_1$, polo que $p_1 = q_1$. Simplificando un factor $p_1 = q_1$ e empregando a hipótese de indución para n/p_1 obtemos que $r = s$, $p_i = q_i$ e $\alpha_i = \beta_i$.
Se $n < 0$, entón a existencia e unicidade da factorización de $-n$ implica a de n. □

En xeral, achar números primos é un problema difícil. Un procedemento sinxelo que se emprega para ese propósito é a *criba de Eratóstenes*, un algoritmo que permite achar tódolos números primos menores que un certo natural. Fórmase unha táboa con tódolos números naturais entre 2 e n, e vanse tachando todos os que non son primos como segue: comézase polo 2 e táchanse tódolos seus múltiplos; vólvese comezar, agora co seguinte primo, e cando se atopa un múltiplo seu que aínda non foi tachado, o número declárase composto. Cando se atopa un enteiro que non foi tachado, ese número considérase primo. O proceso remata cando o cadrado do seguinte número confirmado como primo é maior que n.
A distribución dos números primos é unha das cuestións que máis preocupou historicamente aos matemáticos. Por exemplo, non se sabe se existen infinitas parellas $(n, n+2)$ de xeito que ambos sexan primos; son os chamados *primos xemelgos*. En cambio, si é doado demostrar que existen cadeas de enteiros positivos arbitrariamente longas de xeito que ningún deles sexa primo.

Exemplo. Sexa $k > 1$ un enteiro positivo. Entón, os números $(k+1)! + 2, (k+1)! + 3, \ldots (k+1)! + (k+1)$ non poden ser primos, xa que $(k+1)! + i$ sempre é múltiplo de i, para todo $2 \leq i \leq k+1$, por tratarse da suma de dous números que son múltiplos de i.

3.2. Algoritmo de Euclides e identidade de Bézout

Definición 3.2. Sexan a e b dous números enteiros de xeito que non son ambos iguais a cero. Un enteiro positivo d é un *máximo común divisor* de a e de b se é un divisor de ambos e se, no caso no que c é un enteiro que tamén os divide a ambos, entón $c \mid d$. Se $a = b = 0$, defínese o máximo común divisor como 0.

Proposición 3.6. Sexan a e b dous números enteiros. Entón existe un único máximo común divisor d de a e de b. Escribimos $d = \gcd(a, b)$ (polas siglas en inglés, *greatest common divisor*).

Demostración. Se $a = b = 0$ é evidente. Supoñamos que non son ambos cero. Sexa $S = \{ax + by \mid x, y \in \mathbb{Z}\}$. Como os números $a, b, -a, -b \in S$ e algún é positivo, o conxunto S^+ dos elementos positivos de S é non baleiro. Sexa d o mínimo de S^+, e sexan $x, y \in \mathbb{Z}$ de xeito que $d = ax + by$. Polo algoritmo da división euclidiana, sabemos que existen $q, r \in \mathbb{Z}$ de xeito que $a = dq + r$, con $0 \leq r < d$. Se $r > 0$, entón r sería un elemento de S^+ menor que d, que é unha contradición. Polo tanto, $r = 0$ e $d \mid a$. De xeito similar, $d \mid b$.
Por último, sexa c un divisor de a e de b, de xeito que $a = cu$ e $b = cv$. Entón,

$$d = ax + by = cux + cvy = c(ux + vy),$$

de onde se ten que $c \mid d$.
Para ver a unicidade, supoñamos que d_1 e d_2 dous máximos comúns divisores de a e de b. De aquí temos que $d_1 \mid d_2$ e $d_2 \mid d_1$, polo que $d_1 = d_2$. □

Porén, o resultado anterior non proporciona unha maneira de achalo. Ao longo desta sección exploraremos dúas maneiras de facelo: en termos da factorización ou empregando o chamado *algoritmo de Euclides*. Porén, imos introducir primeiro unha noción similar, que é a do mínimo común múltiplo.

Definición 3.3. Sexan a e b dous enteiros que non son ambos ceros. Un *mínimo común múltiplo* de a e de b é un enteiro positivo que é múltiplo de ambos e que, se c é un enteiro positivo tal que é múltiplo de a e de b, entón tamén é múltiplo de m.

Proposición 3.7. Sexan a e b dous números enteiros. Entón existe un único máximo común divisor m de a e de b. Escribimos $m = \operatorname{lcm}(a, b)$ (polas siglas en inglés, *least common multiple*). Se $a = b = 0$, defínese como 0.

Demostración. Se $a = b = 0$ é obvio. Supoñamos entón que un deles é non cero e, reemprazando un número polo seu oposto, podemos supoñer tamén que $a, b \geq 0$.
Sexa $d = \gcd(a, b)$, e sexa $a = da'$ e $b = db'$. Observamos que o número $m = da'b'$ é múltiplo de a e de b. Sexa $c = ar = bs$ outro múltiplo común de a e de b, de xeito que $da'r = db's$. Dividindo a última igualdade por d, que sabemos que é distinto de 0, temos que $a'r = b's$, onde $\gcd(a', b') = 1$. Polo tanto, $a' \mid s$, polo que $s = a'h$. Polo tanto, $c = bs = ba'h = dha'b'$ é múltiplo de $m = da'b'$, co cal temos que m é un mínimo común múltiplo.
A unicidade é inmediata, igual que no caso do máximo común divisor. □

Podemos observar que se $a = \prod_{i=1}^{r} p_i^{k_i}$ e $b = \prod_{i=1}^{r} p_i^{\ell_i}$, entón

$$\gcd(a, b) = \prod_{i=1}^{r} p_i^{\text{mín}(a_i, b_i)}, \quad \operatorname{lcm}(a, b) = \prod_{i=1}^{r} p_i^{\text{máx}(a_i, b_i)}.$$

É dicir, é especialmente doado achar o mínimo común múltiplo ou o máximo común divisor de dous números coñecendo a súa factorización. Porén, cando os números son grandes, factorizalos é un proceso custoso desde un punto de vista algorítmico. Por iso, hai alternativas máis eficientes para o cálculo do máximo común divisor, empregando unicamente a división euclidiana e sen factorizar ningún dos números. O resultado clave para iso é a seguinte proposición.

Proposición 3.8. Se a, b, q e r son enteiros e $a = bq + r$, entón $\gcd(a, b) = \gcd(b, r)$.

Demostración. A condición é equivalente a $r = a - bq$. Sexa $d_1 = \gcd(a, b)$ e $d_2 = \gcd(b, r)$. Comezamos observando que $d_1 = 0$ se, e soamente se, $a = b = 0$, que é equivalente a $b = r = 0$ e isto, á súa vez, pasa se, e soamente se, $d_2 = 0$. Polo tanto, supoñamos que tanto d_1 como d_2 son non 0. Como d_1 divide a e b, divide b e $r = a - bq$. Polo tanto, $d_1 \mid d_2$. Como d_2 divide b e r, tamén divide b e $a = bq + r$. Polo tanto, $d_2 \mid d_1$. Deste xeito, $d_1 = \pm d_2$; pero, como ambos son positivos, tense que $d_1 = d_2$. □

O algoritmo de Euclides permite achar o máximo común divisor de dous números a e b, con $a \geq b$. Para iso, definimos sucesións (a_n), (b_n), (q_n) e (r_n) do seguinte xeito.

- Os termos iniciais son $a_1 = a$, $b_1 = b$ e (q_1, r_1) son o cociente e o resto da división euclidiana de a por b.
- Para $k \geq 2$, procedemos como segue: se r_{k-1} rematamos o proceso e as sucesións teñen $k - 1$ termos. En caso contrario, $a_k = b_{k-1}$, $b_k = r_{k-1}$ e (q_k, r_k) son o cociente e o resto da división euclidiana de a_k por b_k.
- Se o proceso rematou con n termos en cada sucesión, o máximo común divisor é b_n.

Proposición 3.9. O algoritmo anterior remata e obtén o máximo común divisor dos números a e b.

Ademais, o algoritmo de Euclides permite expresar o máximo común divisor d como combinación lineal de a e de b, é dicir, atopar números enteiros a e b de xeito que

$$ax + by = \gcd(a, b).$$

Para iso, procedemos do seguinte xeito.

1. Se a é múltiplo de b, o máximo común divisor é b, polo que se ten que $a \cdot 0 + b \cdot 1 = 1$.
2. En caso contrario, temos que o máximo común divisor é r_{n-1}, polo que se ten que
$$d = r_{n-1} = a_{n-1} - q_{n-1} b_{n-1}.$$
3. Iterativamente, podemos ir escribindo d en termos de (a_i, b_i). Se temos unha expresión para (a_{i+1}, b_{i+1}), observamos que $a_{i+1} = b_i$ e $b_{i+1} = r_i = a_i - q_i b_i$.

Exemplo. Consideramos os números $a = 200$ e $b = 34$. Aplicando o algoritmo de Euclides, temos

$$\begin{aligned} 200 &= 34 \cdot 5 + 30 \\ 34 &= 30 \cdot 1 + 4 \\ 30 &= 4 \cdot 7 + 2 \\ 4 &= 2 \cdot 2. \end{aligned}$$

Polo tanto, o máximo común divisor é 2. Ademais, o algoritmo permítenos expresar 2 como combinación lineal de 200 e 34:

$$\begin{aligned} 2 &= 30 - 7 \cdot 4 \\ &= 30 - 7 \cdot (34 - 1 \cdot 30) \\ &= -7 \cdot 34 + 8 \cdot 30 \\ &= -7 \cdot 34 + 8 \cdot (200 - 5 \cdot 34) \\ &= 8 \cdot 200 - 47 \cdot 34. \end{aligned}$$

Proposición 3.10. Sexan $a, b, c \in \mathbb{Z}$. A ecuación

$$ax + by = c$$

ten solución se, e soamente se, c é un múltiplo de $\gcd(a, b)$.

Demostración. Sexa $d = \gcd(a, b)$. Se $d \nmid c$, observamos que $ax+by$ sempre será múltiplo de d, pois sono tanto a como b. Deste xeito, o lado esquerdo é múltiplo de d, mentres que o dereito non o é, o que é unha contradición.
Se $c = d$, pola identidade de Bézout, sabemos que hai unha solución $ax' + by' = d$. Se $c = \lambda d$, chega con coller $x = \lambda x'$ e $y = \lambda y'$. □

Exemplo. A ecuación $12x + 9y = 1$ non ten solución, xa que $\gcd(12, 9) = 3$ e 1 non é múltiplo de 3. En cambio, $12x + 9y = 6$ **si** ten solución. Aplicando a identidade de Bézout, chegamos a

$$12 \cdot 1 + 9 \cdot (-1) = 3;$$

como $6 = 3 \cdot 2$, multiplicando por 2 a ecuación anterior obtemos

$$12 \cdot 2 + 9 \cdot (-2) = 6.$$

Outra pregunta natural ten que ver con atopar tódalas solucións dunha ecuación diofantiana. Por exemplo, a ecuación $9x + 7y = 1$ ten a solución $(4, -5)$; pero, a partir dunha, é posible atopalas todas? Sexan (x_1, y_1) e (x_2, y_2) dúas solucións da ecuación. Polo tanto,

$$\begin{cases} 9x_1 + 7y_1 = 1 \\ 9x_2 + 7y_2 = 1. \end{cases}$$

Restando, quédanos que $9(x_1 - x_2) = 7(y_2 - y_1)$; como 7 e 9 son coprimos, é inmediato ver que

$$x_1 - x_2 = 7k, \quad 7y_2 - y_1 = 9k, \quad \text{para algún } k \in \mathbb{Z}.$$

Polo tanto, concluímos que $(x_2, y_2) = (x_1 - 7k, x_2 + 9k)$. Este procedemento é xeral e pódese resumir na seguinte proposición.

Proposición 3.11. Sexa $ax + by = c$, onde $\gcd(a, b) \mid c$. Consideremos unha solución (x_0, y_0) da ecuación. Nese caso, calquera outra solución (x, y) pódese expresar como

$$(x, y) = \left(x_0 - \frac{bk}{\gcd(a, b)}, y_0 + \frac{ak}{\gcd(a, b)} \right), \quad k \in \mathbb{Z}.$$

Demostración. O resultado séguese de restar as ecuacións

$$\begin{cases} ax_0 + by_0 = c \\ ax + by = c \end{cases}$$

e aplicar un argumento de divisibilidade. □

En relación aos divisores dun número, existen diferentes funcións importantes involucradas no seu estudo.

Definición 3.4. Sexa $n = p_1^{a_1} \cdots p_k^{a_k}$. Para calquera $r \geq 0$, definimos

$$\sigma_r(n) = \sum_{d \mid n} d^r,$$

isto é, a suma dos divisores de d elevados á potencia r-ésima. Cúmprese que

$$\tau(n) := \sigma_0(n) = (a_1 + 1) \cdots (a_k + 1)$$

e

$$\sigma(n) := \sigma_1(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{a_k+1} - 1}{p_k - 1}.$$

Dicimos que un número é *perfecto* se $\sigma(n) = 2n$.

Non se sabe se existen infinitos números perfectos ou non; a data 2018, coñecíanse 51 números perfectos: os menores son o 6, o 28, o 496 e o 8128.
Por outra banda, as funcións $\sigma_k(n)$ son *debilmente multiplicativas*, é dicir $\sigma_r(mn) = \sigma_r(m)\sigma_r(n)$ se $\gcd(m, n) = 1$.

Exemplo. Temos que $60 = 2^2 \cdot 3 \cdot 5$. Polo tanto, 60 ten 12 divisores xa que

$$\sigma(60) = (2 + 1)(1 + 1)(1 + 1) = 12,$$

e no referente á suma, os divisores suman 168, xa que

$$\tau(60) = 7 \cdot 4 \cdot 6 = 168.$$

Exemplo. Sexa p un número primo de xeito que $2^p - 1$ tamén é primo (por exemplo, $p = 2$, $p = 3$ ou $p = 5$). Entón,

$$\sigma(2^{p-1}(2^p - 1)) = \frac{2^p - 1}{2 - 1} \cdot \frac{(2^p - 1)^2 - 1}{2^p - 2} = 2^p(2^p - 1),$$

polo que o número $2^{p-1}(2^p - 1)$ é perfecto. Porén, non se sabe se existen infinitos números primos da forma $2^p - 1$.

3.3. Congruencias

Se n é un enteiro, denotamos por $n\mathbb{Z}$ o conxunto dos enteiros múltiplos de n, isto é

$$n\mathbb{Z} = \{nq \colon q \in \mathbb{Z}\}.$$

Definición 3.5. Sexa n un enteiro. Dous enteiros x, y dise que son *congruentes módulo* n se $x - y$ é un múltiplo de n. Escríbese $x \equiv y \pmod{n}$.

Unha comprobación rutineira amosa que a relación de congruencia módulo n é unha relación de equivalencia; escribimos $\mathbb{Z}/n\mathbb{Z}$ para o conxunto cociente; tamén é frecuente empregar a notación $\mathbb{Z}_n$, aínda que aquí nunca se utilizará. Facendo un pequeno abuso de notación, denotamos por $0, 1, \ldots, n - 1$ os elementos de $\mathbb{Z}/n\mathbb{Z}$, entendendo que i se refire á clase de equivalencia do número enteiro i no conxunto cociente.

Proposición 3.12. Sexa $n > 0$ un enteiro. Son equivalentes:

(i) $x \equiv y \pmod{n}$.

(ii) x e y teñen o mesmo resto ao dividir por n.

Proposición 3.13. Sexa $n \geq 0$ un enteiro. Para $a, b, a', b' \in \mathbb{Z}$, se $a \equiv a' \pmod{n}$ e $b \equiv b' \pmod{n}$, entón $a + b \equiv a' + b' \pmod{n}$ e $ab \equiv a'b' \pmod{n}$.

Imos empregar agora o algoritmo de Euclides e a identidade de Bézout para determinar que números admiten inverso módulo n, describindo un método para atopalo.

Proposición 3.14. Sexan n e a enteiros, con $n \geq 1$. Entón, existe un enteiro b de xeito que $ab \equiv 1 \pmod{n}$ se, e soamente se, $\gcd(a, n) = 1$. Dise que b é o *inverso de a módulo n*, e escríbese a^{-1}.

A seguinte táboa amosa a multiplicación módulo 7.

$\times_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Obsérvase, por exemplo, que tódolos números salvo o 0 teñen inverso; o 1 e o 6 son inversos deles mesmos; o 2 é inverso do 4 e viceversa; e o 3 é inverso do 5 e viceversa.

Definición 3.6. O conxunto de elementos que teñen inverso módulo n denótase por $(\mathbb{Z}/n\mathbb{Z})^\times$.

Exemplo. Módulo 10, 3 é o inverso de 7, xa que $3 \cdot 7 \equiv 1 \pmod{10}$. Pomos $7^{-1} \equiv 3 \pmod{10}$. Do mesmo xeito, 9 é o seu propio inverso, xa que $9 \cdot 9 \equiv 1 \pmod{10}$ ou, alternativamente, $(-1) \cdot (-1) \equiv 1 \pmod{10}$. O número 4 non ten inverso módulo 10, xa que $4x$ sempre é par polo que, en particular, non pode ser 1 módulo 10.

Corolario 3.1. Sexan n, a, b e c enteiros, con $n \geq 1$.

(a) Se $ac \equiv bc \pmod{n}$ e $\gcd(c, n) = 1$, entón $a \equiv b \pmod{n}$.

(b) Se $ac \equiv bc \pmod{n}$ e $\gcd(c, n) = d$, entón $a \equiv b \pmod{n/d}$.

Proposición 3.15. A ecuación

$$ax \equiv b \pmod{n}$$

ten unha única solución módulo n se, e soamente se, $\gcd(a, n) = 1$. En caso contrario, sexa $d = \gcd(a, n)$. A ecuación ten solución se, e soamente se, $d \mid b$, e nese caso ten d solucións.

Demostración. Se $\gcd(a, n) = 1$, entón multiplicamos a cada lado da ecuación polo inverso de a módulo n e o resultado é inmediato. Se $d = \gcd(a, n) > 1$, entón é necesario que b sexa múltiplo de d, xa que en caso contrario o lado esquerdo da congruencia sempre sería múltiplo de d é o dereito non podería selo. De ser o caso, a congruencia é equivalente a $(a/d)x \equiv b/d \pmod{n/d}$, que ten unha única solución porque a/d e n/d son relativamente primos. Dúas solucións calquera difiren nun múltiplo de n/d, polo que hai d solucións en total. □

Exemplo. A ecuación $7x \equiv 12 \pmod{19}$ ten unha única solución xa que $\gcd(19, 7) = 1$. Aplicando a identidade de Bézout, temos que $7 \cdot (-8) + 19 \cdot 3 = 1$, polo que o $-8 \equiv -8 + 19 \equiv 11 \pmod{19}$ é o inverso de 7 módulo 19. Polo tanto,

$$x \equiv 7^{-1} \cdot 12 \equiv 11 \cdot 12 \equiv 18 \pmod{19}.$$

Por outra banda, a ecuación $7x \equiv 12 \pmod{20}$ tamén ten unha única solución, xa que $\gcd(20, 7)$. Neste caso, o inverso de 3 módulo 20 é 7, polo que

$$x \equiv 7^{-1} \cdot 12 \equiv 3 \cdot 12 \equiv 16 \pmod{20}.$$

Porén, a ecuación $5x \equiv 12 \pmod{20}$ non ten solución, xa que $\gcd(5, 20) = 5$ e 5 non é un divisor de 12. Se consideramos en cambio a ecuación $5x \equiv 15 \pmod{20}$ si ten solución, aínda que non é única. A ecuación pódese reinterpretar como $5x + 20y = 15$, ou, o que é o mesmo, $x + 4y = 3$, que equivale a $x \equiv 3 \pmod{4}$. Polo tanto, as solucións módulo 20 virán dadas por tódalas clases que sexan congruentes con 3 módulo 4; isto é, as 5 clases

$$x \equiv 3 + 4k \pmod{20}, \quad k = 0, 1, 2, 3, 4.$$

Exemplo. A ecuación $18x \equiv 7 \pmod{60}$ non ten solución, xa que $18x$ sempre será par e, en particular, non pode dar resto 7 ao dividir por 60. A ecuación $18x \equiv 12 \pmod{60}$ si ten solución; como $\gcd(18, 60) = 6$, é equivalente a $3x \equiv 2 \pmod{10}$, cuxas solucións cumpren $x \equiv 3^{-1} \cdot 2 \equiv 4 \pmod{10}$. Polo tanto, hai 6 solucións módulo 60, que se corresponden con tódalas clases que dan resto 4 ao dividir por 10: 4, 14, 24, 34, 44 e 54.

Imos estudar agora os criterios de divisibilidade polos números menores que 11. Escribindo n en base 10, temos

$$n = a_k \cdot 10^k + \ldots + a_1 \cdot 10 + a_0.$$

- O número n é divisible por 2 se, e soamente se, a_0 é par.
- O número n é divisible por 3 se, e soamente se, $a_0 + a_1 + \ldots + a_k$ é múltiplo de 3.
- O número n é divisible por 4 se, e soamente se, o número formada polas dúas últimas cifras é múltiplo de 4.
- O número n é divisible por 5 se, e soamente se, a_0 é 0 ou 5.
- O número n é divisible por 8 se, e soamente se, o número formada polas dúas últimas cifras é múltiplo de 7.
- O número n é divisible por 9 se, e soamente se, $a_0 + a_1 + \ldots + a_k$ é múltiplo de 9.

O caso do 7 é máis sutil. Temos que $10^0 \equiv 1$, $10^1 \equiv 3$, $10^2 \equiv 2$, $10^3 \equiv 6$, $10^4 \equiv 4$, $10^5 \equiv 5$, e a partir de aí a sucesión repítese periodicamente. Polo tanto, a condición é que

$$a_0 + 3a_1 + 2a_2 + 6a_3 + 4a_4 + 5a_5 + a_6 + \ldots$$

sexa múltiplo de 7. Alternativamente, podemos facer o seguinte: escribimos $n = 10a+b$, onde $b \in \{0, 1, \ldots, 9\}$. Entón, tense que n é múltiplo de 7 se, e soamente se, $a - 2b$ é múltiplo de 7. Este método é máis xeral.

Proposición 3.16. Sexa c o inverso dun número primo p módulo 10. Entón, $n = 10a+b$ é múltiplo de p se, e soamente se, $a + cb$ é múltiplo de p.

O resultado anterior pódese estender, máis en xeral, para números enteiros que sexan coprimos con 10.

Exemplo. Sexa $n = 10a + b$ un enteiro.

- n é múltiplo de 7 se, e soamente se, $a - 2b$ é múltiplo de 7, xa que $10 \cdot (-2) \equiv 1$ (mód 7).
- n é múltiplo de 13 se, e soamente se, $a + 4b$ é múltiplo de 13, xa que $10 \cdot 4 \equiv 1$ (mód 13).
- n é múltiplo de 17 se, e soamente se, $a - 5b$ é múltiplo de 17, xa que $10 \cdot (-5) \equiv 1$ (mód 17).
- n é múltiplo de 19 se, e soamente se, $a + 2b$ é múltiplo de 19, xa que $10 \cdot 2 \equiv 1$ (mód 19).

3.4. Resultados sobre congruencias

Un dos resultados máis antigos relativos ás congruencias é o coñecido como teorema chinés dos residuos. O primeiro enunciado aparece a modo de problema con números concretos no libro do século V *Sunzi Suanjing*, escrito polo matemático chinés Sunzi. Nel pregunta o seguinte: *Temos varios obxectos, pero o seu número é descoñecido. Se os*

contamos en grupos de tres, sóbranme dous; se os contamos en grupos de cinco, entón sobran tres; e se os contamos en grupos de sete, sobran dous. Cantos obxectos hai? Un problema da vida cotiá na que podemos atopar unha cuestión similar é a que segue: *Nunha voda, na que había menos de 200 convidados, ao sentalos en grupos de 5 quedaban 2 sós na última mesa; ao polos en grupos de 6, quedaban 5 na última; e, finalmente, ao polos en grupos de 7, había 4 na derradeira mesa. Cantos convidados había na voda?* Unha comprobación amosa que a resposta é 137. Porén, gustaríanos dispoñer dunha forma máis sistemática de acercarnos a este tipo de cuestións. Iso conséguese a través do teorema chinés do residuo.

Proposición 3.17 (Teorema chinés dos residuos)**.** Sexan $a_1, \ldots, a_k$ enteiros, e $n_1, \ldots, n_k$ enteiros positivos relativamente primos dous a dous. Pomos $N = n_1 n_2 \cdots n_k$. Entón, o sistema de congruencias $x \equiv a_i \pmod{n_i}$, con $i \in [k]$ ten solución, e se x_0 é unha solución, o conxunto de solucións é $x_0 + N\mathbb{Z}$. Máis en concreto, sexa b_i o inverso de $\frac{N}{n_i}$ módulo n_i. Entón,

$$x_0 = a_1 b_1 \cdot \frac{N}{n_1} + \ldots + a_k b_k \frac{N}{n_k}.$$

Demostración. Comezamos establecendo a unicidade. Se houbese dúas solucións do sistema, x e y, definimos a súa diferenza $z := y - x$. Entón, tense que $z \equiv 0 \pmod{n_i}$ para todo i, o que quere dicir que z é múltiplo de N. Polo tanto $y - x = Nk$, para algún $k \in \mathbb{Z}$. Alternativamente, $y = x + Nk$, como se quería ver.
Para ver a existencia, chega con ver que o x_0 do enunciado cumpre as condicións. En efecto, para determinar o resto de x_0 ao dividir por n_i unicamente nos importa o sumando $a_i b_i \cdot \frac{N}{n_i}$, pois o resto son múltiplos de n_i. Pero, por definición, $b_i \cdot \frac{N}{n_i} \equiv 1 \pmod{n_i}$, polo que $x_0 \equiv a_i \pmod{n_i}$, como se quería ver. □

Exemplo. Imos atopar un número que dea resto 3 ao dividilo entre 7, resto 2 ao dividilo entre 5 e resto 1 ao dividilo entre 4, isto é,

$$\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 4. \end{cases}$$

Como 7, 5 e 4 son relativamente primos, podemos aplicar o teorema chinés dos restos para atopar unha solución módulo $7 \cdot 5 \cdot 4$. Para iso, consideramos o resto módulo 140 dado por

$$3 \cdot \frac{140}{7} \cdot \left(\frac{140}{7}\right)_7^{-1} + 2 \cdot \frac{140}{5} \cdot \left(\frac{140}{5}\right)_5^{-1} + 1 \cdot \frac{140}{4} \cdot \left(\frac{140}{4}\right)_4^{-1}.$$

No referente aos inversos, temos que $20^{-1} \equiv 6^{-1} \equiv 6 \pmod 7$; $28^{-1} \equiv 3^{-1} \equiv 2 \pmod 5$; e $35^{-1} \equiv 3^{-1} \equiv 3 \pmod 4$. Polo tanto, o resto buscado é

$$3 \cdot 20 \cdot 6 + 2 \cdot 28 \cdot 2 + 1 \cdot 35 \cdot 3 = 360 + 112 + 105 = 577 \pmod{140}.$$

Polo tanto, calquera número que dea resto $577 \equiv 17$ módulo 140 sérvenos; por exemplo, o 17 é unha opción válida.

O teorema chinés dos restos tamén se pode empregar cando os números non son relativamente primos entre si. En primeiro lugar, imos facer a seguinte observación, que nos di que cando temos un resto módulo n tamén o podemos interpretar como un resto módulo d, onde d é un divisor arbitrario de n. Por exemplo, dar un resto módulo 9 dános tamén información sobre o resto módulo 3 (pero non sobre o resto módulo 4).

Proposición 3.18. Sexa $n > 1$ un número enteiro e d un divisor positivo de n. Entón, a aplicación

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z}, \quad x \pmod{n} \mapsto x \pmod{d}$$

está ben definida, isto é, non depende da elección de representante en $\mathbb{Z}/n\mathbb{Z}$. Ademais, a aplicación é sobrexectiva.

Demostración. É unha comprobación rutineira. □

Imos discutir que sucede no caso de dous enteiros, sendo o caso xeral totalmente análogo.

Proposición 3.19. Tomamos dous módulos n_1 e n_2, de xeito que $\gcd(n_1, n_2) = d$, e $n_1 = dm_1$ e $n_2 = dm_2$. Consideramos o sistema de congruencias

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2}. \end{cases}$$

Sexan b_1 e b_2 os restos de a_1 e a_2 módulo d. O sistema de congruencias ten solución se, e soamente se, $b_1 \equiv b_2 \pmod{d}$. Nese caso, ten unha única solución módulo dm_1m_2.

Demostración. A necesidade de condición $b_1 \equiv b_2 \pmod{d}$ é clara, xa que, en caso contrario, as ecuacións son incompatibles. Se a condición se cumpre, escribimos $d = \alpha n_1 + \beta n_2$. Unha comprobación rutineira amosa que

$$x = \frac{a_1\beta n_2 + a_2\alpha n_1}{d} = a_1\beta m_2 + a_2\alpha m_1$$

é unha solución do sistema: por exemplo, temos que

$$x = a_1 - a_1\alpha m_1 + a_2\alpha m_1 = a_1 + m_1\alpha(a_2 - a_1),$$

e $m_1(a_2 - a_1)$ é múltiplo de n_1, xa que $a_2 - a_1$ é múltiplo de d pola condición de que o sistema ten solución. □

Sexan (b_1, c_1) os restos de a_1 módulo d e módulo n_1 e (b_2, c_2) os restos de a_2 módulo d e módulo n_2, respectivamente. No caso máis sinxelo no que $\gcd(n_1, m_2) = 1$, o sistema da proposición anterior é equivalente a

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv c_2 \pmod{m_2}, \end{cases}$$

polo que se pode interpretar que a segunda ecuación dá información xa coñecida módulo d e aporta nova información módulo m_2. Cando m_2 e n_1 teñen factores en común, podemos interpretar como que a segunda información dá máis información módulo algún dos divisores de n_1. Traballaremos estas ideas a través dalgúns exemplos.

Exemplo. O sistema

$$\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 2 \pmod{8} \\ x \equiv 8 \pmod{12} \end{cases}$$

non ten solución, xa que as condicións $x \equiv 2 \pmod{8}$ e $x \equiv 8 \pmod{12}$ non son compatibles. A primeira implica que $x \equiv 2 \pmod{4}$ e a segunda que $x \equiv 0 \pmod{4}$.

Porén, o sistema

$$\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 2 \pmod 8 \\ x \equiv 6 \pmod{12} \end{cases}$$

si ten solución, xa que 7 é coprimo con 8 e 12 e polo tanto o único que temos que asegurar é a compatibilidade da segunda e da terceira ecuación. Como $\gcd(8, 12) = 4$, chega con ver que ambas ecuacións se corresponden coa mesma condición módulo 4, e é claro que esa é $x \equiv 2 \pmod 4$. Polo tanto, a última ecuación é redundante coa segunda módulo 4 e só nos aporta información módulo 3. Temos entón que o sistema é equivalente a

$$\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 2 \pmod 8 \\ x \equiv 0 \pmod 3, \end{cases}$$

que polo teorema chinés ten unha única solución módulo $7 \cdot 8 \cdot 3 = 168$.

É dicir, nestes casos temos que analizar tódolos pares de ecuacións: se hai dous calquera que son incompatibles, todo o sistema é incompatible. En caso contrario, o sistema ten unha única solución módulo o mínimo común múltiplo de tódolos n_i, que podemos obter extraendo a información de cada unha das ecuacións e formulando un sistema no que tódolos módulos sexan relativamente primos.
Imos acabar analizando un caso no que non se cumpre que $m_2 \nmid n_1$, isto é, a nova ecuación incorpora información módulo algún dos factores primos de n_1.

Exemplo. Consideremos o sistema

$$\begin{cases} x \equiv 1 \pmod{12} \\ x \equiv 7 \pmod{18} \end{cases}.$$

O sistema ten solución xa que o máximo común divisor de 12 e 18 é 6, e temos que ambas ecuacións implican que $x \equiv 1 \pmod 6$. Porén, neste caso temos que $12 = 6 \cdot 2$ e $18 = 6 \cdot 3$, polo que, coas notacións anteriores, tanto 2 como 3 non son relativamente primos co máximo común divisor, non podemos proceder ao igual que antes. O mínimo común múltiplo de 12 e 18 é $36 = 2^2 \cdot 3^2$, polo que temos que extraer do sistema a información módulo 2^2 e módulo 3^2. Da primeira ecuación temos que $x \equiv 1 \pmod 4$ e, da segunda, que $x \equiv 7 \pmod 9$. Estas dúas ecuacións dannos que $x \equiv 25 \pmod{36}$.

Presentamos a continuación outro resultado clásico sobre congruencias, o coñecido como *pequeno teorema de Fermat*. O nome de *pequeno* débese a que o *teorema de Fermat* é un resultado moito máis complicado e difícil, que asegura que a ecuación

$$x^n + y^n = z^n, \quad xyz \neq 0$$

non ten solucións enteiras.

Proposición 3.20 (Pequeno teorema de Fermat)**.** Sexa p un número primo e a un número enteiro tal que $(a, p) = 1$. Entón,

$$a^{p-1} \equiv 1 \pmod p.$$

Demostración. Comezamos observando que $\{1, 2, \ldots, p-1\} = \{a, 2a, \ldots, (p-1)a\}$. O primeiro conxunto contén tódolos restos non nulos módulo p. O segundo consta tamén de restos non nulos, xa que se $ia \equiv 0 \pmod{p}$ ou ben i ou ben a serían múltiplos de p, pero non é o caso. Polo tanto, chega con ver que non hai dous iguais. Se $ia \equiv ja \pmod{p}$, entón $(i-j)a$ é múltiplo de p, pero $(a, p) = 1$ e i, j escolléronse de xeito que son números distintos entre 1 e $p-1$ polo que a súa diferenza non pode ser múltiplo de p.
Como os dous conxuntos conteñen os mesmos números, o seu produto é igual módulo p:

$$(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}.$$

Como $(p, (p-1)!) = 1$, podemos multiplicar a ambos lados polo inverso de $(p-1)!$, e concluímos que $a^{p-1} \equiv 1 \pmod{p}$. □

Exemplo. Se $p = 7$, o pequeno teorema de Fermat di que $a^6 \equiv 1 \pmod{7}$ para calquera $a = 1, 2, \ldots, 6$, que é unha comprobación rutineira. Isto permite calcular, por exemplo, potencias arbitrarias módulo 7. Por exemplo, como $2024 = 6 \cdot 337 + 2$, temos que

$$2^{2024} \equiv (2^6)^{337} \cdot 2^2 \equiv 1 \cdot 4 \equiv 4 \pmod{7}.$$

De xeito similar,

$$3^{2024} \equiv (3^6)^{337} \cdot 3^2 \equiv 1 \cdot 3 \equiv 2 \pmod{7}.$$

Imos introducir agora a función phi de Euler, que fai un papel central en aritmética, e que é precisa para xeneralizar o pequeno teorema de Fermat. Por exemplo, permitiranos calcular 2^{2024} módulo 15.

Definición 3.7. Dado un enteiro $n \geq 1$, defínese $\varphi(n)$ como o número de enteiros x de xeito que $1 \leq x \leq n$ e $\gcd(x, n) = 1$. A función φ chámase *función phi de Euler*.

En particular, $\varphi(1) = \varphi(2) = 1$. Observamos tamén que $\varphi(n)$ é o número de elementos invertibles en $\mathbb{Z}/n\mathbb{Z}$, é dicir, o cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proposición 3.21. A función φ cumpre as seguintes propiedades.

(a) Se p é un número primo, $\varphi(p) = p - 1$.

(b) Se p é un número primo e $r \geq 1$ un enteiro, entón $\varphi(p^r) = (p-1)p^{r-1}$.

(c) Se a e b son enteiros positivos e $\gcd(a, b)$, entón $\varphi(ab) = \varphi(a)\varphi(b)$.

(d) Se $n = p_1^{r_1} \cdots p_k^{r_k}$, entón

$$\varphi(n) = (p_1 - 1)p_1^{r_1 - 1} \cdots (p_k - 1)p_k^{r_k - 1}.$$

O seguinte resultado estende o pequeno teorema de Fermat ao caso no que non traballamos módulo un primo, senón módulo un enteiro positivo arbitrario. O papel de $p-1$ faino a función phi de Euler.

Proposición 3.22 (Teorema de Euler)**.** Sexa n un número enteiro positivo e a un número enteiro tal que $(a, n) = 1$. Entón,

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Demostración. Sexan $i_1, \ldots, i_{\varphi(n)}$ os restos módulo n relativamente primos con n. Comezamos observando que $\{i_1, i_2, \ldots, i_{\varphi(n)}\} = \{ai_1, ai_2, \ldots, ai_{\varphi(n)}\}$. O primeiro conxunto contén tódolos restos invertibles módulo n. O segundo consta tamén de restos invertibles, xa que se ai_k ten algún factor en común con n ou ben a ou ben i_k terían factores en común con n, pero non é o caso. Polo tanto, chega con ver que non hai dous iguais. Se $ai_j \equiv ai_k \pmod{n}$, entón $(i_j - i_k)a$ é múltiplo de n, pero $(a, n) = 1$ e i_j, i_k escolléronse de xeito que son números distintos entre 1 e $n-1$ polo que a súa diferenza non pode ser múltiplo de n.
Como os dous conxuntos conteñen os mesmos números, o seu produto é igual módulo p:

$$i_1 \cdots i_{\varphi(n)} \equiv a^{\varphi(n)} \cdot i_1 \cdots i_{\varphi(n)} \pmod{n}.$$

Como $(p, i_j) = 1$, podemos multiplicar a ambos lados polos inversos dos i_j, e concluímos que $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Exemplo. Como $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$, e $\gcd(2, 15) = 1$, entón

$$2^{2024} \equiv (2^8)^{253} \equiv 1 \pmod{15}.$$

En cambio, para calcular 3^{2024} non podemos empregar o teorema de Euler. Nese caso, temos que $3^{2024} \equiv 0 \pmod{3}$ e, polo pequeno teorema de Fermat, $3^{2024} \equiv 1 \pmod{5}$. Polo tanto, o resto cumpre que é 0 módulo 3 e 1 módulo 5; polo teorema chinés dos restos, iso caracteriza o resto módulo 15, e temos que é 6.

Proposición 3.23 (Teorema de Wilson)**.** Sexa p un número primo. Entón,

$$(p-1)! \equiv -1 \pmod{p}.$$

Demostración. Se $p = 2$ o resultado é trivial, así que supoñamos que p é impar. Comezamos observando que a ecuación $x^2 \equiv 1 \pmod{p}$ unicamente ten as solucións $x \equiv \pm 1$. En efecto, $x^2 - 1 = (x-1)(x+1) \pmod{p}$ quere dicir que ou ben $x - 1 \equiv 0$ ou $x + 1 \equiv 0$. Polo tanto, podemos agrupar os números desde 1 ata $p-1$ como segue: o 1 e o $p-1$ pómolos a un lado, e os outros $p-3$ situámolos en parellas, cada un co seu inverso. O produto dos números de cada unha desas $(p-3)/2$ parellas é 1, polo que

$$(p-1)! \equiv 1 \cdot (-1) \equiv -1 \pmod{p}.$$

□

3.5. Raíces primitivas

Sexa $n \geq 1$ un enteiro positivo. Escribimos $(\mathbb{Z}/n\mathbb{Z})^\times$ para denotar o conxunto formado polos restos módulo n que son coprimos con n. Por exemplo, $(\mathbb{Z}/7\mathbb{Z})^\times = \{1, 2, 3, 4, 5, 6\}$ e $(\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\}$.

Definición 3.8. A *orde* dun elemento $a \in (\mathbb{Z}/n\mathbb{Z})$ é o menor enteiro positivo k tal que $a^k \equiv 1 \pmod{n}$. Escribimos $\mathrm{ord}_n(a)$. Un elemento g en $(\mathbb{Z}/n\mathbb{Z})^\times$ dise que é unha *raíz primitiva* se $\mathrm{ord}_n(g) = \varphi(n)$.

Pódese ver que g é raíz primitiva módulo n se, e soamente se,

$$\{1, g, g^2, \ldots, g^{\varphi(n)-1}\}$$

contén tódolos restos módulo n que son coprimos con n. Se tivésemos que $g^i \equiv g^j \pmod{n}$, con $0 \leq i < j < \varphi(n)$, teriamos que $g^{j-i} \equiv 1 \pmod{n}$, polo que g non sería raíz primitiva. Do mesmo xeito, se son todos diferentes, $g^{\varphi(n)}$ é a primeira potencia de expoñente positivo que dá 1 módulo n.

Proposición 3.24. Sexa a un enteiro coprimo con n. Entón, $\mathrm{ord}_n(a)$ divide $\varphi(n)$.

Demostración. Se facemos a división euclidiana de $\varphi(n)$ por $\mathrm{ord}_n(a)$, podemos pór

$$\varphi(n) = k \cdot \mathrm{ord}_n(a) + r,$$

con $0 \leq r < \mathrm{ord}_n(a)$. Entón,

$$1 \equiv a^{\varphi(n)} = a^{k\,\mathrm{ord}_n(a)} \cdot a^r \equiv a^r \pmod{n}.$$

Como $a^r \equiv 1$ módulo n e $0 \leq r < \mathrm{ord}_n(a)$, necesariamente se ten que cumprir que $r = 0$. □

Exemplo. O teorema de Euler asegura que a orde de calquera elemento sempre é un divisor de $\varphi(n)$. Por exemplo, módulo 7, a orde de 1 é 1; a orde de 6 é 2; a orde de 2 e de 4 é 3; e a orde de 3 e de 5 é 6.
En cambio, poderían non existir elementos de orde $\varphi(n)$. Por exemplo, $\varphi(8) = 4$, pero non hai elementos de orde 4: o 1 ten orde 1 e o 3, o 5 e o 7 teñen orde 2.
A seguinte táboa ilustra a situación.

n^k mód 7	1	2	3	4	5	6
n^0	1	1	1	1	1	1
n^1	1	2	3	4	5	6
n^2	1	4	2	2	4	1
n^3	1	1	6	1	6	6
n^4	1	2	4	4	2	1
n^5	1	4	5	2	3	6
n^6	1	1	1	1	1	1

En cambio, non hai raíces primitivas módulo 8, xa que a orde de tódolos elementos é 1 ou 2 e non hai elementos de orde 4.

n^k mód 8	1	3	5	7
n^0	1	1	1	1
n^1	1	3	5	7
n^2	1	1	1	1

Por exemplo, $\mathrm{ord}_5(1) = 1$, $\mathrm{ord}_5(2) = 4$, $\mathrm{ord}_5(3) = 4$ e $\mathrm{ord}_5(4) = 2$. Temos entón que o 2 e o 3 son as raíces primitivas módulo 5, xa que a súa orde é $\varphi(5) = 4$. De xeito similar, as raíces primitivas módulo 11 son 2, 6, 7 e 8.
A demostración de que existen raíces primitivas módulo primo ou módulo potencias de primos impares parte dos seguintes dous resultados previos.

Proposición 3.25. Sexa $n \geq 1$ un enteiro positivo. Cúmprese que

$$\sum_{d|n} \varphi(d) = n.$$

Demostración. En $\mathbb{Z}/n\mathbb{Z}$, o número de veces que temos que sumar un número consigo mesmo para que sexa 0 é sempre un divisor de n. Imos contar a cantidade deses números para un divisor d. É dicir, queremos atopar os a que cumpren que ad é múltiplo de n, pero ai non o é. Polo tanto, ten que sucede que $a = nk/d$, con $0 \leq k \leq d-1$ e k relativamente primo con d, polo que temos $\varphi(d)$ números. En particular,

$$\sum_{d|n} \varphi(d) = n.$$

□

O segundo resultado previo que necesitamos adoita coñecerse como *lema do levantamento do expoñente*. Se m é un enteiro, pomos $v_p(m)$ para denotar o maior enteiro non negativo k tal que $p^k \mid m$; falamos da *valoración p-ádica de m*; por convenio, pomos $v(0) = +\infty$. Unha comprobación rutineira amosa que se a e b son enteiros positivos cúmprense as seguintes propiedades:

(a) $v_p(ab) = v_p(a) + v_p(b)$;

(b) $v_p(a+b) \geq \text{mín}\{v_p(a), v_p(b)\}$ e se $v_p(a) \neq v_p(b)$ a desigualdade é estrita.

Proposición 3.26. Sexan a e b números enteiros e p un número primo impar de xeito que $p \mid (a-b)$, pero $p \nmid a$. Se $r \geq 1$ é un número enteiro,

$$v_p(a^r - b^r) = v_p(a-b) + v_p(r).$$

Demostración. Para maior comodidade, escribimos $a = b+k$, onde $v_p(k) = v_p(a-b) \geq 1$. A demostración procederá por indución en n. Porén, en primeiro lugar imos establecer o caso no que $v_p(n) = 0$. Temos que

$$\begin{aligned} a^n - b^n &= (b+k)^n - b^n \\ &= b^n + nkb^{n-1} + k^2(\text{expresión polinómica en } a,b,k) - b^n \\ &= nkb^{n-1} + k^2(\text{expresión polinómica en } a,b,k). \end{aligned}$$

Polo tanto, $a^n - b^n$ é a suma dun número que ten valoración p-ádica $v_p(nkb^{n-1}) = v_p(k)$ e doutro que ten valoración p-ádica maior ou igual que $2v_p(k)$. Polo tanto, $v_p(a^n - b^n) = v_p(k)$, como queriamos ver.
Imos demostrar o caso $n = p$ e a continuación pasaremos a realizar a indución. Neste caso,

$$a^p - b^p = (b+k)^p - b^p = pkb^{p-1} + \sum_{i=2}^{p} \binom{p}{i} k^i b^{p-i}.$$

Dentro da suma, tódolos sumandos son múltiplos de p^{k+2}, xa que, se $i < p$, $v_p(k^i) \geq 2k$ e $v_p\left(\binom{p}{i}\right) \geq 1$, mentres que $v_p(k^p) = pk \geq k+2$. Polo tanto, como $v_p(pkb^{k-1}) = v_p(p) + v_p(k) = k+1$, temos que $v_p(a^p - b^p) = k+1$.
Supoñamos agora que o resultado é certo para $v_p(n) = s$ e demostrémolo para $s+1$. En particular, supoñamos que $n = p^{s+1} \cdot r$, onde $\gcd(p,r) = 1$. Entón,

$$\begin{aligned} v_p(a^n - b^n) &= v_p((a^{p^s r})^p - (b^{p^s r})^p) \\ &= v_p(a^{p^s r} - b^{p^s r}) + v_p(p) \\ &= v_p(a-b) + s + 1, \end{aligned}$$

onde a última igualdade é consecuencia da hipótese de indución. □

Imos pasar agora a establecer a existencia de raíces primitivas. Unha primeira observación é que se n admite raíces primitivas, entón hai un único elemento de orde 2, que necesariamente é o menos 1. É dicir, a ecuación

$$x^2 \equiv 1 \pmod{n}$$

só ten unha solución. Automaticamente teremos que se $n = 2^k$, con $k \geq 3$ non hai raíces primitivas, xa que -1, $2^{k-1} - 1$ e $2^{k+1} + 1$ son todos eles elementos de orde 2. Este argumento ímolo xeneralizar na seguinte proposición.

Proposición 3.27 (Existencia de raíces primitivas)**.** Sexa $n > 1$ un enteiro. Existen raíces primitivas módulo n se, e soamente se, $n = 2$, $n = 4$, $n = p^k$ ou $n = 2p^k$, onde p é un primo impar e $k \geq 1$.

Demostración. Imos comezar estudando o caso de $(\mathbb{Z}/p\mathbb{Z})^\times$, sendo p un primo impar. Comezamos recordando que a orde dun elemento ten que ser necesariamente un divisor de $\varphi(p) = p - 1$, polo pequeno teorema de Fermat. Para cada divisor d de $p - 1$, temos que un elemento ten orde d se $x^d - 1 = 0$ e non se cumpre que $x^i - 1 = 0$ para ningún divisor de d estritamente menor ca el. Observamos tamén que se x ten orde d, os números $x^0, \ldots, x^{d-1}$ son todos eles solucións de $x^d - 1 = 0$ e, por Ruffini, esta ecuación non pode ter máis solucións en $\mathbb{Z}/p\mathbb{Z}$. Polo tanto, entre esas d solucións, exactamente $\varphi(d)$ teñen orde d, xa que

$$\operatorname{ord}_p(x^i) = \frac{\operatorname{ord}_p(x)}{\gcd(\operatorname{ord}_p(x), i)}.$$

Polo tanto, o número de elementos de orde d é 0 ou $\varphi(d)$. Temos entón que

$$\sum_{d|p-1} \text{número de elementos de orde } d \leq \sum_{d|p-1} \varphi(d) = p - 1,$$

polo que necesariamente tódalas desigualdades teñen que ser igualdade. En particular, hai $\varphi(p-1)$ elementos de orde $p - 1$.
Pasamos agora ao caso de potencia de primo. Afirmamos que hai un elemento que ten orde $p^{k-1}(p-1)$. Para que se dea $a^i \equiv 1 \pmod{p^k}$, ten que suceder que $a^i \equiv 1 \pmod{p}$, polo que $i = r(p-1)$. En primeiro lugar, observamos que se a e b son dous restos módulo p^k congruentes cunha raíz primitiva fixada, temos que $v_p(a^{p-1} - b^{p-1}) = v_p(a - b)$. En particular, entre estes p^{k-1} números, $(p-1)p^{k-2}$ cumpren que $v_p(a^{p-1} - 1) = 1$. Escollemos un destes números a. Entón,

$$v_p(a^{r(p-1)} - 1) = v_p(a^{p-1} - 1) + v_p(r) = 1 + v_p(r),$$

e teremos que este valor será k se, e soamente se, $v_p(r) = k - 1$. Polo tanto, o menor enteiro positivo que cumpre esta condición é $(p-1)p^{k-1}$ como queriamos.
Se $n = \prod_{i=1}^k p_i^{r_i}$ é un produto de primos impares (con multiplicidades), entón, polo teorema chinés dos restos

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^\times &\simeq \prod_{i=1}^k (\mathbb{Z}/p_i\mathbb{Z})^\times \\ &\simeq \prod_{i=1}^k \mathbb{Z}/(p_i - 1)p_i^{r_i}\mathbb{Z} \\ &\simeq \prod_{i=1}^k \mathbb{Z}/(p_i - 1)\mathbb{Z} \times \prod_{i=1}^k \mathbb{Z}/p_i^{r_i - 1}\mathbb{Z},\end{aligned}$$

e se hai dous primos diferentes necesariamente entón hai máis dun elemento de orde 2, polo que non pode haber raíces primitivas.
Finalmente, para o caso de potencias de 2, temos de xeito trivial que tanto o 2 como o 4 admiten raíces primitivas. Para $n = 2^k$, con $k \geq 3$, non hai raíces primitivas xa que a ecuación $x^2 \equiv 1 \pmod{2^k}$ ten 4 solucións. Se $n = 2^{r_0} \prod_{i=1}^{k} p_i^{r_i}$, onde os p_i son primos impares, temos dous casos: cando $r_0 \in \{0, 1\}$ e $k = 1$, entón hai raíces primitivas. Se $r_0 \geq 2$, entón hai necesariamente máis dun elemento de orde 2, o que non é posible.
Concluímos polo tanto que os únicos módulos que teñen raíces primitivas son 2, 4, p^k e $2p^k$, onde p é un primo impar. □

En particular, se $k \geq 2$, módulo p^k temos

$$\varphi(\varphi(p^k)) = \varphi((p-1)p^{k-1}) = \varphi(p-1)(p-1)p^{k-2}$$

raíces primitivas, como queriamos. Aquí empregamos que φ é debilmente multiplicativa, e que polo tanto $\varphi(ab) = \varphi(a)\varphi(b)$ se $\gcd(a, b) = 1$.

Exemplo. No caso do 9 temos a seguinte táboa:

n^k mód 9	1	2	4	5	7	8
n^1	1	2	4	5	7	8
n^2	1	4	7	7	4	1
n^3	1	8	1	8	1	8
n^4	1	7	4	4	4	1
n^5	1	5	7	2	7	8
n^6	1	1	1	1	1	1

As raíces primitivas son o 2 e o 5, que son congruentes módulo 3 coa única raíz primitiva módulo 3, que era o 2. Porén, dos 3 elementos módulo 9 que eran congruentes con 2, hai un que non serve, que é o 8. Esta situación non é un caso concreto, sucederá sempre: dado un primo impar p e unha raíz primitiva g módulo p, haberá $p-1$ restos módulo p^2 que sexan congruentes con g módulo p e raíces primitivas; e un único que sendo congruente con g módulo p non sexa raíz primitiva.

3.6. A lei de reciprocidade cuadrática

O obxectivo desta sección é resolver ecuacións de grao dous (ou superior!) módulo n. Imos comezar comparando dúas ecuacións diferentes módulo 11. A primeira delas é a ecuación

$$x^2 - x - 1 \equiv 0 \pmod{11}.$$

Pódese comprobar que $x \equiv 4$ e $x \equiv 8$ son solucións, xa que

$$4^2 - 4 - 1 = 11 \equiv 0 \pmod{11} \quad \text{e} \quad 8^2 - 8 - 1 = 55 \equiv 0 \pmod{11}.$$

A maneira de achar estas solucións é aplicando a fórmula da ecuación de segundo grao, que o único que require é que 2 teña inverso módulo n:

$$x \equiv 2^{-1}\left(1 \pm \sqrt{5}\right) \equiv 2^{-1}\,(1 \pm 4) = 6 \cdot (1 \pm 4),$$

onde se empregou que $\sqrt{5} \equiv 4$ xa que $4^2 \equiv 5 \pmod{11}$. En cambio, se consideramos a ecuación

$$x^2 - x - 3 \equiv 0 \pmod{11}$$

vemos que non ten solución. O discriminante da ecuación de segundo grao é $1+4\cdot 3 = 13 \equiv 2 \pmod{11}$, e é doado comprobar que non hai ningún número que, ao elevalo ao cadrado, sexa congruente con 2 módulo 11. Polo tanto, dicimos que a ecuación non ten solucións módulo 11.
Imos comezar estudando cando as ecuacións da forma

$$x^2 \equiv d \pmod{n}$$

teñen solución. En primeiro lugar, se $n = p_1^{r_1} \cdots p_k^{r_k}$, necesariamente cómpre que cada unha das ecuacións $x^2 \equiv d \pmod{p_i^{r_i}}$ teña solución; iso é, ademais, suficiente, polo teorema chinés dos restos.
Para abordar en primeiro lugar o estudo da ecuación $x^2 \equiv d \pmod{p}$, onde p é un primo, introducimos o chamado símbolo de Legendre.

Definición 3.9. Sexa p un número primo e a un enteiro. Defínese

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } a \text{ é múltiplo de } p; \\ 1 & \text{se } x^2 \equiv a \pmod{p} \text{ ten solución e } a \not\equiv 0 \pmod{p} \\ -1 & \text{se } x^2 \equiv a \pmod{p} \text{ non ten solución.} \end{cases}$$

Exemplo. Cúmprese que $\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$, xa que 1, 2 e 4 son residuos cuadráticos módulo 7: $1^2 \equiv 6^2 \equiv 1 \pmod{7}$, $3^2 \equiv 4^2 \equiv 2 \pmod{7}$ e $2^2 \equiv 5^2 \equiv 4 \pmod{7}$. En cambio, $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$.

Supoñamos que $p \neq 2$ e $a \not\equiv 0 \pmod{p}$. Entón, a ecuación $x^2 \equiv a \pmod{p}$ ten ou 0 ou 2 solucións. En efecto, se d é unha solución, entón $-d$ tamén o será, e $d \not\equiv -d \pmod{p}$. Entón

$$x^2 - a = (x-d)(x+d) \equiv 0 \pmod{p},$$

que só ten as solucións $x = \pm d$.

Proposición 3.28. Sexa p un primo impar e a un enteiro comprimo con p. Entón,

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}.$$

Demostración. Sexa g unha raíz primitiva módulo p. Temos que $a = g^i$, para $0 \leq i < p-1$, e cúmprese que a é un cadrado perfecto se, e soamente se, i é par. Por outra banda,

$$a^{\frac{p-1}{2}} = g^{\frac{i(p-1)}{2}} = \begin{cases} +1 & \text{se } i \text{ é par;} \\ -1 & \text{se } i \text{ é impar.} \end{cases}.$$

□

Proposición 3.29. O símbolo de Legendre é multiplicativo:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Demostración. Se a ou b son múltiplos de p, o resultado é inmediato. En caso contrario, sexa $a = g^x$ e $b = g^y$. Entón, o resultado simplemente afirma que $(-1)^{x+y} = (-1)^x(-1)^y$, que é certo. □

Sexan agora p e q dous números primos impares. Cando un deles é *pequeno*, resulta doado determinar se o outro é residuo cuadrático ou non. Por exemplo, 1007 non é residuo cuadrático módulo 5, xa que $1007 \equiv 2 \pmod 5$, e 2 non é un cadrado módulo 5. En cambio, a pregunta contraria non é tan sinxela: como podemos saber se 5 é residuo cuadrático módulo 1007 sen necesidade de ir comprobando tódolos cadrados desde 1 ata 503? A resposta a esta pregunta vén dada pola lei de reciprocidade cuadrática.

Proposición 3.30 (Lei de reciprocidade cuadrática)**.** Sexan p e q dous primos impares diferentes. Cúmprese que

$$\Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

É dicir, se ambos primos son 3 módulo 4, entón os dous símbolos de Legendre son distintos; e en caso contrario son iguais.

Demostración. Polo teorema chinés dos restos, hai unha bixección

$$\varphi\colon (\mathbb{Z}/pq\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$$

dada por $\varphi(x) = (x, x)$. Consideramos os conxuntos

$$A = \{r \in (\mathbb{Z}/pq\mathbb{Z})^\times \text{ con } 1 \le r < pq/2\}$$

e

$$B = \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \text{ con } 1 \le y < q/2\}.$$

Dado $(x, y) \in B$, existe $r \in A$ de xeito que $\varphi(r) = (x, y)$ ou $\varphi(r) = (-x, -y)$. En particular,

$$\prod_{(x,y)\in B} (x, y) = \epsilon \prod_{r\in A} (r, r),$$

onde $\epsilon \in \{\pm 1\}$.
De cara a simplificar a notación, pomos $p' = \frac{p-1}{2}$ e $q' = \frac{q-1}{2}$. Comezamos observando que

$$\begin{aligned}\prod_{(x,y)\in B} (x, y) &= ((p-1)!^{q'}, (q')^{2p'}) = ((-1)^{q'}, ((q-1)!(-1)^{q'})^{p'}) \\ &= ((-1)^{q'}, (-1)^{p'}(-1)^{p'q'}),\end{aligned}$$

onde se empregou dúas veces o teorema de Wilson para asegurar que $(q')^2 = (q-1)!(-1)^{q'}$.
De xeito similar, en $(\mathbb{Z}/p\mathbb{Z})^\times$,

$$\prod_{r\in A} r = \Big(\prod_{\substack{r<pq/2\\ p\nmid r}} r\Big)\cdot\Big(\prod_{\substack{r<pq/2\\ q\mid r}} r\Big)^{-1} = \frac{(p-1)!^{q'}\cdot p'!}{(q)(2q)\cdots(p'q)} = \frac{(-1)^{q'}}{q^{p'}} = (-1)^{q'}\Big(\frac{q}{p}\Big).$$

Por simetría, en $(\mathbb{Z}/q\mathbb{Z})^\times$ temos que $(-1)^{p'}\Big(\frac{p}{q}\Big)$. Polo tanto,

$$((-1)^{q'}, (-1)^{p'}(-1)^{p'q'}) = \epsilon\Big((-1)^{q'}\Big(\frac{q}{p}\Big), (-1)^{p'}\Big(\frac{p}{q}\Big)\Big).$$

De aquí dedúcese que

$$\epsilon = \Big(\frac{q}{p}\Big) = (-1)^{p'q'}\Big(\frac{p}{q}\Big),$$

e temos entón o resultado buscado. □

A lei de reciprocidade cuadrática ten dúas limitacións: o caso do -1 e o caso do primo 2.

Proposición 3.31 (Leis suplementarias)**.** Sexa p un primo impar.

(a) -1 é un residuo cuadrático módulo p se, e soamente se, $p \equiv 1 \pmod 4$.

(b) 2 é un residuo cuadrático módulo p se, e soamente se, $p \equiv \pm 1 \pmod 8$.

Demostración. (a) Supoñamos que $p = 4k+1$, e consideremos $x = (2k)!$. Entón,

$$x^2 \equiv (2k)! \cdot (2k)! \equiv (4k)! \equiv -1 \pmod p,$$

polo que -1 é un residuo cuadrático.

Sexa agora $p = 4k+3$ e supoñamos que existe x de xeito que $x^2 \equiv -1 \pmod p$. Elevando ao cadrado ambos lados da ecuación, $x^4 \equiv 1 \pmod 4$. Polo pequeno teorema de Fermat, $x^{4k+2} \equiv 1 \pmod 4$, polo que a orde de x módulo p divide $\gcd(4, 4k+2) = 2$. Iso quere dicir, en concreto, que $x^2 \equiv 1 \pmod p$, que é unha contradición.

(b) Para o caso 2, consideramos o conxunto $\{2, 4, \ldots, p-1\}$. O produto de tódolos elementos é

$$2 \cdot 4 \cdots (p-1) = 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$$

Alternativamente, temos que

$$\begin{aligned} p - 1 &\equiv (-1)^1 \cdot 1 \\ 2 &\equiv (-1)^2 \cdot 2 \\ p - 3 &\equiv (-1)^3 \cdot 3, \end{aligned}$$

e así sucesivamente, onde tódalas congruencias se tomaron módulo p. Polo tanto, o produto é igual a

$$(-1)^{\frac{p^2-1}{8}} \left(\frac{p-1}{2}\right)!$$

Igualando as dúas expresións, e usando que $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}}$, chegamos que a que

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Observamos finalmente que $p^2 - 1$ sempre é múltiplo de 8, e tomando congruencias módulo 16 temos que $p^2 \equiv 1$ se, e soamente se, $p \equiv \pm 1 \pmod 8$.

□

Exemplo. Imos estudar se o -30 é residuo cuadrático módulo 1007 (que é un primo). Pola multiiplicatividade do símbolo de Legendre,

$$\left(\frac{-30}{1007}\right) = \left(\frac{-1}{1007}\right)\left(\frac{2}{1007}\right)\left(\frac{3}{1007}\right)\left(\frac{5}{1007}\right).$$

Antes de nada, observamos que 1007 é 3 módulo 4 e 7 módulo 8.

- Pola primeira lei suplementaria, $\left(\frac{-1}{1007}\right) = -1$.

- Pola segunda, $\left(\frac{2}{1007}\right) = 1$.
- Pola lei de reciprocidade cuadrática, $\left(\frac{3}{1007}\right) = -\left(\frac{1007}{3}\right) = -\left(\frac{2}{3}\right) = 1$.
- Pola lei de reciprocidade cuadrática, $\left(\frac{5}{1007}\right) = \left(\frac{1007}{5}\right) = \left(\frac{2}{5}\right) = -1$.

Multiplicando os catro números, temos que -30 é un residuo cuadrático módulo 1007.

Máis en xeral, queremos abordar o problema de cando a ecuación

$$x^2 \equiv a \pmod{n}$$

ten solución. Se $n = p_1^{a_1} \cdots p_k^{a_k}$, polo teorema chinés do residuo, a ecuación é equivalente a resolver o sistema de k ecuacións da forma $x^2 \equiv a \pmod{p_i^{a_i}}$. Se algunha delas non ten solución, o sistema non pode ter solución; se cada unha das ecuacións do sistema ten c_i solucións, hai en total $c_1 \cdots c_k$ solucións módulo n.

Proposición 3.32. Sexa p un primo impar, $k \geq 2$ un enteiro e a un resto diferente de 0 módulo p. Entón, $x^2 \equiv a \pmod{p^k}$ ten solucións se, e soamente se, $x^2 \equiv a \pmod{p}$ ten solución. En calquera caso, ten 2 solucións.
Se $p = 2$, entón $x^2 \equiv a \pmod{2^k}$ ten solución se, e soamente se, $x^2 \equiv a \pmod{8}$ ten solución.

Demostración. Imos demostrar por indución o seguinte: sexa x_1 unha solución de $x^2 \equiv a \pmod{p}$. Entón, existe unha única solución x_k de $x^2 \equiv a \pmod{p^k}$ que é congruente con x_1 módulo p. Para $k = 1$ o resultado é trivialmente certo, así que supoñámolo certo ata k. Temos entón que os posibles x_{k+1} son da forma $x_{k+1} = x_k + \alpha p^k$. Entón,

$$x_{k+1}^2 = x_k^2 + 2\alpha p^k \pmod{p^{k+1}}.$$

Como $a - x_k^2 = cp^k$, temos que a ecuación é equivalente a $2\alpha p^k \equiv cp^k$, polo que α é o único elemento en $\mathbb{Z}/p\mathbb{Z}$ que cumpre $\alpha \equiv 2^{-1}c \pmod{p}$.
O caso de $p = 2$ é similar, pero hai que ser máis coidadoso porque 2 non é invertible. □

Exemplo. A ecuación

$$x^2 \equiv 8 \pmod{15}$$

non ten solución, porque $x^2 \equiv 3 \pmod{5}$ non ten solución.
A ecuación

$$x^2 \equiv 4 \pmod{15}$$

ten 4 solucións: a ecuación é equivalente ao sistema

$$\begin{cases} x^2 \equiv 1 & \pmod{3} \\ x^2 \equiv 4 & \pmod{5}. \end{cases}$$

A primeira ten as solucións $x \equiv 1, 2 \pmod{3}$ e a segunda $x \equiv 2, 3 \pmod{5}$. Cada elección nunha das ecuacións dá lugar a unha solución, polo que obtemos $x \equiv 2, 7, 8, 13 \pmod{15}$.

O estudo dos residuos cuadráticos pode estenderse a potencias de orde superior. A seguinte proposición indica o número de restos diferentes que poden deixar as potencias n-ésimas módulo p.

Proposición 3.33. Sexa $n \geq 1$ un número enteiro. O conxunto

$$\{a^n \mid 1 \leq a \leq p-1\}$$

dá un total de $\frac{p-1}{\gcd(p-1,n)}$ restos diferentes módulo p.

Demostración. Sexa g unha raíz primitiva módulo p. O número de restos diferentes módulo p do conxunto do enunciado correspóndese co número de restos diferentes do conxunto

$$\{in \mid 0 \leq i \leq p-2\}$$

módulo $p-1$, que se corresponde co dado no enunciado. □

Exemplo. Os únicos restos posibles módulo 11 dunha potencia quinta son 1, -1 e 0. En cambio, unha potencia quinta pode tomar tódolos restos posibles módulo 7. Este tipo de resultados son útiles para establecer que determinadas ecuacións non teñen solucións. Por exemplo, sexa $n = 7k + 3$, con $k \in \mathbb{Z}$. Tense entón que a ecuación $a^3 + b^3 = n$ non pode ter solución. Se a tivera, ambos lados darían o mesmo resto ao dividir por 7: o lado da dereita dá resto 3, pero o da esquerda só pode dar restos $0, \pm 1 ou \pm 2$, é dicir, nunca pode dar resto 3 nin resto 4. A dificultade nestes casos está en escoller un módulo axeitado, para o que adoita ser útil ter en conta a proposición anterior.

Capítulo 4

Algoritmos

Este tema ten un dobre obxectivo. Por un lado, introducir a notación asintótica habitual para comparar o crecemento de diferentes tipos de funcións. Por exemplo, informalmente temos claro que a función $f(n) = \log(n)$ *crece máis lento* que un polinomio, e que un polinomio *crece máis lento* que $g(n) = 2^n$. Dispor dunha notación axeitada para describir isto será útil, á súa vez, para falar do custo dos algoritmos, sucesións finitas de instrucións precisas chamadas pasos que se empregan para realizar unha tarefa, un cálculo ou para resolver un problema. Algúns dos exemplos típicos de algoritmos que estudaremos son a busca dun elemento nunha lista ou a ordenación dos elementos dunha lista. Na parte final, presentamos algunhas nocións de criptografía e discutimos o algoritmo RSA, que emprega a aritmética modular para codificar mensaxes.
Ao longo de todo o capítulo, $\log(n)$ refírese ao logaritmo natural, é dicir, $\log(n) = \log_e(n)$.

4.1. Notación asintótica

Definición 4.1. Sexan $f, g\colon \mathbb{N} \to \mathbb{R}$. Consideramos as seguintes notacións:

(a) $f \in \mathcal{O}(g)$ se existe unha constante $C > 0$ e un enteiro n_0 de xeito que $|f(n)| \leq C \cdot |g(n)|$ para todo $n \geq n_0$. Dicimos que f *é O grande de* g.

(b) $f \in \Omega(g)$ se $g \in \mathcal{O}(f)$. Dicimos que f *é omega grande de* g.

(c) $f \in \Theta(g)$ se $f \in \mathcal{O}(g)$ e $g \in \mathcal{O}(f)$. Dicimos que f *é theta de* g.

(d) $f \in o(g)$ se $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$. Dicimos que f *é o pequena de* g.

(e) $f \sim g$ se $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$. Dicimos que f *é asintoticamente igual a* g.

Tense que se existe o límite $\lim_{n\to\infty} \frac{f(n)}{g(n)}$ e é distinto de infinito, entón $f(n) \in \mathcal{O}(g(n))$. De xeito análogo, sucede que se existe o límite $\lim_{n\to\infty} \frac{f(n)}{g(n)}$ e é distinto de cero, entón $f(n) \in \Omega(g(n))$. Finalmente, se existe o límite $\lim_{n\to\infty} \frac{f(n)}{g(n)}$ e é distinto de cero e infinito, entón $f(n) \in \Theta(g(n))$. Porén, podería suceder que o límite non existise (por exemplo, que a sucesión oscilase entre dous valores) e entón habería que realizar a discusión empregando a definición.
Enunciamos a continuación as propiedades básicas do símbolo $\mathcal{O}$. En primeiro lugar, observamos que se $f(n) \in \mathcal{O}(g(n))$ e $g(n) \in \mathcal{O}(h(n))$, entón $f(n) \in \mathcal{O}(h(n))$. Por outra

banda, tamén notamos que $f \in \mathcal{O}(1)$ se, e soamente se, f é unha función limitada; e $f \in o(1)$ se, e soamente se, $\lim_{n\to\infty} f(n) = 0$. A modo de comentario histórico, apuntamos que a notación *big-*$\mathcal{O}$ foi introducida polo matemático alemán Paul Bachmann nun libro sobre teoría de números. É frecuente referirse a el como *símbolo de Landau*, pois foi empregado polo matemático alemán Edmund Landau en moitos dos seus traballos. En ciencias da computación, o seu uso estendeuse grazas a Donald Knut, quen tamén introduciu as notacións *big-*Ω e *big-*Θ.

Exemplo. O polinomio $p(n) = a_k n^k + a_{k-1} n^{k-1} + \ldots + a_1 n + a_0$, cando $a_n \neq 0$, cumpre que $p(n) = \Theta(n^k)$. É dicir, o crecemento dun polinomio vén marcado unicamente polo seu grao.

Proposición 4.1. Cúmprense as seguintes propiedades.

(a) Se $f \in \mathcal{O}(g)$ e c é unha constante, entón $cf \in \mathcal{O}(g)$.

(b) Se $f_1 \in \mathcal{O}(g_1)$ e $f_2 \in \mathcal{O}(g_2)$, entón $f_1 + f_2 \in O(|g_1| + |g_2|)$ e $f_1 f_2 \in \mathcal{O}(g_1 g_2)$.

(c) Se $f_1 \in \mathcal{O}(g_1)$ e $f_2 \in \mathcal{O}(g_2)$, entón $f_1 + f_2 \in \mathcal{O}(\text{máx}\{|g_1|, |g_2|\})$.

Demostración. (a) Inmediato a partir da demostración.

(b) Se $f_1(n) \in \mathcal{O}(g_1)$, entón $|f_1(n)| \leq C_1 |g_1(n)|$ para todo $n \geq N_1$. Se $f_2(n) \in \mathcal{O}(g_2)$, entón $|f_2(n)| \leq C_2 |g_2(n)|$ para todo $n \geq N_2$. Polo tanto,

$$\begin{aligned} |f_1(n) + f_2(n)| &\leq |f_1(n)| + |f_2(n)| \\ &\leq C_1 |f_1(n)| + C_2 |f_2(n)| \\ &\leq \text{máx}\{C_1, C_2\}(|f_1(n)| + |f_2(n)|), \end{aligned}$$

para todo $n \geq \text{máx}\{N_1, N_2\}$. Por outra banda, para todo $n \geq \text{máx}\{N_1, N_2\}$ cúmprese que

$$\begin{aligned} |(f_1 f_2)(n)| &= |f_1(n) f_2(n)| \\ &= |f_1(n)| \cdot |f_2(n)| \\ &\leq C_1 C_2 |(g_1 g_2)(n)|, \end{aligned}$$

onde $C_1 C_2 > 0$.

(c) Séguese de xeito inmediato a partir da propiedade anterior.

□

Exemplo. Tense que $n^a = \mathcal{O}(n^b)$ se $a \leq b$ e $n^a = \mathcal{O}(b^n)$ se $b > 1$. Por outra banda, $(\log n)^a = \mathcal{O}(n^b)$ se $b > 1$ e $\log_a(n) = \mathcal{O}(\log_b(n))$ para todo $a, b > 0$.

Proposición 4.2 (Fórmula de Stirling)**.** Se consideramos a función $f(n) = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$, entón $n! \sim f(n)$, é dicir,

$$\lim_{n\to\infty} \frac{f(n)}{n!} = 1.$$

Omitimos a demostración do resultado, xa que require de diferentes manipulacións con ingredientes da análise matemática.

Exemplo. Tense que $\log(n!) = \mathcal{O}(n \log n)$, xa que

$$\begin{aligned}\log\left(\sqrt{2\pi n}\left(\frac{n}{e}\right)^n\right) &= \frac{1}{2}\log(2\pi n) + n\log\left(\frac{n}{e}\right) \\ &= \frac{1}{2}\log(2\pi) + \frac{1}{2}\log(n) + n\log(n) - n,\end{aligned}$$

e o termo dominante asintoticamente é $n\log(n)$.

No relativo aos números binomiais, temos que

$$\frac{2^{2n}}{2n+1} \leq \binom{2n}{n} \leq 2^{2n}.$$

Como corolario da fórmula de Stirling, podemos deducir que o denominador *correcto* é $\sqrt{\pi n}$.
Outra sucesión da que nos interesará frecuentemente estudar o seu crecemento é a formada polos chamados *números harmónicos*, que se definen como

$$H_n = \frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{n}.$$

Proposición 4.3. Para todo $n \geq 1$ cúmprese que

$$\log(n) < H_n < \log(n) + 1,$$

é dicir, $H_n = \mathcal{O}(\log n)$.

A demostración baséase en controlar o crecemento da sucesión de H_n mediante unha representación integral. Máis concretamente, sexa $m \geq 1$ un enteiro positivo e $f\colon [1, +\infty) \to \mathbb{R}$ unha función decrecente, non negativa e con $\lim_{x\to\infty} f(x) = 0$. Entón, $\sum_{n=m}^{\infty} f(n)$ converxe se $\lim_{n\to\infty} \int_m^n f(x)\,dx < +\infty$ e diverxe cando o límite da integral é $+\infty$. Ademais,

$$\lim_{n\to\infty} \int_m^n f(x)\,dx \leq \sum_{n=m}^{\infty} f(n) \leq f(m) + \lim_{n\to\infty} \int_m^n f(x)\,dx.$$

Imos ver outro exemplo que ilustra o uso das integrais de cara a facer estimacións asintóticas.

Exemplo. Sexa $k \geq 1$ un enteiro. Consideramos a función

$$f(n) = 1^k + 2^k + \ldots + n^k.$$

Entón, $f(n) \in \Theta(n^{k+1})$. É inmediato comprobar que $f(n) \in \mathcal{O}(n^{k+1})$, xa que

$$1^k + 2^k + \ldots + n^k \leq n^k + n^k + \ldots + n^k = n^{k+1}.$$

Imos agora ver que $f(n) \in \Omega(n^{k+1})$. Para iso, observamos que, se $a = 1, \ldots, n$, tense que

$$a^k \geq \int_{a-1}^{a} x^k\,dx = \frac{a^{k+1} - (a-1)^{k+1}}{k+1}.$$

Sumando tódalas desigualdades desde $a = 1$ ata $a = n$, quédanos que

$$f(n) = 1^k + 2^k + \ldots + n^k \geq \frac{n^{k+1}}{k+1},$$

o cal proba o resultado que queriamos.

4.2. Algoritmos

A noción de algoritmo é central do desenvolvemento das matemáticas computacionais e das ciencias da computación.

Definición 4.2. Un *algoritmo* é unha sucesión finita de instrucións precisas chamadas *pasos* para realizar unha tarefa, un cálculo ou para resolver un problema.

Nun algoritmo, cada paso é unha instrución clara (non ambigua) que pode ser executada nun tempo finito. Ademais, a sucesión na que os pasos teñen que ser executados está claramente definida e estará garantido que o proceso remata despois dun número finito de pasos. Imos resumir algunhas das propiedades dos algoritmos e introducir parte do vocabulario que precisaremos no seu estudo.

- *Entrada* (ou *input*). Un algoritmo ten valores de entrada que son elementos dun conxunto especificado.
- *Saída* (ou *output*). Para cada conxunto de valores de entrada, un algoritmo produce valores de saída dun conxunto especificado. Os valores de saída son a solución do problema.
- *Definición.* Os pasos dun algoritmo deben estar definidos con precisión.
- *Corrección.* Un algoritmo debe producir saídas correctas para cada conxunto de valores de entrada.
- *Duración finita.* Un algoritmo debe producir a saída despois dun número finito de pasos para calquera conxunto de valores de entrada. Porén, este número de pasos pode ser arbitrariamente grande.
- *Efectividade.* Debe ser posible realizar cada paso do algoritmo con exactitude e nun intervalo finito de tempo.
- *Xeneralidade.* O procedemento debe ser aplicable a tódolos problemas da forma desexada, non só para un conxunto particular de datos de entrada.

Non se debe confundir a efectividade coa eficiencia, que é un concepto que ten que ver coa rapidez do algoritmo (polo xeral, que sexa polinómico na entrada).
Polo xeral, unha pregunta que nos vai interesar é determinar a cantidade de operacións que debe realizar un algoritmo. A *complexidade en tempo* dun algoritmo pódese expresar en termos do número de operacións que precisa o algoritmo. Nos exemplos que traballaremos, veremos que ás veces miraremos cal é *o caso peor*, é dicir, cantas operacións cómpre realizar como máximo; pero, en moitos casos, o que faremos é analizar *o caso medio*, é dicir, non nos importará que haxa algún caso no que o noso algoritmo sexa *lento* se, en xeral, require de poucas operacións.
Imos comezar discutindo dous resultados que se poden empregar para determinar o custo de algoritmos nos que o custo para un tamaño da entrada depende do custo para tamaños menores; nestes casos, falaremos de *recorrencias*, xa que, fixados os primeiros valores, os seguintes quedan xa totalmente determinados.

Proposición 4.4 (Teorema de resolución de recorrencias subtractivas)**.** Dada unha recorrencia da forma

$$T(n) = aT(n-c) + g(n), \quad c \geq 1,\ g(n) = \Theta(n^k),\ k \geq 0,$$

tense que

$$T(n) = \begin{cases} \Theta(n^k) & \text{se } a < 1, \\ \Theta(n^{k+1}) & \text{se } a = 1, \\ \Theta(a^{n/c}) & \text{se } a > 1. \end{cases}$$

Exemplo. Supoñamos que formulamos o seguinte método para o cálculo do factorial dun enteiro positivo. Se $n = 1$, dicimos que vale 1. Se $n > 1$, dicimos que vale n multiplicado polo factorial de $n - 1$. Temos entón que $T(n) = \Theta(n)$.

O resultado máis importante, porén, ten que ver coas chamadas recorrencias divisoras.

Proposición 4.5 (Teorema de resolución de recorrencias divisoras)**.** Dada unha recorrencia da forma

$$T(n) = aT(n/b) + g(n), \quad b > 1,\ g(n) = \Theta(n^k),\ k \geq 0,$$

con $\alpha = \log_b(a)$, tense que

$$T(n) = \begin{cases} \Theta(n^k) & \text{se } \alpha < k, \\ \Theta(n^k \log n) & \text{se } \alpha = k, \\ \Theta(n^\alpha) & \text{se } \alpha > k. \end{cases}$$

Exemplo. Consideramos unha recorrencia da forma

$$T(n) = T\left(\frac{n}{2}\right) + 1.$$

Neste caso, $a = 1$ e $b = 2$, polo que $\alpha = 0$ e $k = 0$. Polo teorema anterior, $T(n) = \Theta(\log(n))$.

Definición 4.3. Un algoritmo de busca é un algoritmo que, dada unha lista, localiza nela un elemento dado.

Exemplo. Se non temos ningunha información sobre a lista, podemos seguir o seguinte procedemento: recorremos tódolos elementos un por un ata dar co que buscamos; se non o atopamos despois de percorrer a lista enteira, dicimos que non está. Este argumento ten custo lineal $\mathcal{O}(n)$ xa que, en principio, require visitar tódolos elementos.

Se a lista está ordenada, podemos empregar o que se coñece como *busca binaria*. Dividimos a lista en 2 e collemos o elemento do medio (se a lista é de tamaño par collemos calquera deles). Se ese é o elemento buscado, rematamos. En caso contrario, miramos se é menor ou maior; se é menor, buscamos entre os máis pequenos, e se é maior, entre os máis grandes.

Proposición 4.6. A busca binaria cumpre a recorrencia

$$T(n) = T\left(\frac{n}{2}\right) + 1,$$

xa que en cada paso realizamos unha comparación e logo redúcese á metade o tamaño da lista. Polo tanto, ten un custo de $\Theta(\log(n))$.

Demostración. Aplicando o teorema de resolución de recorrencias divisoras, temos que $\alpha = k = 0$. Polo tanto, estamos no segundo caso, é o custo é $\Theta(\log(n))$. □

Unha variante é a *busca ternaria*. Para atopar un elemento x nunha lista ordenada, dividímola en tres partes, de xeito que a e b sexan os elementos inicial e final do intervalo central. Se $x < a$, entón seguimos buscando no primeiro terzo; se $x > b$, entón buscamos no último terzo. Proseguimos así sucesivamente ata quedarnos cun intervalo de lonxitude 1. A busca binaria cumpre a recorrencia

$$T(n) = T\left(\frac{n}{3}\right) + 2,$$

xa que en cada paso realizamos dúas comparacións e logo dividimos por tres o tamaño da lista. Polo teorema de resolución de recorrencias divisoras, ten un custo de $\Theta(\log(n))$. Noutros casos de algoritmos recursivos non é tan doado calcular o custo. Por exemplo, no caso da sucesión de Fibonacci temos que

$$T(n) = T(n-1) + T(n-2) + 1,$$

e resulta polo tanto doado ver que $T(n) = \mathcal{O}(2^n)$ e $T(n) = \Omega(2^{n/2})$. En realidade, tense que $T(n) = \Theta(\varphi^n)$, onde $\varphi = \frac{1+\sqrt{5}}{2}$.
Outro algoritmo de busca que se emprega sobre unha lista ordenada é a chamada *busca ternaria*. Neste caso, divídese a lista en tres metades iguais; comparando o valor buscado cos extremos do intervalo central, podemos reducirnos a unha lista na que o tamaño é un terzo da inicial.

Definición 4.4. Un algoritmo de ordenación é un algoritmo que coloca os elementos dunha lista seguindo a orde dada por unha relación de orde.

Polo xeral, empregaremos as relacións de orde dadas pola orde numérica ou a orde lexicográfica. Calquera algoritmo de ordenación precisa, polo menos, $\Omega(n)$ operacións, xa que terá que visitar, como mínimo, tódolos elementos da lista. Dise que un algoritmo de ordenación é de *propósito xeral* se funciona comparando unicamente parellas de elementos.

Proposición 4.7. Calquera algoritmo de ordenación de propósito xeral precisa dun tempo de $\Omega(n \log n)$.

Demostración. Hai un total de $n!$ permutacións dunha lista de n elementos, polo que se o algoritmo realiza C comparacións, necesitamos que $2^C \geq n!$ xa que, en caso contrario, non seriamos capaces de diferencias tódalas posibles permutacións. Polo tanto, o número de comparacións é $\Omega(\log(n!))$. Polo visto anteriormente, $\log(n!) \in \Theta(n \log n)$, o que conclúe o resultado. □

Os algoritmos de ordenación máis coñecidos son os seguintes.

- *Selection sort.* O algoritmo divide a lista de elementos en dúas partes: por unha parte os elementos da cal xa están ordenador e outra cos elementos que aínda non están ordenados. Inicialmente, a parte ordenada está baleira. O algoritmo busca o elemento mínimo ou máximo (dependendo da orde que se queira) da parte non ordenada, e intercámbiase co elemento de máis á esquerda da parte non ordenada; a continuación, móvense o resto de elementos da parte non ordenada unha posición á dereita.

  Para atopar o primeiro elemento cómpre realizar $n-1$ comparacións, para o segundo $n-2$, e así sucesivamente. En total, o número de comparacións que se realizan é

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

polo que se trata dun elemento de custo cuadrático.

- *Insertion sort.* Inicialmente, a lista de elementos está dividida en dúas partes: unha, ordenada e outra, desordenada. En cada iteración, o algoritmo colle o primeiro elemento da parte non ordenada e compárao co último elemento da parte ordenada. Se é máis grande, déixao na posición actual e prosegue co elemento que hai á súa dereita. En caso contrario, atopa a posición correcta na parte ordenada da lista, movendo tódolos elementos máis grandes unha posición cara á dereita, colocándoo na posición correcta.

  Un cálculo análogo ao anterior mostra que o algoritmo ten custo cuadrático.

- *Quicksort.* Neste caso, se o número de elementos dunha lista é 0 ou 1, acabamos. En caso contrario, seleccionamos un elemento calquera da lista, ao que chamamos pivote, e que aquí denotamos coa letra x. Facemos unha partición do resto de elementos da lista en dous subconxuntos disxuntos: un conxunto contén os elementos maiores ou iguais que o pivote, e o outro, os elementos menores ou iguais que o pivote. Logo, aplicamos o algoritmo a cada unha das sublistas por separado. A elección do pivote fai que o algoritmo do quicksort poida ter un custo alto ou baixo. No caso peor, que ocorre por exemplo cando a lista está ordenada de xeito crecente ou decrecente, entón o custo é $\Theta(n^2)$. En cambio, no caso mellor, no que o pivote é a mediana, o custo é $\Theta(n \log n)$. Imos establecer logo que o custo esperado é tamén da orde de $n \log n$.

- *Mergesort.* Divídese a parte non ordenada en n sublistas, cada unha cun só elemento. Fusionamos sucesivamente as sublistas, creando sublistas novas ordenadas ata que obteñamos unha soa lista. Tense que

$$T(n) = \begin{cases} \Theta(1) & \text{se } n \leq 1, \\ 2T(n/2) + \Theta(n) & \text{se } n > 1. \end{cases}$$

  Aplicando o teorema de resolución das recorrencias divisorias, temos que $T(n) = \Theta(n \log n)$. A diferenza do quicksort, este algoritmo nunca precisa de realizar un número de comparacións da orde de n^2. Porén, presenta outros inconvenientes non relacionados coa eficiencia no tempo de execución, senón na memoria que precisa.

Enunciamos a continuación un resultado importante sobre o quicksort. A modo de notación, S_n denota o conxunto das $n!$ aplicacións bixectivas de $[n]$ en si mesmo; un elemento dese conxunto chámase *permutación*.

Proposición 4.8. Se escollemos as estradas do quicksort de xeito uniforme entre as $n!$ permutacións de $\{1, 2, \ldots, n\}$, o número esperado de comparacións é $\Theta(n \log n)$.

Demostración. Dada unha permutación σ, sexa c_σ o número de comparacións que fai o quicksort. Escribimos $c_{\sigma_{ij}} \in \{0, 1\}$ segundo o i-ésimo elemento se compara co j-ésimo elemento (en cuxo caso vale 1) ou non se compara (en cuxo caso vale 0). Tense que

$$c_\sigma = \sum_{i=1}^{n} \sum_{j=i+1}^{n} c_{\sigma_{ij}}.$$

Temos que o elemento i só se compara co elemento j cando un deles ou é pivote. Polo tanto, a proporción de veces que iso pasa é $\frac{2}{j-i+1}$, xa que se consideramos os $j - i + 1$

números entre i e j (incluíndo a ambos) realizamos a comparación se o pivote é i ou j, pero non cando é calquera dos que están entre eles. Polo tanto,

$$\frac{1}{n!}\sum_{\sigma\in S_n} c_{\sigma_{ij}} = \frac{2}{j-i+1}.$$

Para achar o valor medio de c, facemos a media de tódolos valores de σ, e obtemos

$$\begin{aligned} c &= \sum_{i=1}^{n}\sum_{j=i+1}^{n}\frac{2}{j-i+1} \\ &= 2\sum_{i=1}^{n}\sum_{k=2}^{n-i+1}\frac{1}{k} \\ &\leq 2\sum_{i=1}^{n}\sum_{k=1}^{n}\frac{1}{k} \\ &= 2\sum_{i=1}^{n} H_i \leq 2nH_n = \mathcal{O}(n\log n). \end{aligned}$$

Como xa vimos que o tempo mínimo para un algoritmo de propósito xeral é $\Omega(n\log n)$, concluímos que $T(n) = \Theta(n\log(n))$. □

Rematamos discutindo un algoritmo moi útil para calcular potencias de números, que é a chamada *exponenciación rápida* ou *exponenciación binaria*. A súa vantaxe reside en que reduce drasticamente o número de multiplicacións necesarias, sobre todo cando os expoñentes son grandes. Funciona descompondo o expoñente na súa representación binaria, o que permite calcular a potencia en tempo logarítmico (e non lineal). Imos explicar o algoritmo a través dun exemplo, que é o cálculo de 3^{13}.

1. Descompomos o expoñente 13 na súa representación binaria: $13 = (1101)_2$.

2. Cálculo das potencias de 3 correspondentes a expoñentes que son potencias de dous, sen exceder o número do que se quere calcular a potencia (13 neste caso):

$$3^1 = 3, \quad 3^2 = 9, \quad 3^4 = (3^2)^2 = 9^2 = 81, \quad 3^8 = (3^4)^2 = 81^2 = 6561.$$

3. Realizar as multiplicacións correspondentes á descomposición binaria:

$$3^{13} = 3^{8+4+1} = 3^8 \cdot 3^4 \cdot 3 = 6561 \cdot 81 \cdot 3 = 1594323.$$

Neste caso, en lugar de realizar as 12 operacións que farían falta para calcular 3^{13} segundo o método convencional, realizamos unicamente 5: elevamos ao cadrado tres veces e realizamos dúas multiplicacións ao final.
Este algoritmo pódese presentar tamén de forma recorrente. Para calcular a^{2n}, facemos $(a^n)^2$, de xeito que se precisa unha operación máis que para o cálculo de a^n; e para calcular a^{2n+1}, facemos $(a^n)^2 \cdot a$, de xeito que se precisan dúas operacións máis que para o cálculo de a^n. Polo teorema de resolución de recorrencias subtractivas, precisamos de $\mathcal{O}(\log n)$ operacións.

4.3. Criptografía e algoritmo RSA

A criptografía é a disciplina que se encarga do estudo dos códigos cifrados. As súas orixes remóntanse ao ano 2000 antes de Cristo en Exipto, onde os xeroglíficos eran empregados para decorar as tumbas. Un dos xeitos máis sinxelos de cifrar é o coñecido como *cifrado de substitución*, no que cada carácter é substituído por outro, de xeito bixectivo. Un caso particular é o *cifrado por translación*, no que alfabeto se despraza un número dado de posicións. Se numeramos as letras do 0 ao $n-1$ (sendo n a lonxitude do alfabeto), o cifrado por translación correspóndese coa bixección $x \mapsto x + c$, onde $c \in \{0, 1, \ldots, n-1\}$. Cando $c = 3$, fálase de *cifrado César*.
Outro caso importante é o coñecido como *cifrado afín*.

Definición 4.5. Un cifrado afín nun alfabeto de n letras vén dado por unha bixección de $\mathbb{Z}/n\mathbb{Z}$ da forma $f(x) = ax + b$.

Proposición 4.9. A función $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ dada por $x \mapsto ax + b$ é bixectiva se, e soamente se $\gcd(a, n) = 1$.

Demostración. Para que a función sexa bixectiva, ten que existir unha inversa, é dicir, para cada $y \in \mathbb{Z}/n\mathbb{Z}$ ten que existir un único $x \in \mathbb{Z}/n\mathbb{Z}$ de xeito que $y = f(x) = ax + b$. Iso é equivalente a $ax \equiv y - b \pmod{n}$, que ten unha única solución con independencia do valor de y se, e soamente se, $\gcd(a, n) = 1$. □

Imos explorar agora o algoritmo RSA, que é un método moito máis complexo. Foi desenvolvido por Ron Rivest, Adi Shamir e Leonard Adleman nos anos setenta, e o nome do algoritmo fórmase a partir das iniciais dos seus apelidos.
O algoritmo RSA empregado en criptografía funciona da seguinte maneira.

1. Escóllense dous primos distintos p e q, xeralmente grandes.
2. Calcúlase o seu produto $n = pq$; esta é a primeira das claves públicas.
3. Calcúlase $\varphi(n) = (p-1)(q-1)$. Observamos que $\varphi(n)$ é o número de enteiros menores ou iguais que n que son coprimos con n; se non se coñece o valor de p e q, o seu cálculo é computacionalmente moi custoso.
4. A segunda das claves públicas é un enteiro e que é relativamente primo con $\varphi(n)$.
5. A clave privada é un enteiro d que cumpre que $de \equiv 1 \pmod{\varphi(n)}$, isto é, que é un inverso de e módulo $\varphi(n)$.
6. Para encriptar un número m, calcúlase $m^e \pmod{n}$.
7. Para desencriptar un número t, calcúlase $t^d \pmod{n}$.

Imos considerar un exemplo con primos pequenos para amosar como funciona.

1. Escollemos $p = 7$ e $q = 11$.
2. A primeira clave pública é entón $n = 77$.
3. Tense que $\varphi(n) = 6 \cdot 10 = 60$.
4. A clave pública e pode ser calquera número que sexa coprimo con 60, por exemplo, collemos $e = 7$.

5. Consideramos un inverso de 7 módulo 60. Neste caso, $d = 43$ funciona. Alternativamente, resolvemos
$$7x + 60y = 1$$
empregando a identidade de Bézout. Nese caso, as división sucesivas son $60 = 7 \cdot 8 + 4$, $7 = 4 \cdot 1 + 3$ e $4 = 3 \cdot 1 + 1$. Entón
$$\begin{aligned} 1 &= 4 - 1 \cdot 3 = 4 - 1 \cdot (7 - 1 \cdot 4) \\ &= (-1) \cdot 7 + 2 \cdot 4 = (-1) \cdot 7 + 2 \cdot (60 - 7 \cdot 8) \\ &= 2 \cdot 60 - 17 \cdot 7. \end{aligned}$$
Polo tanto, -17 é un inverso, e podemos coller logo $-17 + 60 = 43$.

6. Para encriptar un número m, facemos m^7 módulo 60. Por exemplo, se $m = 2$, o número encriptado sería
$$2^7 = 128 \equiv 51 \pmod{77}.$$

7. Para desencriptar un número t, facemos t^{43} módulo 60. Por exemplo, se $t = 8$, o número encriptado sería 51^{43} (pódese comprobar que é 2 módulo 77).

Outro tipo de algoritmos que empregan ferramentas da teoría de números son todos aqueles que usan a aritmética de curvas elípticas (ECC) para a encriptación das mensaxes.

Capítulo 5

Combinatoria

A combinatoria é a rama das matemáticas que se encarga de contar. Ao longo deste tema, traballaremos os procedementos básicos, partindo de dous resultados elementais, pero que teñen gran potencial, como son o principio do pombal e o principio do dobre reconto. Tras introducir o vocabulario relativo ás permutacións, ás variacións e ás combinacións, pasamos a traballar as propiedades dos números binomiais (xa introducidos ao traballar o principio de indución) e o principio de inclusión-exclusión.

5.1. Principios básicos de enumeración

O primeiro resultado que se presenta é o coñecido como *principio do pombal*.

Proposición 5.1 (Principio do pombal)**.** Se distribuímos n obxectos en m caixas e $n > m$, polo menos unha das caixas conterá dous ou máis obxectos. Máis en xeral, se distribuímos n obxectos en m caixas e $n > rm$, polo menos unha caixa terá $r + 1$ ou máis obxectos.

Demostración. Procedemos por redución ao absurdo. Se cada caixa ten, como moito, r obxectos, como hai m caixas, o número total de obxecto é menor ou igual que mr, é dicir, $n \leq mr$. Porén, iso é contraditorio coas condicións do enunciado. □

Exemplo. Unha persoa comeu unha bolsa de 22 madalenas ao longo dos sete días da semana. Entón, houbo un día no que comeu polo menos 4 madalenas.

Imos discutir agora un segundo exemplo no cal a aplicación non é tan obvia.

Exemplo. Ao longo de 30 días celebrouse un torneo de tenis. Cada día disputouse polo menos un partido e, en total, non se xogaron máis de 45. Imos demostrar que hai un período de días consecutivos durante os cales se xogaron exactamente 14 partidos.
Para resolver o problema, chamámoslle p_k ao número de partidos que se xogaron o día k, e pomos $s_k = \sum_{i=1}^{k} p_i$ para o número de partidos que se xogaron os primeiros k días. Tense que a sucesión $\{s_1, \ldots, s_{30}\}$ é estritamente crecente, e $s_{30} \leq 45$. Se consideramos agora os 60 números

$$\{s_1, s_2, \ldots, s_{30}, s_1 + 14, s_2 + 14, \ldots, s_{30} + 14\},$$

tense que dous deles teñen que ser iguais polo principio do pombal, xa que todos eles son menores ou iguais que 59. Como $s_i \neq s_j$ se $i \neq j$, e $s_i + 14 \neq s_j + 14$ se $i \neq j$, temos que existen índices i, j de xeito que $s_j = s_i + 14$, polo que $p_{i+1} + \ldots + p_j = 14$, e temos un período de días consecutivos durante os cales se xogaron 14 partidos.

Máis alá das aplicacións elementais do mesmo, imos discutir dous resultados clásicos como son os atribuídos a Erdös–Szekeres e a Dirichlet.

Proposición 5.2 (Erdös–Szekeres)**.** Toda sucesión de n^2+1 números reais diferentes contén unha subsucesión estritamente crecente de lonxitude $n+1$ ou unha sucesión estritamente decrecente de lonxitude $n+1$.

Demostración. Sexa $a_1, a_2, \ldots, a_{n^2+1}$ a sucesión de números reais diferentes. Para cada a_i, consideramos o par (c_i, d_i), onde c_i é a lonxitude da subsucesión estritamente crecente máis longa que comeza en a_i e d_i a da subsucesión estritamente decrecente máis longa que comeza en a_i. Se $c_i > n$ ou $d_i > n$ para algún $i \in [n^2+1]$, entón rematamos. Se $c_i, d_i \leq n$ para todo i, tódolos pares (c_i, d_i) están formados por números entre 1 e n, polo que hai n^2 posibilidades e, polo principio do pombal, dúas deles deben ser iguais, é dicir, $(c_i, d_i) = (c_j, d_j)$, con $i < j$. Se $a_i < a_j$, engadimos a_i á subsucesión estritamente crecente de lonxitude c_j que comeza en a_j e obtemos unha subsucesión estritamente crecente de lonxitude $c_j + 1$ que comeza en a_i, o que é unha contradición con $c_i = c_j$. Se $a_i > a_j$, entón engadimos a_i á subsucesión estritamente decrecente de lonxitude d_j que comeza en a_j e obtemos unha máis longa, contradicindo que $d_i = d_j$. □

Proposición 5.3 (Dirichlet)**.** Para todo número irracional $\alpha \in \mathbb{R}$ e cada natural N hai dous enteiros p e q, con $1 \leq q \leq N$, de xeito que

$$|q\alpha - p| < \frac{1}{N}.$$

En particular, a desigualdade

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

cúmprese para infinitas parellas de enteiros (p, q).

Demostración. Podemos supoñer, sen perder xeneralidade, que $\alpha \in (0, 1)$. Dividimos o intervalo $[0, 1]$ en N subintervalos de lonxitude $1/N$, e consideramos os números $\alpha, 2\alpha, \ldots, (N+1)\alpha$. Dous destes números, $i\alpha$ e $j\alpha$, con $j > i$, teñen a parte fraccionaria no mesmo intervalo. Polo tanto, para algún enteiro p,

$$|(j-i)\alpha - p| < \frac{1}{N}.$$

Pondo $q = j - i \leq N$ e dividindo por q, temos que

$$|\alpha - p/q| < 1/qN \leq 1/q^2.$$

O feito de que haxa infinitos valores de p e q vén de que temos un número finito de intervalos para escoller pero un número infinito de números enteiros. □

Outros dous principios moi habituais en combinatoria, de demostración inmediata, son os coñecidos como *principio da suma* e *principio do produto*.

Proposición 5.4 (Principio da suma)**.** Se A e B son dous conxuntos finitos con intersección baleira, entón $|A \cup B| = |A| + |B|$.

Máis en xeral, se $A_1, \ldots, A_n$ son conxuntos finitos e disxuntos dous a dous, tense que

$$|A_1 \cup \cdots \cup A_n| = |A_1| + \ldots + |A_n|.$$

O principio do produto xa se discutiu ao estudarmos o produto cartesiano de dous conxuntos.

Proposición 5.5 (Principio do produto)**.** Se A e B son dous conxuntos finitos, entón $|A \times B| = |A| \cdot |B|$.

Imos pasar agora a discutir o principio de *dobre reconto*. Afirma que, para sumar as entradas dunha táboa, é o mesmo sumar primeiro cada unha das filas e logo sumar esas cantidades; ca sumar primeiro cada unha das columnas e logo sumar os resultados. A versión continua desta proposición é o coñecido como *teorema de Fubini*, e ambos se poden interpretar como o mesmo resultado desde a óptica da teoría da medida. Antes de formular o enunciado matemático, imos ilustralo co seguinte exemplo que amosa o custo das diferentes comidas ao longo dunha semana.

Día	**Almorzo**	**Xantar**	**Cea**	**Total día**
Luns	5	10	7	22
Martes	4	11	6	21
Mércores	6	9	8	23
Xoves	5	12	7	24
Venres	4	10	6	20
Sábado	5	11	7	23
Domingo	6	9	8	23
Total comida	**35**	**72**	**49**	**156**

Pódese observar que para determinar o prezo total podemos sumar día por día e despois considerar a suma dos 7 días; ou, alternativamente, sumar o correspondente a cada comida e sumar ao final os tres números.

Proposición 5.6 (Principio do dobre reconto)**.** Sexan A e B dous conxuntos finitos e $S \subseteq A \times B$. Para $a \in A$ e $b \in B$ definimos

$$f_a(S) = |\{b \in B \mid (a, b) \in S\}|$$
$$c_b(S) = |\{a \in A \mid (a, b) \in S\}|$$

entón

$$S = \sum_{a \in A} f_a(S) = \sum_{b \in B} c_b(S).$$

Exemplo. Nunha clase de 57 estudantes cada neno coñece exactamente 8 nenas e cada nena coñece exactamente 11 nenos. Sexa m o número de nenas e n o número de nenos. Entón, $11m = 8n$ e $m + n = 57$. Resolvendo o sistema, temos que $m = 24$ e $n = 33$.

Proposición 5.7 (Tríos de Steiner)**.** Un *sistema de tríos de Steiner* é unha colección de subconxuntos de 3 elementos de $[n]$ de xeito que cada parella de dous elementos pertence a un único trío. Se $[n]$ admite un trío de Steiner, entón $n \equiv 1, 3 \pmod 6$.

Demostración. Contaremos de dúas maneiras o conxunto

$$\mathcal{M} = \{((x, y), S) \in [n]^2 \times S \mid x \neq y,\ \{x, y\} \subset S\},$$

onde S é un conxunto de 3 elementos. Para cada parella de puntos hai un único trío que os contén, e cada trío contén 3 parellas. Polo tanto,

$$\frac{n(n-1)}{2} = |\mathcal{M}| = 3|S|.$$

Polo tanto, $|S| = \frac{n(n-1)}{6}$. Isto demostra que n non pode ser congruente con 2 módulo 3.
Falta por demostrar que n ten que ser impar. Para iso, fixamos $x \in [n]$ e miramos as posibilidades para y. Sabemos que existe un único z para o cal $\{x, y, z\}$ é un trío. Como iso é certo para calquera eleccióin de y, estamos dicindo que podemos agrupar tódolos elementos de $[n] - x$ en parellas, polo que $n - 1$ ten que ser un número par. □

En calquera caso, isto non demostra que calquera $n \equiv 1, 3 \pmod 6$ admita un trío de Steiner. O resultado é certo, pero a construción é difícil; para o caso $n = 7$, por exemplo, temos o coñecido como *plano de Fano*.

5.2. Seleccións

O obxectivo desta parte do tema é determinar de cantas maneiras se poden seleccionar k elementos dun conxunto de cardinal n. Porén, antes de resolver problemas de combinatoria, é crucial entender como as condicións poden cambiar o enfoque dos cálculos que cómpre realizar. Importa a orde? Pódense repetir os elementos? Estas son as preguntas que definen o tipo de selección que faremos. Comezamos presentando un resumo das diferentes posibilidades e das respectivas fórmulas, que traballaremos ao longo desta sección.

	Importa orde	**Non importa orde**
Podo repetir	n^k	$\binom{n+k-1}{k}$
Non podo repetir	$n(n-1)\cdots(n-k+1)$	$\binom{n}{k}$

Cando **importa** a orde adoitamos falar de *permutacións* (con repetición ou sen), mentres que cando **non importa** falamos de *combinacións*.

Definición 5.1. Unha *k-permutación con repetición* dun conxunto A de n elementos é unha selección ordenada de k elementos non necesariamente diferentes de A.

Proposición 5.8. O número de k-permutacións con repeticións dun conxunto de n-elementos é n^k.

Demostración. Unha k-permutación con repetición correspóndese cun elemento do produto cartesiano A^k, que ten cardinal $|A|^k$. □

Exemplo. O número de posibles números de teléfono de 9 cifras é 10^9, xa que para calquera cifra podemos escoller calquera elemento de $\{0, 1, 2, \ldots, 9\}$. En xeral, o número de palabras de lonxitude k que se poden formar cun alfabeto de n letras é n^k.

Definición 5.2. Unha *k-permutación* dun conxunto A de n elementos é unha selección ordenada de k elementos diferentes de A.

Proposición 5.9. O número de k-permutacións dun conxunto de n elementos é

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

se $1 \leq k \leq n$, e 0 se $k > n$.

Demostración. Para o primeiro elemento temos n opcións; para o segundo $n-1$ (todas salvo o primeiro); e así ata chegar ao k-ésimo, para o que hai $n-(k-1)$ posibilidades. □

Exemplo. O número de códigos de 4 cifras que se poden formar cos 4 díxitos diferentes é $10 \cdot 9 \cdot 8 \cdot 7$. Máis en xeral, o número de palabras de lonxitude k, con tódalas letras distintas, que se poden formar cun alfabeto de n letras é $n(n-1) \cdot (n-k+1)$.

Un caso especialmente importante dáse cando $n = k$. Nese caso, falamos das permutacións dun conxunto de n elementos.

Definición 5.3. O conxunto das permutacións de $[n]$ denótase por S_n e chámase *grupo simétrico*.

Do resultado anterior, tense que $|S_n| = n!$. Entre as permutacións de $[n]$, hai algunhas que teñen especial relevancia. Por exemplo, as *transposicións* son as permutacións que intercambian entre eles dous elementos diferentes e fixan tódolos demais.

Exemplo. Nunha clase de 5 alumnos, o profesor quere que todos saian ao encerado a facer un exercicio. Poden facer iso de $5! = 120$ xeitos posibles.
En cambio, supoñamos agora que queremos sentar aos 5 alumnos nun círculo; aí, non hai un *primeiro* elemento, de xeito que se fixamos unha posición inicial, é o mesmo ter a permutación $(1, 2, 3, 4, 5)$ que a $(2, 3, 4, 5, 1)$. Polo tanto, o número de opcións neste caso é $5!/5 = 4! = 24$.

Definición 5.4. Unha *k-combinación* dun conxunto A de n elementos é unha selección de k elementos diferentes de A na cal non se ten en conta a orde dos elementos.

Proposición 5.10. O número de k-combinacións dun conxunto de n elementos é

$$\frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$$

se $0 \leq k \leq n$, e 0 se $k > n$.

Exemplo. O número de posibles apostas para a lotería primitiva é $\binom{49}{6}$. Cunha baralla de 52 cartas pódense formar $\binom{52}{5}$ mans de 5 cartas.

Definición 5.5. Unha *k-combinación con repetición* dun conxunto A de n elementos é unha selección non ordenada de k elementos de A non necesariamente diferentes.

Proposición 5.11. O número de k-combinacións con repetición dun conxunto de n elementos é

$$\binom{n+k-1}{k}$$

para $n \geq 1$ e $k \geq 0$.

Demostración. Imos establecer unha bixección entre as k-combinacións e as palabras binarias (formadas por ceros e uns) que constan de k uns e $n-1$ ceros. O número de palabras é claramente $\binom{n+k-1}{k} = \binom{n+k-1}{n-1}$.
Dada unha palabra de lonxitude $n+k-1$, sexa $i_1, \ldots, i_{n-1}$ as posicións dos ceros. Entón, asociámoslle o multiconxunto (conxunto con elementos repetidos) no que o 1 aparece $i_1 - 1$ veces, o 2 $i_2 - i_1 + 1$ veces, e así ata o n, que sairá $n + k - 1 - i_{n-1}$ veces. Reciprocamente, dado un multiconxunto, asociámoslle a palabra que ten primeiro k_1 uns, logo un 0, logo k_2 douses, e así ata chegar ao final, onde pomos k_n veces o n. Está claro que isto é unha bixección, co cal se conclúe a proba. □

Alternativamente, estamos a dicir que a ecuación

$$x_1 + \ldots + x_n = k, \quad x_1, \ldots, x_n \geq 0$$

ten un total de $\binom{n+k-1}{k}$ solucións.
Se, en cambio, consideramos

$$x_1 + \ldots + x_n = k, \quad x_1, \ldots, x_n \geq 1,$$

podemos facer o cambio de variable $y_i = x_i - 1$, de xeito que nos queda a ecuación

$$y_1 + \ldots + y_n = k - n, \quad y_1, \ldots, y_n \geq 0,$$

que ten $\binom{k-1}{n-1}$ solucións. Máis en xeral, sempre que se impón unha condición da forma $x_i \geq r$, podemos facer o cambio $y_i = x_i - r$.

Exemplo. Imos discutir algunhas diferenzas entre os diferentes tipos de selección que comentamos. Consideremos unha orquestra na que hai diferentes instrumentos: violín, viola, clarinete e piano. Nun conservatorio hai 12 alumnos: 5 de violín, 4 de viola, 2 de clarinete e 1 de piano.

(a) Se queremos organizar unha actuación cun músico de cada instrumento, primeiro temos que seleccionar un violín (de 5 maneiras posibles), logo unha viola (de 4) e finalmente un clarinete (de 2). As opcións son $5 \cdot 4 \cdot 2 = 40$.

(b) Se queremos organizar unha actuación con 3 violíns e 2 violas, podemos escoller os violinistas de $\binom{5}{3} = 10$ maneiras e as violas de $\binom{4}{2} = 6$ formas. Polo tanto, hai $10 \cdot 6 = 60$ opcións.

Imos rematar esta sección considerando o caso dos *multiconxuntos*, é dicir, conxuntos nos que se admite que os elementos estean repetidos (pero nos que, como é habitual, non importa a orde). De xeito formal, temos a seguinte definición de multiconxunto.

Definición 5.6. Sexa A un conxunto finito. Un *multiconxunto* de A é unha aplicación $\mu\colon A \to \mathbb{Z}^{\geq 1}$. Dicimos que o tamaño do multiconxunto é k se $\sum_{a \in A} \mu(a) = k$.

Imos establecer como estender os conceptos de permutacións ao caso dos multiconxuntos.

Proposición 5.12. Unha *permutación dun multiconxunto de k elementos* é unha ordenación dos elementos do multiconxunto. Denotamos por $\binom{k}{k_1,\ldots,k_n}$ o número de permutacións do multiconxunto.

Proposición 5.13. Se $k, k_1, \ldots, k_n$ son enteiros non negativos de xeito que $\sum_{i=1}^{n} k_i = k$, entón

$$\binom{k}{k_1, k_2, \ldots, k_n} = \frac{k!}{k_1! k_2! \cdots k_n!}.$$

Demostración. Consideramos o k-multiconxunto $\{1^{k_1}, \ldots, n^{k_n}\}$. Unha ordenación deste multiconxunto queda determinada ao fixarmos as k_1 posicións que ocupará o elemento 1, as k_2 posicións que ocupará o elemento 2 e así sucesivamente. Podemos escoller as k_1 posicións de 1 de $\binom{k}{k_1}$ maneiras; entre as $k - k_1$ restantes podemos escoller as k_2 posicións que ocupará o 2 de $\binom{k-k_1}{k_2}$ maneiras; e así sucesivamente. Polo tanto, o número de ordenacións do multiconxunto é

$$\binom{k}{k_1}\binom{k-k_1}{k_2}\cdots\binom{k-k_1-\ldots-k_{n-1}}{k_n}.$$

Aplicando a fórmula dos factoriais á expresión anterior, obtemos o que queriamos demostrar. □

5.3. Propiedades dos números binomiais e multinomiais

Os *números combinatorios* ou *números binomiais*, que xa aparecen na sección anterior, representan o número de maneiras de seleccionar k obxectos dun conxunto de n elementos. Consideramos que unicamente toman valores diferentes de 0 cando $0 \leq k \leq n$. Nese caso, como xa se discutiu con anterioridade, pódense calcular como

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}.$$

En particular, tense que

$$\binom{n}{k} = \binom{n}{n-k}.$$

Os números binomiais cumpren a recorrencia

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

A demostración deste tipo de identidades pódese realizar de xeito alxébrico ou de xeito combinatorio. Imos amosalo neste caso concreto.

- **De xeito alxébrico.**

$$\begin{aligned}\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} \\ &= \frac{(n-1)!(n-k) + (n-1)!k}{k!(n-k)!} \\ &= \frac{n!}{k!(n-k)!} = \binom{n}{k}.\end{aligned}$$

- **De xeito combinatorio.** Nun conxunto de n elementos, podemos separar un deles. Entón, de cara a escoller k, ou ben seleccionamos o último ou non. Nos casos nos que si o seleccionamos, temos que escoller $k-1$ elementos entre os $n-1$ restantes. En cambio, se non o seleccionamos, temos que escoller k elementos entre os $n-1$ restantes. Polo tanto,

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Unha identidade importante e que xa se discutiu que involucra aos números binomiais é o *binomio de Newton*. Para $a, b \in \mathbb{R}$, cúmprese que

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Exemplo. Pondo no binomio de Newton $a = b = 1$, temos que

$$2^n = \sum_{k=0}^{n} \binom{n}{k}.$$

Pondo $a = -1$ e $b = 1$, resulta que

$$0 = \sum_{k=0}^{n} (-1)^k \binom{n}{k}.$$

Imos pór agora outro exemplo máis complexo.

Proposición 5.14 (Fórmula de Vandermonde)**.** Sexan m, n, r tres enteiros positivos. Entón,

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}.$$

Demostración. Imos dar dúas demostracións deste resultado, unha de tipo alxébrico e outro de tipo combinatorio.
Comezamos coa alxébrica. Polo teorema do binomio de Newton temos que

$$(1+x)^{m+n} = \sum_{r=0}^{m+n} \binom{m+n}{r} x^r.$$

Ao mesmo tempo, temos que

$$\begin{aligned}\sum_{r=0}^{m+n} \binom{m+n}{r} x^r &= (1+x)^{m+n} \\ &= (1+x)^m (1+x)^n \\ &= \Big(\sum_{i=0}^{m} \binom{m}{i} x^i\Big)\Big(\sum_{j=0}^{n} \binom{n}{j} x^j\Big) \\ &= \sum_{r=0}^{m+n} \Big(\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}\Big) x^r.\end{aligned}$$

Comparando os coeficientes con x^r temos o resultado buscado.
Imos dar agora unha demostración de tipo combinatorio. Nunha urna con m bólas de color azul e n bólas de color vermello, queremos escoller r. Iso podémolo facer de $\binom{m+n}{r}$ formas. Alternativamente, podemos comezar decidindo o número de bólas de cor azul, k que seleccionamos, que pode ser calquera número entre 0 e r (entendendo que se $r > m$ non é posible). Nese caso, collemos $\binom{m}{k}$ de cor azul e as $r-k$ restantes escollémolas de $\binom{n}{r-k}$ formas; polo tanto, o número de maneiras de escoller k de cor azul e $r-k$ de cor vermello é $\binom{m}{k}\binom{n}{r-k}$. Sumando para os valores de k entre 0 e r temos o resultado. □

Un corolario importante é o seguinte: pondo $m = n = r$ obtemos que

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2.$$

A seguinte proposición resume outras propiedades relevantes dos números binomiais.

Proposición 5.15. Sexan n e k dous enteiros non negativos. Cúmprense as seguintes propiedades:

(a) $\sum_{r=0}^{k} \binom{n+r}{r} = \binom{n+k+1}{k}$.

(b) $\sum_{r=0}^{k} \binom{n+r}{n} = \binom{n+k+1}{n+1}$.

Demostración. A primeira parte é consecuencia da ecuación recorrente que cumpren os números binomiais:

$$\begin{aligned}\binom{n+k+1}{k} &= \binom{n+k}{k} + \binom{n+k}{k-1} \\ &= \binom{n+k}{k} + \binom{n+k-1}{k-1} + \binom{n+k-1}{k-2} \\ &= \binom{n+k}{k} + \binom{n+k-1}{k-1} + \binom{n+k-2}{k-2} + \ldots + \binom{n+1}{1} + \binom{n+1}{0} \\ &= \sum_{r=0}^{k} \binom{n+r}{r}.\end{aligned}$$

A segunda parte é consecuencia inmediata da primeira, observando que $\binom{n+r}{n} = \binom{n+r}{r}$. □

Proposición 5.16 (Teorema do multinomio)**.** Para todo enteiro $m \geq 0$, tense que

$$(a_1 + a_2 + \ldots + a_r)^m = \sum_{m_1+\ldots+m_r=m} \binom{m}{m_1, \ldots, m_r} a_1^{m_1} \cdots a_r^{m_r}.$$

Demostración. Os termos da expresión

$$(a_1 + a_2 + \ldots + a_r)^m = (a_1 + a_2 + \ldots + a_r) \cdots (a_1 + a_2 + \ldots + a_r)$$

obtéñense multiplicando de tódolos xeitos posibles un dos sumandos $a_1, \ldots, a_r$ de cada factor, é dicir, son expresións da forma $x_1 x_2 \cdots x_m$, onde $x_i \in \{a_1, \ldots, a_r\}$ representa o sumando do i-ésimo factor. Se agrupamos as m variables, obtemos unha expresión da forma $a_1^{m_1} \cdots a_r^{m_r}$, onde $m_1 + \ldots + m_r = m$ e onde ademais os expoñentes m_i son non negativos. O coeficiente correspondente a $a_1^{m_1} \cdots a_r^{m_r}$ é polo tanto o número de expresións $x_1 \cdots x_n$ onde as variables $a_1, \ldots, a_r$ aparecen respectivamente $m_1, \ldots, m_r$ veces. Hai tantas como posibles ordenacións do multiconxuntos $\{a_1^{m_1}, \ldots, a_r^{m_r}\}$, é dicir, $\binom{m}{m_1,\ldots,m_r}$. □

Exemplo. Imos calcular o coeficiente con xy^5z^2 na expansión de $(x - 2y + 3z)^8$. O coeficiente que aparece na suma é

$$\begin{aligned}\binom{8}{1,5,2} x^1(-2y)^5(3z)^2 &= \frac{8!}{1! \cdot 5! \cdot 2!} x \cdot (-32y^5) \cdot (9z^2) \\ &= 168 \cdot (-32 \cdot 9) x y^5 z^2 \\ &= -48384 x y^5 z^2.\end{aligned}$$

5.4. Principio de inclusión-exclusión

Consideremos unha familia de conxuntos finitos, $A_1, A_2, \ldots, A_n$. Unha k-intersección dos conxuntos é calquera conxunto da forma $A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}$, con $1 \leq i_1 < i_2 < \cdots < i_k \leq n$. Definimos

$$\alpha_k = \sum_{1 \leq i_1 < \ldots < i_k \leq n} |A_{i_1} \cap \ldots A_{i_k}|.$$

Proposición 5.17 (Principio de inclusión-exclusión)**.** Para calquera familia de conxuntos finitos $A_1, \ldots, A_n$,

$$|A_1 \cup \ldots A_n| = \sum_{k=1}^{n} (-1)^{k+1} \alpha_k.$$

Demostración. Imos ver que cada elemento $a \in A_1 \cup A_2 \cup \ldots \cup A_n$ se conta exactamente unha vez na expresión $\sum_{k=1}^{n} (-1)^{k+1} \alpha_k$. Para iso, supoñamos que a pertence exactamente a r deses conxuntos, é dicir, $a \in A_{i_1} \cup \ldots \cup A_{i_r}$, pero non pertence aos outros conxuntos. Deste xeito, o elemento a cóntase r veces en α_1, $\binom{r}{2}$ veces en α_2, $\binom{r}{3}$ veces en α_3, e así sucesivamente. Polo tanto, o número de veces que estamos a contar o elemento a é

$$r - \binom{r}{2} + \ldots + (-1)^{r+1} \binom{r}{r} = 1 - \left(\binom{r}{0} - \binom{r}{1} + \ldots + (-1)^r \binom{r}{r} \right) = 1,$$

como queriamos ver. □

Exemplo. Un grupo de alumnos e alumnas examinouse de matemáticas, de historia e de latín. Houbo 10 aprobados en matemáticas, 20 en historia e 25 en latín. Sabemos ademais, que 5 aprobaron matemáticas e historia, 7 matemáticas e latín e 12 historia e latín. Finalmente, houbo só 3 alumnos que aprobaran os 3 exames. Se queremos saber cantos alumnos aprobaron polo menos un exame, aplicamos o principio de inclusión-exclusión e temos

$$10 + 20 + 25 - 5 - 7 - 12 + 3 = 34.$$

Definición 5.7. Un *desarranxo* de $[n]$ é calquera permutación σ de $[n]$ de xeito que $\sigma(i) \neq i$ para todo $i \in [n]$. O número de desarranxos de $[n]$ denótase por D_n.

Proposición 5.18. O número de desarranxos de $[n]$ é

$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Demostración. Para $i \in [n]$, definimos o conxunto

$$A_i = \{\sigma \mid \sigma \text{ é unha permutación de } [n] \text{ e } \sigma(i) = i\}.$$

Os desarranxos son as permutacións do complementario de $A_1 \cup \ldots \cup A_n$. Imos calcular o cardinal deste conxunto empregando o principio de inclusión-exclusión:

$$|A_1 \cup \ldots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \alpha_k.$$

O cardinal de $A_{i_1} \cap \ldots \cap A_{i_r}$ é $(n-r)!$, xa que se están a fixar os valores das permutacións en $i_1, \ldots, i_r$. Polo tanto,

$$\alpha_r = \binom{n}{r} (n-r)! = \frac{n!}{r!}.$$

De aquí dedúcese que o número de desarranxos é

$$\begin{aligned} D_n &= n! - |A_1 \cup \ldots \cup A_n| \\ &= n! - \sum_{r=1}^{n} (-1)^{r+1} \alpha_r \\ &= n! - \sum_{r=1}^{n} (-1)^{r+1} \frac{n!}{r!} \\ &= n! \Big(1 - \frac{1}{1!} + \frac{1}{2!} + \ldots + (-1)^n \frac{1}{n!}\Big) \\ &= n! \sum_{r=2}^{n} \frac{(-1)^r}{r!}, \end{aligned}$$

como se quería demostrar. □

Por exemplo, tense que

$$D_5 = 120 - (5 \cdot 4! - 10 \cdot 3! + 10 \cdot 2! - 5 \cdot 1! + 1 = 44.$$

É un exercicio interesante comprobar que

$$\lim_{n \to \infty} \frac{D_n}{n!} = e^{-1}.$$

Isto é, a proporción de desarranxos no conxunto das permutacións tende a $1/e$.
Imos discutir outra das aplicacións habituais do principio de inclusión-exclusión, que é o cálculo do número de aplicacións sobrexectivas entre dous conxuntos.

Proposición 5.19. O número de aplicacións sobrexectivas $f\colon A \to B$, onde $|A| = k$ e $|B| = n$, é

$$\sum_{i=1}^{n} (-1)^{n-i} \binom{n}{i} i^k.$$

Demostración. Sexa $B = \{b_1, \ldots, b_n\}$, e definimos

$$F_i = \{f\colon A \to B\colon f^*(b_i) = \emptyset\}.$$

As aplicacións non sobrexectivas son as do conxunto $F_1 \cup \ldots \cup F_n$. Por outra banda, as intersección $F_{i_1} \cap \ldots \cap F_{i_r}$ correspóndense coas aplicacións para as cales $i_1, \ldots, i_r$ non están na imaxe da aplicación. Polo tanto, $|F_{i_1} \cap \ldots \cap F_{i_r}| = (n-r)^k$. Aplicando o principio de inclusión exclusión temos que o número de aplicacións sobrexectivas é

$$\begin{aligned} n^k - |F_1 \cup \ldots \cup F_n| &= n^k - \sum_{r=1}^{n} (-1)^{r+1} \binom{n}{r} (n-r)^k \\ &= \sum_{r=0}^{n} (-1)^r \binom{n}{r} (n-r)^k. \end{aligned}$$

Facendo o cambio de variable $i = n - r$, a expresión anterior pode escribirse como

$$\sum_{i=1}^{n} (-1)^{n-i} \binom{n}{i} i^k.$$

□

A seguinte táboa resume o número de aplicacións bixectivas, inxectivas e sobrexectivas entre dous conxuntos finitos.

$f\colon A \to B, \quad \lvert A\rvert = k, \lvert B\rvert = n$		
Total		n^k
Bixectiva	$n = k$	$n!$
Inxectiva	$k \leq n$	$\binom{n}{k}k!$
Sobrexectiva	$k \geq n$	$\sum_{i=1}^{n}(-1)^{n-i}\binom{n}{i}i^k$

Exemplo. Imos contar o número de maneiras de conseguir unha suma de 16 ao tirar catro dados de seis caras cada un. Iso é equivalente a contar as solucións positivas de $x + y + z + t = 16$, pero nas que temos que impor que $x, y, z, t \leq 6$. O número de solucións enteiras positivas é $\binom{15}{3} = 455$. Se $x > 6$, podemos pór $x = 6 + x'$ e temos que descontar polo tanto as solucións enteiras positivas de $x' + y + z + t = 10$, que son $\binom{9}{3} = 84$. O mesmo ocorre para $y > 6$, $z > 6$ e $t > 6$. Finalmente, como restamos dúas veces aquelas nas que dous dos dados son maiores que 6, temos que volvelas sumar. Se $x, y > 6$, a única opción é $x = y = 7$ e $z = t = 1$, polo que o resultado é

$$455 - 4 \cdot 84 + 6 \cdot 1 = 125.$$

5.5. Particións dun conxunto

Definición 5.8. Sexan k, n dous enteiros positivos. Unha k-partición dun conxunto A de n elementos é unha colección $\{A_1, \ldots, A_k\}$ de subconxuntos non baleiros de A, disxuntos dous a dous, e tal que a unión é A. O número de k-particións dun conxunto é o *número de Stirling de segunda especie* e pomos $\left\{{n \atop k}\right\}$.

Proposición 5.20. Cúmprense as seguintes propiedades:

(a) $\left\{{n \atop 1}\right\} = \left\{{n \atop n}\right\} = 1$.

(b) $\left\{{n \atop k}\right\} = 0$ se $k > n$.

(c) $\left\{{n \atop 2}\right\} = 2^{n-1} - 1$.

(d) $\left\{{n \atop k}\right\} = \left\{{n-1 \atop k-1}\right\} + k\left\{{n-1 \atop k}\right\}$ se $n \geq 3$ e $n - 1 \geq k \geq 2$.

(e) $\left\{{n \atop k}\right\} = \frac{1}{k!}\sum_{i=1}^{k}(-1)^{k-i}\binom{k}{i}i^n$.

Demostración. (a) Inmediata.

(b) Trivial.

(c) Observamos que unha parte dunha partición en 2 subconxuntos coas condicións que se piden está formada por un subconxunto non baleiro e diferente do total e o seu complementario. O número de subconxuntos non baleiros e diferentes do total é $2^n - 2$, e cómpre dividir entre 2 porque non importa a orde. Obtense así o resultado buscado.

(d) Fixamos un dos elementos do conxunto. Hai dúas opcións: se ese elemento está só na súa parte, entón hai que dividir os restantes $n - 1$ en $k - 1$ partes; senón, dividimos os $n-1$ restantes en k partes e podemos engadir o elemento distinguido a calquera delas.

(e) O número de aplicacións sobrexectivas $f\colon A \to B$, con $|A| = k$ e $|B| = n$ é $\left\{ {k \atop n} \right\} n!$. A partir da expresión para o número de aplicacións sobrexectivas temos o resultado buscado.

□

Exemplo. A propiedade (d) permite calcular de xeito recursivo os números de Stirling de segunda especie. Imos ilustralo cun exemplo no que tamén se usa a propiedade(c):

$$\begin{aligned}
\left\{ {8 \atop 3} \right\} &= 63 + 3 \cdot \left\{ {7 \atop 3} \right\} \\
\left\{ {7 \atop 3} \right\} &= 31 + 3 \cdot \left\{ {6 \atop 3} \right\} \\
\left\{ {6 \atop 3} \right\} &= 15 + 3 \cdot \left\{ {5 \atop 3} \right\} \\
\left\{ {5 \atop 3} \right\} &= 7 + 3 \cdot \left\{ {4 \atop 3} \right\} \\
\left\{ {4 \atop 3} \right\} &= 3 + 3 \cdot \left\{ {3 \atop 3} \right\} = 6.
\end{aligned}$$

Unha vez temos $\left\{ {4 \atop 3} \right\}$, podemos calcular os anteriores:

$$\left\{ {5 \atop 3} \right\} = 25, \quad \left\{ {6 \atop 3} \right\} = 90, \quad \left\{ {7 \atop 3} \right\} = 301, \quad \left\{ {8 \atop 3} \right\} = 966.$$

Alternativamente, a propiedade (e) permite calcular $\left\{ {8 \atop 3} \right\}$ directamente:

$$\left\{ {8 \atop 3} \right\} = \frac{3 \cdot 1^8 - 3 \cdot 2^8 + 3^8}{6} = 966.$$

Para determinar tódalas posibles maneiras de realizar particións dun conxunto (é dicir, sen importar o número de partes), introducimos a noción de número de Bell.

Definición 5.9. O número de particións dun conxunto de n elementos é o *número de Bell* B_n:

$$B_n = \sum_{k=1}^{n} \left\{ {n \atop k} \right\}.$$

Outro concepto que desenvolveremos máis adiante é o de *partición dun enteiro*. De cara a presentar a seguinte táboa, adiantamos a definición. Unha *k-partición* dun enteiro n é unha expresión de n como suma de k enteiros positivos sen ter en conta a orde dos sumandos. Escribimos $p_k(n)$ para representar o número de k-particións de n, e $p(n)$ para o número de particións de n.

Exemplo. Para determinar $p_3(8)$ observamos que

$$\begin{aligned}
8 &= 6 + 1 + 1 \\
8 &= 5 + 2 + 1 \\
8 &= 4 + 3 + 1 \\
8 &= 4 + 2 + 2 \\
8 &= 3 + 3 + 2.
\end{aligned}$$

Polo tanto, $p_3(8) = 5$. Non incluímos casos como $8 = 3 + 4 + 1$ xa que é o mesmo que $8 = 4 + 3 + 1$.

A seguinte táboa representa o número de maneiras de distribuír n bólas en k caixas, segundo as bólas ou as caixas sexan distinguibles ou non distinguibles entre si.

	Bólas dist.	**Bólas non dist.**
Caixas dist.	k^n	$\binom{n+k-1}{n}$
Caixas non dist.	$\sum_{i=1}^{k} \left\{ {n \atop i} \right\}$	$\sum_{i=1}^{k} p_i(n)$

Imos repetir a mesma táboa se impomos que en cada caixa teña que haber, polo menos, unha bóla.

	Bólas dist.	**Bólas non dist.**
Caixas dist.	$k! \left\{ {n \atop k} \right\}$	$\binom{n-1}{n-k}$
Caixas non dist.	$\left\{ {n \atop k} \right\}$	$p_k(n)$

Imos repetir agora o cálculo se impomos que en cada caixa ten que haber polo menos unha bóla.

5.6. Números de Catalan

Sexa $n \geq 1$ un enteiro positivo. Sexa C_n o número de maneiras de ir do punto $(0,0)$ ao punto $(2n,0)$, facendo unicamente pasos cara á dereita, que poden ser ascendentes ou descendentes, e de xeito que nunca pasemos ao semiplano negativo (con $y < 0$); a modo de notación, podemos falar de pasos da forma $(1,1)$ (ascendentes) ou da forma $(1,-1)$ (descendentes). É unha comprobación rutineira ver que iso se corresponde co número de camiños do $(0,0)$ ao (n,n), facendo unicamente pasos de lonxitude 1 cara á dereita ou cara á arriba, e sen cruzar nunha a diagonal $y = x$ (é dicir, sen estar nunca nunha posición da forma (i,j), con $j > i$). Por simplicidade, definimos $C_0 = 1$.
Sexa P_n o número de sucesións de n parénteses de apertura e n parénteses de peche, de xeito que sexan *correctas*, é dicir, todo paréntese de peche se corresponda cun de apertura.
Finalmente, sexa T_n o número de maneiras de *triangular* un polígono convexo de $n+2$ lados en triángulos, usando unicamente diagonais e de xeito que non haxa segmentos que se cortan fóra dos vértices.

Proposición 5.21. Tense que

$$C_n = P_n = T_n = \frac{1}{n+1}\binom{2n}{n}.$$

Demostración. En primeiro lugar, a correspondencia entre camiños, parénteses e triangulacións procede mediante unha bixección estándar. Imos polo tanto contar os camiños de $(0,0)$ a $(2n,0)$ cumprindo as restricións que se dan na definición. Consideramos en primeiro lugar tódolos camiños de $(0,0)$ a $(2n,0)$, utilizando segmentos da forma $(1,1)$ e $(1,-1)$. En total hai $\binom{2n}{n}$, xa que equivale a contar palabras de lonxitude $2n$ con n parénteses de apertura e n de peche. Imos contar agora os camiños que cruzan o eixe OX, é dicir, que pasan por algún punto de ordenada -1. A cada un destes camiños podémoslle asignar o camiño de $(0,-2)$ a $(2n,0)$ que se obtén ao facer unha simetría con respecto á recta $y = -1$ do anaco de vai de $(0,0)$ ao primeiro punto de ordenada -1 e deixando igual o resto do camiño. Polo tanto, temos tantos camiños que atravesan o eixe OX como camiños de $(0,-2)$ a $(2n,0)$ con segmentos da forma $(1,1)$ e $(1,-1)$. O

número destes camiños é $\binom{2n}{n+1}$, porque temos que escoller $n+1$ lugares para colocarmos o movemento ascendente. Polo tanto,

$$\begin{aligned} C_n &= \binom{2n}{n} - \binom{2n}{n+1} = \frac{(2n)!}{n!n!} - \frac{(2n)!}{(n+1)!(n-1)!} \\ &= \frac{(2n)!}{n!n!}\Big(1 - \frac{n}{n+1}\Big) = \frac{1}{n+1}\binom{2n}{n}. \end{aligned}$$

□

Os números que aparecen na proposición anterior coñécense como números de Catalan, en referencia ao matemático belga Eugène Catalan. Calculando, temos $C_1 = 1$, $C_2 = 2$, $C_3 = 5$, $C_4 = 14$, $C_5 = 42$ e así sucesivamente.

Capítulo 6

Recorrencias

O obxectivo deste tema é estudar as chamadas sucesións recorrentes, nas que os termos se definen en función dos anteriores. Para iso, introducimos unhas ferramentas de gran utilidade, as chamadas *funcións xeradoras*. Posteriormente, empréganse para o estudo das recorrencias lineais, tanto homoxéneas como non homoxéneas, e péchase o tema facendo unha introdución ás particións de enteiros.
O problema *clásico* que podemos ter en mente ao longo deste tema é o da sucesión de Fibonacci, unha das máis clásicas da matemática. A sucesión de Fibonacci, presente en diferentes ámbitos (por exemplo, na bioloxía), defínese como

$$\begin{cases} f_0 = 0, \\ f_1 = 1, \\ f_n = f_{n-1} + f_{n-2} \quad \text{se } n \geq 2. \end{cases}$$

Un problema que a priori non é nada trivial é o seguinte: pódese atopar unha forma pechada para a sucesión, é dicir, que non dependa dos termos anteriores. A resposta é afirmativa:

$$f_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n.$$

Para chegar a esta conclusión, empregaremos as técnicas de funcións xeradoras, que desenvolveremos na primeira parte do tema.

6.1. Sucesións recorrentes

Definición 6.1. Unha sucesión (a_n) dise que é *recorrente* se, salvo os primeiros termos, a_n pódese obter en función de n e dos termos anteriores. A *ecuación da recorrencia* dunha sucesión é unha expresión $f(a_{n-1}, \ldots, a_0, n)$ que se cumpre para todo n a partir dun determinado valor.

Exemplo. A sucesión de factoriais é recorrente, xa que se pode definir mediante a fórmula

$$a_0 = 1, \quad a_n = n a_{n-1} \text{ para todo } n \geq 1.$$

A sucesión dos números de Catalan tamén é recorrente, porque se cumpre que $C_0 = 1$ e

$$C_n = \sum_{k=0}^{n-1} C_k C_{n-k-1} \quad \text{para todo } n \geq 1.$$

Para demostralo, pensamos en termos de parénteses, n de apertura e n de peche, e consideramos a posición da paréntese de peche correspondente á paréntese de apertura. Por exemplo, se está ao final de todo, entre as dúas quedan $n-1$ parénteses de apertura e de peche. En xeral, esta paréntese de peche deixa k parénteses de apertura e peche á esquerda e $n-1-k$ á dereita, onde $0 \leq k \leq n-1$. Polo tanto, temos que $C_n = \sum_{k=0}^{n-1} C_k C_{n-k-1}$, como queriamos ver. Convén observar que pór $C_0 = 1$ representa a convención de que ao empregarmos 0 parénteses, enténdese que existe unha única palabra, que é a palabra baleira.

Definición 6.2. Unha sucesión (a_n) é *recorrente de orde k* se, excepto os k primeiros termos, cada termo se pode obter en función dos k anteriores. É dicir, para todo $n \geq n_0$, cúmprese unha ecuación recorrente do tipo

$$a_{n+k} = f(a_{n+k-1}, a_{n+k-2}, \ldots, a_n, n).$$

Resolver unha recorrencia consiste en atopar unha expresión xeral para o termo a_n, é dicir, unha expresión que non dependa dos termos anteriores. Isto pode facerse mediante diferentes procedementos, por exemplo, por indución.

Exemplo. Definimos a sucesión $a_0 = 0$ e $a_n = 2a_{n-1} + 1$ para todo $n \geq 1$. Calculando, temos que $a_1 = 1$, $a_2 = 3$, $a_3 = 7$ e así sucesivamente. Isto suxire conxecturar que $a_n = 2^n - 1$. Para $n = 0$ o resultado é certo. Supoñámolo certo para n e demostrémolo para $n+1$:

$$a_{n+1} = 2a_n + 1 = 2(2^n - 1) + 1 = 2^{n+1} - 2 + 1 = 2^{n+1} - 1.$$

Outra alternativa consiste en manipular sucesivamente a expresión ata chegar a unha expresión explícita.

Exemplo. Definimos a sucesión $a_0 = 1$ e $a_n = 3a_{n-1} + 1$ para todo $n \geq 1$. Se aplicamos iterativamente a definición, obtemos que

$$\begin{aligned} a_n &= 3a_{n-1} + 1 \\ &= 3(3a_{n-2} + 1) = 9a_{n-2} + 3 \\ &= 9(3a_{n-3} + 1) + 3 + 1 = 27a_{n-3} + 9 + 3 + 1 \\ &= 3^n a_0 + 3^{n-1} + \ldots + 9 + 3 + 1 = 3^n + 3^{n-1} + \ldots + 9 + 3 + 1 \\ &= \frac{3^{n+1} - 1}{2}. \end{aligned}$$

Imos discutir dous exemplos moi clásicos de sucesións recorrentes.

Definición 6.3. Unha *progresión aritmética* con termo inicial a e diferenza d e unha sucesión definida por $a_0 = a$ e $a_{n+1} = a_n + d$, para todo $n \geq 0$. Unha *progresión xeométrica* con termo inicial a e razón r e unha sucesión definida por $a_0 = a$ e $a_{n+1} = a_n \cdot r$, para todo $n \geq 0$.

Ao longo deste tema, empregaremos con frecuencia que a suma dos primeiros termos dunha progresión xeométrica con termo inicial a e razón $r \neq 1$ vén dada por

$$S_n = \sum_{i=0}^{n} \frac{a_0(r^{n+1} - 1)}{r - 1}.$$

Se a razón cumpre que $|r| < 1$, o límite desta suma cando n tende a infinito é

$$S := \lim_{n \to \infty} S_n = \frac{a_0}{1 - r}.$$

6.2. Funcións xeradoras

As series de potencias son as xeneralizacións naturais dos polinomios. Mentres que un polinomio (con coeficientes en $\mathbb{C}$) é unha expresión do tipo

$$a_0 + a_1 x + \ldots + a_n x^n, \quad a_0, a_1, \ldots, a_n \in \mathbb{C},$$

as series de potencias terán infinitos coeficientes. Isto pode ocasionar problemas de converxencia: por exemplo, se consideramos a serie $f(x) = \sum_{n\geq 0} x^n$ e avaliamos en $x = 2$, temos que

$$f(2) = 1 + 2 + 2^2 + \ldots,$$

que obviamente non é un número como tal. Porén, neste contexto traballaremos coas series desde un punto de vista puramente *formal*, esquecéndonos de calquera consideración sobre a súa rexión de converxencia.

Definición 6.4. Unha *serie formal* de potencias sobre $\mathbb{C}$ é unha expresión do tipo

$$\sum_{n\geq 0} a_n x^n,$$

onde $a_n \in \mathbb{C}$ para todo $n \geq 0$. O conxunto das series formais sobre $\mathbb{C}$ denótase por $\mathbb{C}[\![x]\!]$. Neste conxunto pódense definir dúas operacións, a *suma* e o *produto*. Sexan $A(x) = \sum_{n\geq 0} a_n x^n$ e $B(x) = \sum_{n\geq 0} b_n x^n$ dous elementos de $\mathbb{C}[\![x]\!]$.

- A suma $A(x) + B(x)$ é a serie formal de potencias

$$A(x) + B(x) = \sum_{n\geq 0} (a_n + b_n) x^n.$$

- O produto $A(x)B(x)$ é a serie formal de potencias

$$A(x)B(x) = \sum_{n\geq 0} c_n x^n, \quad \text{con } c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

Finalmente, escribimos $0 = \sum_{n\geq 0} 0 \cdot x^n$ e $1 = 1 + \sum_{n\geq 1} 0 \cdot x^n$ para as series 0 e 1, que desempeñarán un importante papel no estudo das series de potencias.

En particular, temos que $\mathbb{C}[x]$ é un espazo vectorial (de dimensión finita), e tamén é un anel, xa que temos definido un produto. A seguinte proposición resume as principais propiedades das series de potencias. Demostramos unicamente a (g), sendo as outras unha comprobación rutineira.

Proposición 6.1. As series de potencias cumpren as seguintes propiedades.

(a) A suma de series formais de potencias é conmutativa e asociativa.

(b) O produto de series formais de potencias é conmutativo e asociativo.

(c) O produto é distributivo con respecto á suma.

(d) A serie 0 é o elemento neutro da suma.

(e) A serie $-A(x)$ é a oposta da serie $A(x)$.

(f) A serie 1 é o elemento neutro do produto.

(g) A serie $A(x) \in \mathbb{C}[\![x]\!]$ é invertible se, e soamente se, $a_0 \neq 0$.

Demostración. (g) Comezamos observando que a inversa é unha serie de potencias $B(x) \in \mathbb{C}[\![x]\!]$ de xeito que $A(x)B(x) = 1$. Pomos $A(x) = \sum_{n\geq 0} a_n x^n$ e $B(x) = \sum_{n\geq 0} b_n x^n$. Como $A(x)B(x) = 1$, temos que $a_0 b_0 = 1$ e

$$\sum_{i=0}^{n} a_i b_{n-i} = 0 \quad \text{se } n \geq 1.$$

Polo tanto, $A(x)$ non ten inversa se $a_0 = 0$. Se $a_0 \neq 0$, podemos definir de xeito recursivo os números $b_n \in \mathbb{C}$, de xeito que se cumpran as condicións anteriores. Como $a_0 \neq 0$, definimos $b_0 = 1/a_0$. Supoñamos agora que temos definidos números $b_0, \dots b_{n-1}$ de xeito que $\sum_{i=0}^{k} a_i b_{k-i} = 0$ para todo k con $1 \leq k \leq n-1$. Da ecuación para b_n, deducimos que

$$b_n = \frac{-1}{a_0} \sum_{i=1}^{n} a_i b_{n-i} \in \mathbb{C}.$$

□

Exemplo. A inversa de $\sum_{n\geq 0} x^n$ é $1-x$, xa que $(1-x)\sum_{n\geq 0} x^n = 1$. Alternativamente, podemos interpretar $\sum_{n\geq 0} x^n$ como a suma dunha progresión xeométrica de razón x e primeiro termo igual a 1.

O obxectivo do que queda de sección é explicar como empregar as series de potencias para o estudo de diferentes tipos de sucesións, especialmente as sucesións recorrentes.

Definición 6.5. A función xeradora ordinaria da sucesión (a_n) é a serie formal de potencias

$$A(x) = \sum_{n\geq 0} a_n x^n.$$

Definición 6.6. Sexa $A(x)$ unha serie formal. A *derivada formal* de $A(x)$ (ou simplemente *derivada*) é a serie

$$A'(x) = \sum_{n\geq 1} (n a_n) x^{n-1}.$$

Observamos que para calcular o coeficiente con x^n na serie $A(x)$ podemos coller o termo constante en $\frac{A^{(n)}(x)}{n!}$.
A seguinte proposición resume as propiedades máis importantes das funcións xeradoras.

Proposición 6.2. Sexan $A(x)$ e $B(x)$ as funcións xeradoras ordinarias das sucesións (a_n) e (b_n).

(a) $A(x) + B(x)$ é a función xeradora ordinaria da sucesión $(a_n + b_n)$.

(b) $A(x)B(x)$ é a función xeradora ordinaria de (c_n), onde $c_n = \sum_{i=0}^{n} a_i b_{n-i}$.

(c) $\alpha A(x)$ é a función xeradora ordinaria de (αa_n).

(d) $A'(x)$ é a función xeradora ordinaria de $((n+1)a_{n+1})$.

(e) $x^m A(x)$ é a función xeradora ordinaria da sucesión que comeza con m ceros e logo segue con $a_0, a_1, \ldots,$

(f) Se $m \geq 1$,
$$\frac{A(x) - a_0 - a_1 x - \ldots - a_{m-1}x^{m-1}}{x^m}$$
é a función xeradora ordinaria da sucesión $a_m, a_{m+1}, \ldots$.

(g) $A(\alpha x)$ é a función xeradora ordinaria da sucesión $(\alpha^n a_n)$.

(h) $A(x^m)$ é a función xeradora ordinaria da sucesión que introduce entre cada termo de (a_n) un total de $m-1$ ceros.

(i) $A(x)/(1-x)$ é a función xeradora ordinaria da sucesión de sumas parciais.

Demostración. Tódalas propiedades son consecuencia directa das propiedades das series de potencias. Imos discutir a proba dalgunha delas.

(d) Pola definición de derivada formal, a serie $A'(x)$ ten por coeficiente n-ésimo $(n+1)a_n$, polo que $A'(x)$ é a función xeradora da sucesión que ten ese coeficiente n-ésimo.

(i) Temos que a sucesión $(a_0, a_1, a_2, \ldots)$ se pode escribir como
$$(a_0, a_1, a_2, \ldots) + (0, a_0, a_1, \ldots) + (0, 0, a_0, \ldots) + \ldots$$
A función xeradora do primeiro sumando é $A(x)$, a do segundo é $xA(x)$, a do terceiro $x^2A(x)$, e así sucesivamente. Polo tanto, a función xeradora é
$$A(x)(1 + x + x^2 + \ldots) = \frac{A(x)}{1-x}.$$

□

Exemplo. Sexa $s_n = 1^2 + 2^2 + \ldots + n^2$.

- Comezamos coa función xeradora da sucesión na que tódolos termos son iguais a 1, que é $\frac{1}{1-x}$.
- A partir da anterior, aplicando sumas parciais, temos que a función xeradora de $a_n = n$ é $\frac{x}{(1-x)^2}$. Alternativamente, podemos derivar e desprazar unha posición, chegando ao mesmo resultado.
- Combinando derivación e desprazamento cara á dereita, temos que a de $(0, 1^2, 2^2, \ldots)$ é $\frac{x+x^2}{(1-x)^3}$.
- Aplicando sumas parciais novamente, temos que o resultado é
$$\frac{x + x^2}{(1-x)^4}.$$

Exemplo. Sexa $t_n = n2^n$. Nese caso, unha vez sabemos que a función xeradora da sucesión $a_n = n$ é $\frac{x}{(1-x)^2}$, temos que, pola propiedade (e), a función xeradora de t_n é
$$\frac{3x}{(1-3x)^2}.$$

Exemplo. Imos considerar un terceiro exemplo. Sexa (f_n) a sucesión de Fibonacci, na que se cumpre que $f_0 = 0$, $f_1 = 1$ e $f_n = f_{n-1} + f_{n-2}$ se $n \geq 2$. Denotamos por $F(x)$ a función xeradora asociada. Podemos entón calcular, a partir desa, a función xeradora de $(f_2, f_3, \ldots)$, simplemente aplicando a propiedade (f). Nese caso,

$$f_2 + f_3 x + f_4 x^2 + \ldots = \frac{F(x) - f_0 - f_1 x}{x^2} = \frac{F(x) - x}{x^2}.$$

Imos traballar agora un exemplo máis complicado relacionado cos números binomiais.

Proposición 6.3. Para todo enteiro $m \geq 1$, tense que

$$\frac{1}{(1-x)^m} = \sum_{n \geq 0} \binom{m+n-1}{m-1} x^n.$$

Demostración. Pomos

$$\frac{1}{(1-x)^m} = (1 + x + x^2 + \ldots)^m.$$

Obtemos x^n na expresión anterior cada vez que collemos x^{i_1}, x^{i_2}, e así ata x^{i_m} de cada un dos m factores da expresión anterior con $i_1 + \ldots + i_m = n$, onde os $i_j \geq 0$. O número de solucións en enteiros positivos desa ecuación sabemos que é $\binom{m+n-1}{m-1}$, como queriamos ver. □

En particular,

$$\frac{1}{(1-\alpha x)^m} = \sum_{n \geq 0} \binom{m+n-1}{m-1} \alpha^n x^n.$$

Finalmente, presentamos a seguinte xeneralización do teorema do binomio de Newton que empregaremos, por exemplo, para estudar os números de Catalan.

Proposición 6.4. Para todo enteiro $m \geq 1$,

$$(1+x)^{-m} = \sum_{n \geq 0} \binom{-m}{n} x^n.$$

Exemplo. Temos que

$$\binom{1/2}{n} = \frac{(-1)^{n-1}(2n-3)!!}{2^n n!},$$

onde $n!!$ refírese ao produto dos enteiros positivos menores ou iguais que n e que teñen a mesma paridade que n.

Imos ver agora como empregar as ferramentas de funcións xeradoras para a resolución de recorrencias. Para iso, desenvolveremos un exemplo con detalle, seguindo estes pasos.

1. Identificación da función xeradora de cada lado da recorrencia $A(x)$, empregando as propiedades elementais de desprazamento.

2. Igualar os dous termos para obter unha expresión racional para $A(x)$.

3. Descompoñer en fraccións simples a expresión de $A(x)$.

4. Identificar cada un dos sumandos.

Exemplo. Consideramos a sucesión (a_n) definida por $a_0 = 2$, $a_1 = 4$ e

$$a_{n+2} = 4a_{n+1} - 3a_n \quad \text{para todo } n \geq 0.$$

Sexa $A(x) = \sum_{n=0}^{\infty} a_n x^n$. Imos considerar a función xeradora do lado esquerdo e do lado dereito da ecuación anterior. Temos que

$$a_2 + a_3 x + a_4 x^2 + \ldots = \frac{A(x) - a_0 - a_1 x}{x^2} = \frac{A(x) - 2 - 4x}{x^2}.$$

De xeito similar,

$$4a_{n+1} - 3a_n = \frac{4(A(x) - 2)}{x} - 3A(x).$$

Igualando as dúas expresións e multiplicando por x^2, quédanos a ecuación

$$A(x) - 2 - 4x = 4xA(x) - 8x - 3x^2 A(x).$$

Polo tanto,

$$A(x) = \frac{-4x + 2}{3x^2 - 4x + 1}.$$

De cara a identificar de que sucesión se trata, descompoñemos a expresión en fraccións simples:

$$3x^2 - 4x + 1 = (x - 1)(3x - 1),$$

polo que

$$\frac{-4x + 2}{3x^2 - 4x + 1} = \frac{A}{x - 1} + \frac{B}{3x - 1}.$$

Igualando as expresións, obtemos que $A = -1$ e $B = -1$. Polo tanto,

$$A(x) = \frac{1}{1 - x} + \frac{1}{1 - 3x}.$$

Temos que $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$ e

$$\frac{1}{1 - 3x} = \sum_{n=0}^{\infty} (3x)^n.$$

Polo tanto, $a_n = 1 + 3^n$.

Imos tratar agora outra situación na que na descomposición en fraccións simples temos raíces múltiples.

Exemplo. Consideramos agora a sucesión (a_n) definida por $a_0 = 1$, $a_1 = 4$, $a_2 = 28$, $a_3 = 32$ e

$$a_{n+4} = 8a_{n+2} - 16a_n \quad \text{para todo } n \geq 0.$$

Sexa $A(x) = \sum_{n=0}^{\infty} a_n x^n$. Imos considerar a función xeradora do lado esquerdo e do lado dereito da ecuación anterior. Temos que

$$a_4 + a_5 x + a_6 x^2 + \ldots = \frac{A(x) - 1 - 4x - 28x^2 - 32x^3}{x^4}.$$

De xeito similar,

$$8a_{n+2} - 16a_n = \frac{8(A(x) - 1 - 4x)}{x^2} - 16A(x).$$

Igualando as dúas expresións e multiplicando por x^2, quédanos a ecuación

$$A(x) - 1 - 4x - 28x^2 - 32x^3 = 8x^2A(x) - 8x^2 - 32x^3 - 16x^4A(x).$$

Polo tanto,

$$A(x) = \frac{20x^2 + 4x + 1}{16x^4 - 8x^2 + 1}.$$

De cara a identificar de que sucesión se trata, descompoñemos a expresión en fraccións simples:

$$16x^4 - 8x^2 + 1 = (2x + 1)^2(2x - 1)^2,$$

polo que, descompoñendo en fraccións simples,

$$\frac{12x^2 + 4x + 1}{16x^4 - 8x^2 + 1} = \frac{-1}{2x + 1} + \frac{1}{(2x + 1)^2} + \frac{1}{2x - 1} + \frac{2}{(2x - 1)^2}.$$

Temos agora o seguinte:

(a) a sucesión asociada á función $\frac{-1}{2x+1}$ é $-(-2)^n$;

(b) a asociada a $\frac{1}{(2x+1)^2}$ é $(n + 1)(-2)^n$;

(c) a asociada a $\frac{1}{2x-1}$ é -2^n;

(d) finalmente, a asociada a $\frac{2}{(1-2x)^2}$ é $(2n + 2)2^n$.

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

Un exemplo menos obvio no que atopar a función xeradora require dalgunhas manipulacións previas é o caso dos números de Catalan.

Proposición 6.5. Sexa $C(x)$ a función xeradora dos números de Catalan. Cúmprese que

$$C(x) = \frac{1 - \sqrt{1 - 4x}}{2x}.$$

Demostración. Temos que $C(x) = \sum_{n\geq 0} C_n x^n$. Podemos observar que

$$\begin{aligned} C(x) &= C_0 + \sum_{n\geq 1} C_n x^n \\ &= C_0 + \sum_{n\geq 1} \left(\sum_{k=0}^{n-1} C_k C_{n-k-1} \right) x^n \\ &= 1 + x \sum_{n\geq 0} \left(\sum_{k=0}^{n} C_k C_{n-k} \right) x^n \\ &= 1 + xC(x)^2. \end{aligned}$$

Isto correspóndese coa ecuación de segundo grao

$$xC(x)^2 - C(x) + 1 = 0,$$

polo que

$$C(x) = \frac{1 \pm \sqrt{1 - 4x}}{2x}.$$

Como se ten que cumprir que

$$\lim_{x\to 0} C(x) = C_0 = 1,$$

necesariamente hai que coller o signo menos, polo que

$$C(x) = \frac{1-\sqrt{1-4x}}{2x}.$$

□

Este resultado pódese empregar para dar unha demostración alternativa de que o termo xeral da sucesión correspondente aos números de Catalan é $\frac{1}{n+1}\binom{2n}{n}$. Para iso, observamos que

$$\begin{aligned}\sqrt{1-4x} &= \sum_{n\geq 0}\binom{1/2}{n}(-4x)^n \\ &= \sum_{n\geq 0}\binom{n-3/2}{n}4^n x^n \\ &= 1+\sum_{n\geq 1}\binom{n-3/2}{n}4^n x^n \\ &= 1+4x\sum_{n\geq 0}\binom{n-1/2}{n+1}4^n x^n.\end{aligned}$$

Iso quere dicir que

$$C_n = -2^{2n+1}\binom{n-1/2}{n+1}.$$

Polo tanto, desenvolvendo o coeficiente binomial,

$$C_n = -\frac{2^{2n+1}}{(n+1)!}\prod_{i=0}^{n}\left(n-\frac{1}{2}-i\right) = -\frac{2^n}{(n+1)!}\prod_{i=0}^{n}(2n-1-2i).$$

O produto consta de tódolos números impares entre -1 e $2n-1$, polo que se pode escribir como

$$C_n = \frac{2^n}{(n+1)!}\prod_{i=1}^{n}(2i-1) = \frac{1}{n!(n+1)!}\prod_{i=1}^{n}(2i-1)(2i) = \frac{1}{n+1}\binom{2n}{n}.$$

Na última sección tamén veremos outro exemplo de función xeradora, a correspondente ás particións dun enteiro, cuxo estudo será moito máis complicado.

6.3. Resolucións de recorrencias

O obxectivo desta sección é presentar un método xeral para resolver de xeito sistemático certos tipos de recorrencias. Nos exemplos anteriores, as recorrencias lineais amosaban o mesmo patrón: a función xeradora tiña un denominador con información sobre a recorrencia e un numerador de grao menor que o denominador que codificaba os termos iniciais. Imos formalizar esta idea.

Definición 6.7. Unha sucesión (a_n) é *recorrente lineal con coeficientes constantes de orde k* se cumpre unha ecuación recorrente de tipo

$$a_{n+k} + c_1 a_{n+k-1} + c_2 a_{n+k-2} + \ldots + c_k a_n = f(n),$$

onde $c_1, \ldots, c_k \in \mathbb{C}$, $c_k \neq 0$. Se $f(n) = 0$, dicimos que a sucesión é *homoxénea*; en caso contrario, dicimos que é *non homoxénea*.

As principais recorrencias que traballamos son as homoxéneas e as non homoxéneas con termos da forma $p(n)a^n$, onde $p(n)$ é un polinomio e $a \in \mathbb{R}$. Presentamos de forma esquemática o xeito de proceder en cada caso.
Comezamos co caso homoxéneo

$$a_{n+i} = c_{i-1} a_{n+i-1} + \ldots + c_0 a_n.$$

1. Calcúlase a ecuación característica reemprazando a_{n+i} por X^i.
2. Áchanse as solucións da ecuación característica (por exemplo, por Ruffini). Imos supor, neste primeiro acercamento, que as raíces son todas reais (é dicir, que non son números complexos).
3. Escribimos o termo xeral como

   $$a_n = p_{\lambda_1}(n)\lambda_1^n + \ldots + p_{\lambda_r}(n)\lambda_r^n,$$

   onde $p_{\lambda_i}(n)$ é un polinomio de grao $m_\lambda - 1$ con m_λ parámetros, sendo m_λ a multiplicidade de λ como raíz da ecuación característica.
4. Determinamos os parámetros empregando as condicións iniciais.

Imos ilustrar o método con dous exemplos. No primeiro, as raíces son simples, polo que a resolución é inmediata.

Exemplo. Consideramos a recorrencia

$$a_{n+2} = 5a_{n+1} - 6a_n, \quad a_0 = 1,\ a_1 = 4.$$

A ecuación característica é

$$X^2 = 5X - 6,$$

e aplicando Ruffini temos que

$$X^2 - 5X + 6 = (X-2)(X-3) = 0.$$

A expresión da recorrencia é por tanto

$$a_n = \alpha \cdot 2^n + \beta \cdot 3^n.$$

Pondo $n = 0$ e $n = 1$,

$$\begin{aligned} 1 &= \alpha + \beta \\ 4 &= 2\alpha + 3\beta. \end{aligned}$$

Resolvendo, obtemos que $\alpha = -1$ e $\beta = 2$, polo que

$$a_n = -2^n + 2 \cdot 3^n.$$

No segundo caso que imos amosar, unha das raíces é dobre. Iso quere dicir que temos que considerar polinomios de grao 1 (e non simplemente constantes) multiplicando á exponencial.

Exemplo. Consideramos agora a recorrencia

$$b_{n+3} = 4b_{n+2} - 5b_{n+1} + 2b_n, \quad b_0 = 5,\ b_1 = 9,\ b_2 = 16.$$

A ecuación característica é

$$X^3 = 4X^2 - 5X + 2,$$

polo que, aplicando Ruffini, quédanos

$$X^3 - 4X^2 + 5X - 2 = (X-1)^2(X-2) = 0.$$

A expresión da recorrencia é por tanto

$$b_n = (\alpha + \beta n) \cdot 1^n + \gamma \cdot 2^n.$$

Pondo $n = 0$, $n = 1$ e $n = 2$,

$$\begin{aligned} 5 &= \alpha + \gamma \\ 9 &= \alpha + \beta + 2\gamma \\ 16 &= \alpha + 2\beta + 4\gamma. \end{aligned}$$

Resolvendo, obtemos que $\alpha = 2$, $\beta = 1$ e $\gamma = 3$, polo que

$$b_n = 2 + n + 3 \cdot 2^n.$$

Pasamos agora ao caso non homoxéneo da forma

$$a_{n+i} = c_{i-1}a_{n+i-1} + \ldots + c_0 a_n + \mu_1^{n+i} p_1(n) + \ldots + \mu_k^{n+i} p_k(n).$$

1. Calcúlase a ecuación característica reemprazando a_{n+i} por X^i.
2. Áchanse as solucións da ecuación característica (por exemplo, por Ruffini). A multiplicidade dunha raíz λ, neste contexto, é a multiplicidade como raíz da ecuación característica máis $d+1$, onde d é o grao do polinomio que sae con λ^{n+i}.
3. Escribimos o termo xeral como

   $$a_n = p_{\lambda_1}(n)\lambda_1^n + \ldots + p_{\lambda_r}(n)\lambda_r^n,$$

   onde $p_{\lambda_i}(n)$ é un polinomio de grao $m_\lambda - 1$ con m_λ parámetros, sendo m_λ a multiplicidade de λ como raíz da ecuación característica.
4. Determinamos os parámetros empregando as condicións iniciais.

Exemplo. Consideramos a recorrencia

$$a_{n+2} = 5a_{n+1} - 6a_n + 1, \quad a_0 = 1,\ a_1 = 4.$$

A ecuación característica é

$$X^2 = 5X - 6,$$

polo que, aplicando Ruffini, quédanos que

$$X^2 - 5X + 6 = (X-2)(X-3) = 0.$$

A expresión da recorrencia é por tanto

$$a_n = \alpha \cdot 2^n + \beta \cdot 3^n + \gamma \cdot 1^n,$$

xa que a parte non homoxénea é $1^n \cdot (1)$. Tense ademais que $a_2 = 15$. Pondo $n = 0$, $n = 1$ e $n = 2$,

$$\begin{aligned} 1 &= \alpha + \beta + \gamma \\ 4 &= 2\alpha + 3\beta + \gamma \\ 15 &= 4\alpha + 9\beta + \gamma. \end{aligned}$$

Resolvendo, obtemos que $\alpha = -2$, $\beta = 5/2$ e $\gamma = 1/2$, polo que

$$a_n = -2^{n+1} + \frac{5}{2} \cdot 3^n + \frac{1}{2}.$$

Finalmente, observamos que as raíces tamén poden ser complexas.

Exemplo. Consideramos a recorrencia

$$a_{n+2} = -4a_n, \quad a_0 = 1,\ a_1 = 2.$$

A ecuación característica é

$$X^+4 = (X + 2i)(X - 2i).$$

A expresión da recorrencia é por tanto

$$a_n = \alpha \cdot (2i)^n + \beta \cdot (-2i)^n.$$

Pondo $n = 0$ e $n = 1$,

$$\begin{aligned} 1 &= \alpha + \beta \\ 2 &= 2i\alpha - 2i\beta. \end{aligned}$$

Resolvendo, obtemos que $\alpha = \frac{1-i}{2}$ e $\beta = \frac{1+i}{2}$, polo que

$$a_n = \frac{1-i}{2}(2i)^n + \frac{1+i}{2} \cdot (-2i)^n.$$

Alternativamente, observando que as raíces complexas son $\pm 2i$, podemos escribir

$$a_n = 2^n \left(a \cos\left(\frac{\pi}{2} n\right) + b \sin\left(\frac{\pi}{2} n\right) \right).$$

Pondo $n = 0$, temos que $a = 1$, e pondo $n = 1$, obtemos $b = 1$. Polo tanto,

$$a_n = 2^n \left(\cos\left(\frac{\pi}{2} n\right) + \sin\left(\frac{\pi}{2} n\right) \right).$$

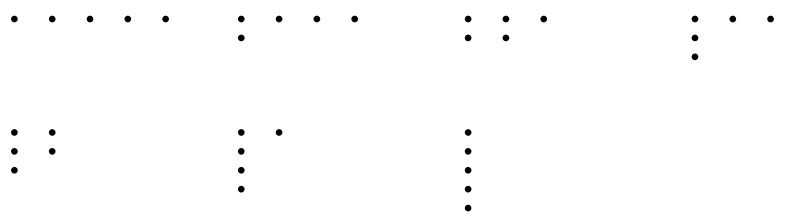
As dúas expresións que obtivemos son equivalentes.

6.4. Particións de enteiros

Definición 6.8. Unha *k-partición* dun enteiro n é unha expresión de n como suma de k enteiros positivos sen ter en conta a orde dos sumandos. Escribimos $p_k(n)$ para representar o número de k-particións de n, e $p(n)$ para o número de particións de n.

Exemplo. As 3-particións de 7 son $(5,1,1)$, $(4,2,1)$, $(3,3,1)$ e $(3,2,2)$, polo que $p_3(7) = 4$. Os primeiros valores da sucesión $(p(n))$ son $p(1) = 1$, $p(2) = 1$, $p(3) = 3$, $p(4) = 5$ e $p(5) = 7$.

O *diagrama de Ferrers* da partición $(x_1, \ldots, x_k)$ de n é unha representación gráfica que consiste en distribuír n puntos en k filas con x_i puntos en cada unha aliñados á esquerda. Imos representar os diagramas de Ferrers das setes particións correspondentes ao 5.



Proposición 6.6. A función xeradora da sucesión $(p(n))_{n\geq 0}$, onde $p(n)$ é o número de particións dun enteiro $n \geq 1$ e $p(0) = 1$, é

$$P(x) = \prod_{i\geq 1} \frac{1}{1-x^i}.$$

Máis en xeral, sexa $q_k(n)$ o número de particións de n onde tódalas partes son menores ou iguais a k. Entón,

$$\sum_{n\geq 0} q_1(n)x^n = \frac{1}{1-x}, \quad \sum_{n\geq 0} q_2(n)x^n = \frac{1}{1-x}\frac{1}{1-x^2}, \ldots$$

Proposición 6.7. O número de particións de n en partes diferentes é igual ao número de particións de n en partes impares.

Demostración. Imos dar unha demostración con funcións xeradoras, aínda que tamén é posible establecer unha bixección entre os dous conxuntos empregando os diagramas de Ferrers. A función xeradora ordinaria da sucesión que conta o número de particións de n en partes diferentes é

$$P_1(x) = \prod_{i\geq 1}(1+x^i),$$

mentres que a función xeradora ordinaria que conta o número de particións en partes impares é

$$P_2(x) = \prod_{i\geq 1} \frac{1}{1-x^{2i-1}}.$$

Para comprobar que as dúas funcións son iguais, observamos que

$$\begin{aligned} P_1(x) &= \prod_{i\geq 1} \frac{(1+x^i)(1-x^i)}{1-x^i} \\ &= \frac{\prod_{i\geq 1}(1-x^{2i})}{\prod_{i\geq 1}(1-x^i)} \\ &= \frac{1}{1-x^{2i-1}} = P_2(x). \end{aligned}$$

□

Capítulo 7

Teoría de grafos

A teoría de grafos, polo xeral moi ligada ao estudo da combinatoria, é o estudo de certas estruturas matemáticas que teñen un gran interese tanto desde o punto de vista da modelización como da matemática pura.

7.1. Definicións básicas

Definición 7.1. Un *grafo* é un par (V, A), onde V é un conxunto finito non baleiro e $A \subseteq \{\{u, v\} \mid u, v \in V,\ u \neq v\}$. Os elementos de V chámanse *vértices* e os de A, *arestas*.

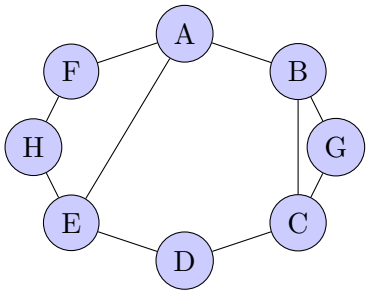
A representación gráfica dun grafo $G = (V, A)$ consiste en debuxar un punto no plano por cada vértice de V é unha curva con extremos u e v por cada aresta $\{u, v\}$. Esta definición admite diferentes variantes que son interesantes nalgúns contextos. Por exemplo, permitir máis dunha aresta entre dous vértices (*arestas múltiples*) e tamén arestas dun vértice a si mesmo (*lazos*), ademais de considerar as arestas como pares ordenados (*digrafos* ou *grafos dirixidos*).

Definición 7.2. Sexan $G = (V, A)$ e $G' = (V', A')$ dous grafos. Un *isomorfismo* de G a G' é unha aplicación bixectiva $f\colon V \to V'$ de xeito que $uv \in A$ se, e soamente se, $f(u)f(v) \in A'$. Nese caso, dicimos que G e G' son isomorfismos, e escribimos $G \equiv G'$. Un *automorfismo* do grafo G é un isomorfismo de G a G.

Definición 7.3. Sexan u e v vértices dun grafo $G = (V, A)$. Un $u - v$ *recorrido de lonxitude* k é unha sucesión $u_0, u_1, \ldots, u_k$ con $u_0 = u$, $u_k = v$ e de xeito que $u_i u_{i+1} \in A$ para todo $0 \leq i \leq k-1$. Un $u-v$ *camiño* é un $u-v$ recorrido onde todos os vértices son diferentes. Un recorrido dise que é *pechado* se $u = v$. Un *ciclo* é un recorrido pechado de lonxitude polo menos 3 no que todos os vértices son diferentes, excepto o primeiro é o último.
Dicimos que un *sendeiro* é un recorrido que non repite arestas, e un *circuíto* é un sendeiro pechado.

Definición 7.4. A orde e a medida de G son $|V|$ e $|A|$, respectivamente. O *grao* dun vértice u é $g(u) = |\{v \mid uv \in A\}|$. O maior e o menor dos graos dun grafo G denótanse por $\Delta(G)$ e $\delta(G)$.
A *sucesión de graos* dun grafo G de orde n é unha lista de lonxitude n onde aparecen os graos dos vértices de G en orde decrecente.

Exemplo. O seguinte é un grafo de 8 vértices e 10 arestas. A sucesión de graos dos vértices é $(3, 3, 3, 2, 3, 2, 2, 2)$.



Se dous grafos son isomorfos, teñen a mesma sucesión de graos. O recíproco, en cambio, non é certo.

Exemplo. Se $G = (V, A)$ é un grafo de orde n e medida m, entón $m \leq \binom{n}{2}$. Do mesmo xeito, dado un conxunto de vértices $V = \{u_1, \ldots, u_n\}$, hai $2^{n(n-1)/2}$ grafos diferentes, xa que cada parella de vértices pode estar unida ou non por unha aresta.

Proposición 7.1 (Lema do apertón de mans)**.** Nun grafo (V, A) cúmprese que

$$\sum_{u \in V} g(u) = 2|A|.$$

De aquí dedúcese, por exemplo, que todo grafo contén un número par de vértices de grao impar. Por outra banda, se G é un grafo d-regular de orde n e medida m, entón $nd = 2m$.

Definición 7.5. Sexa G un grafo con $V = \{v_1, \ldots, v_n\}$ e $A = \{a_1, \ldots, a_m\}$. A *matriz de adxacencia* de G é unha matriz $M_A(G)$ con n filas e n columnas, tal que o elemento da fila i e da columna j é

$$\begin{cases} 1 & \text{se } v_i \sim v_j; \\ 0 & \text{en caso contrario.} \end{cases}$$

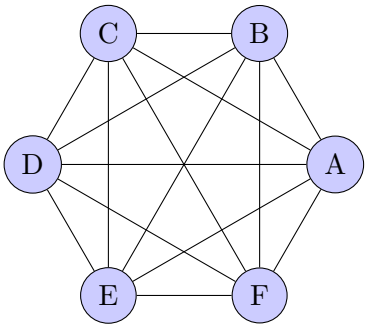
A *matriz de incidencia* é unha matriz $M_I(G)$ con n filas e m columnas, tal que o elemento da fila i e a columna j é

$$\begin{cases} 1 & \text{se } v_i \text{ é incidente con } a_j; \\ 0 & \text{en caso contrario.} \end{cases}$$

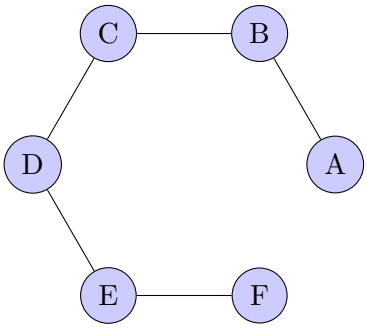
Tanto a matriz de adxacencia como a de incidencia dependen da ordenación escollida de vértices e arestas. En ambas matrices, a suma das entradas da fila i é $g(v_i)$.
Imos presentar agora algúns grafos. Sexa n un enteiro positivo e $V = \{x_1, x_2, \ldots, x_n\}$.

- O *grafo nulo* de orde n, que denotaremos N_n, é o grafo de orde n e medida 0. Ao grafo N_1 chámaselle *grafo trivial*.

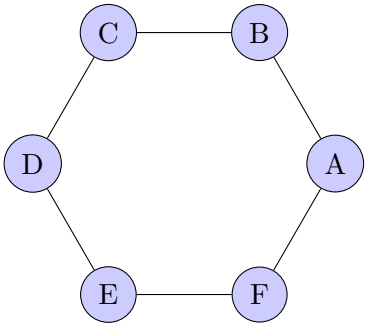
- O *grafo completo* de orde n, que denotaremos K_n, é o grafo de orde n que ten tódalas arestas posibles, $\binom{n}{2}$. O seguinte debuxo representa o grafo completo de seis vértices, K_6.



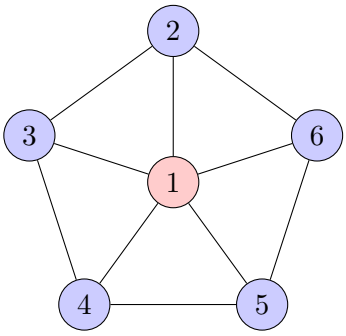
- O *grafo traxecto* de orde n, que denotaremos por $T_n = (V, A)$, é o grafo que ten por conxunto de arestas $A = \{x_1x_2, x_2x_3, \ldots, x_{n-1}x_n\}$. Amosamos aquí o debuxo correspondente ao grafo T_6.



- O *grafo ciclo* de orde $n \geq 3$, que denotaremos por $C_n = (V, A)$ é o grafo que ten por conxunto de arestas $A = \{x_1x_2, x_2x_3, \ldots, x_{n-1}x_n, x_nx_1\}$. Amosamos aquí o debuxo correspondente ao grafo C_6.



- O *grafo roda* de orde $n \geq 4$, que denotamos por $W_n = (V, A)$ é o grafo que ten por conxunto de arestas $A = \{x_1x_2, x_2x_3, \ldots, x_{n-1}x_1\} \cup \{x_nx_1, x_nx_2, \ldots, x_nx_{n-1}\}$. Amosamos a continuación un exemplo.



Definición 7.6. Sexan r e s enteiros positivos. Un grafo é *r-regular* se todos os vértices teñen grao r. Un grafo $G = (V, A)$ é *bipartito* se o conxunto de vértices V admite unha partición en dúas partes $\{V_1, V_2\}$ de xeito que toda aresta ten un extremo en V_1 e outro en V_2. Os conxuntos V_1 e V_2 chámanse as *partes estables* de G. En caso de que cada vértice de V_1 sexa adxacente a todos os vértices de V_2 dicimos que o grafo é *bipartito completo* e denotámolo por $K_{r,s} = (V, A)$, onde $|V_1| = r$ e $|V_2| = s$. Ao grafo $K_{1,s}$ chámaselle *grafo estrela*.

Exemplo. O grafo $K_{r,s}$ ten $r + s$ vértices e rs arestas. É regular unicamente cando $r = s$. A partir de aquí, podemos ver que un grafo bipartito de n vértices ten, como moito $\frac{n^2}{4}$ arestas. Se as partes estables teñen r e s vértices, con $r + s = n$, entón temos que o número máximo de arestas pódese acoutar superiormente por

$$|A| \leq rs \leq \left(\frac{r+s}{2}\right)^2 = \frac{n^2}{4},$$

onde na primeira desigualdade empregouse que $4rs \leq (r + s)^2$ para $r, s \in \mathbb{R}^{>0}$.

Presentamos agora o concepto de subgrafo e algunhas nocións relacionadas.

Definición 7.7. Sexa $G = (V, A)$ un grafo. Dicimos que $H = (V', A')$ é un *subgrafo* de G se H é un grafo tal que $V' \subseteq V$ e $A' \subseteq A$. Dicimos que o subgrafo é un *subgrafo xerador* de G se $V' = V$.
Se $S \subseteq V$ e S non é baleiro, o subgrafo de G *xerado* ou *inducido* por S ten S como conxunto de vértices e o conxunto de arestas está formado por tódalas arestas de G incidentes en dous vértices de S. De xeito similar, se $T \subseteq A$ e A non é baleiro, o subgrafo de G *xerado* ou *inducido* por T ten como conxunto de vértices todos aqueles incidentes a algunha das arestas de T e o conxunto de arestas é T.
Unha *clique* nun grafo $G = (V, A)$ é un conxunto de vértices, $C \subset V$, no que calquera par de vértices distintos son adxacentes. É dicir, é un subgrafo no que cada vértice está conectado a tódolos demais vértices do subgrafo, o que equivale a dicir que o subgrafo de G inducido por C é un grafo completo.

A partir dun grafo, podemos realizar diferentes construcións auxiliares relativas á adición ou á eliminación dun vértice ou aresta. Sexa $G = (V, A)$, con $|V| = n$ e $|A| = m$.

1. *Supresión dun vértice $u \in V$.* É o grafo que se obtén eliminando o vértice u e tódalas arestas incidentes con u. Trátase dun grafo de orde $n - 1$ e medida $m - g(u)$.

2. *Supresión dunha aresta $a \in A$.* É o grafo que se obtén suprimindo a aresta a. Trátase dun grafo da mesma orde e medida $m - 1$.

3. *Adición dunha aresta* $a = uv \notin A$, con $u, v \in V$. É o grafo que se obtén a partir de G engadindo unha aresta que non é de G. Trátase dun grafo da mesma orde e medida $m + 1$.

4. *Contracción dunha aresta* $a = uv \in A$. É o grafo que se obtén identificando dous vértices incidentes á aresta a. É un grafo de orde $n - 1$ e medida

$$m - 1 - |\{w \in V \mid uw \in A \text{ e } vw \in A\}|.$$

Imos discutir por último agora algunhas operacións con grafos.

1. *Grafo complementario* de G. É o grafo $G^c = (V, A')$, onde

$$A' = \{uv \mid u, v \in V \text{ e } uv \notin A\}.$$

Polo tanto, G^c é un grafo de orde n, medida $\binom{n}{2} - m$, e, para todo vértice $u \in V$,

$$g_G(u) + g_{G^c}(u) = n - 1.$$

2. *Grafo liña* de G. Se G é un grafo de medida m, con $m \geq 1$, definimos o grafo liña como o grafo $L(G) = (V', A')$, onde $V' = A$ e A' está definido do seguinte xeito: se $a, b \in V' = A$, e $a \neq b$, son adxacentes en $L(G)$ se, e soamente se, a e b son arestas incidentes en G. Tense que

$$g_{L(G)}(uv) = g_G(u) + g_G(v) - 2,$$

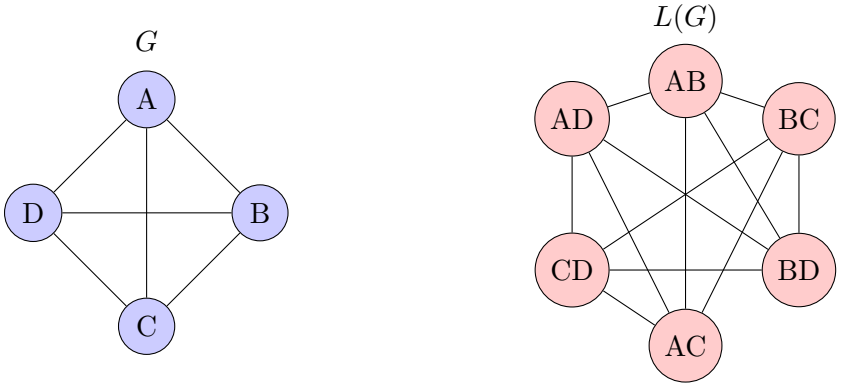
onde $u, v \in V$ e $uv \in A$. Por outra banda, $L(G)$ ten orde m e medida

$$\frac{1}{2} \sum_{u \in V} g_G(u)^2 - m.$$

Para demostrar este último resultado, procedemos como segue. O número de vértices de $L(G)$ coincide co número de arestas de G. Por outro lado, as arestas de $L(G)$ son da forma $\{uv, uw\}$, onde u, v, w son vértices diferentes de G e uv e uw son arestas de G. Fixado un vértice u de G, hai tantas arestas da forma $\{uv, uw\}$ en $L(G)$ como pares non ordenados de vértices adxacentes a u; ese número é $g(u)$. Polo tanto, o número de arestas é

$$\sum_{u \in V} \binom{g(u)}{2} = \frac{1}{2} \sum_{u \in V} g(u)^2 - \frac{1}{2} g(u) = \frac{1}{2} \sum_{u \in V} g(u)^2 - m.$$

Exemplo. Imos amosar como construír o grafo liña do grafo completo de 4 vértices.



3. *Unión* de G_1 e G_2 cando $V_1 \cap V_2 = \emptyset$. É o grafo $G_1 \cup G_2 = (V_1 \cup V_2, A_1 \cup A_2)$, que ten orde $n_1 + n_2$ e medida $m_1 + m_2$.

4. *Suma* de G_1 e G_2 cando $V_1 \cap V_2 = \emptyset$. É o grafo $G_1 + G_2$, no que o conxunto de vértices é $V_1 \cup V_2$ e o de arestas é

$$A_1 \cup A_2 \cup \{uv \mid u \in V_1, v \in V_2\},$$

polo que ten orde $n_1 + n_2$ e medida $m_1 + m_2 + n_1 n_2$. Por exemplo, o grafo roda pódese expresar como a suma $W_n = C_{n-1} + K_1$, e o grafo bipartito completo é a suma $K_{r,s} = N_r + N_s$.

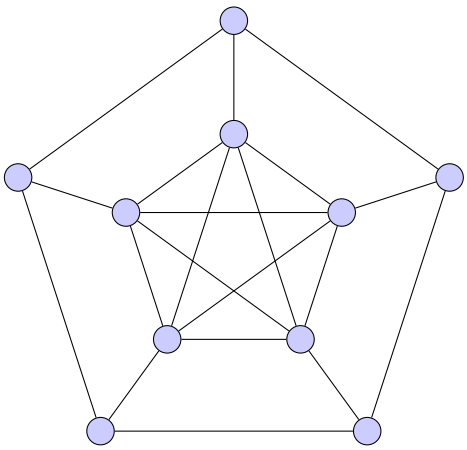
5. *Produto cartesiano* de G_1 e G_2. É o grafo $G_1 \square G_2 = (V_1 \times V_2, A')$, onde A' está definido como segue: se $u, u' \in V_1$ e $v, v' \in V_2$, tense que $(u, v) \sim (u', v')$ se, e soamente se, $u = u'$ e $vv' \in A_2$, ou $v = v'$ e $uu' \in A_1$. Máis en xeral, o produto cartesiano de r grafo, con $r \geq 2$, defínese recursivamente. Para $r = 2$ é o que acabamos de definir. Se $r \geq 3$, temos que

$$G_1 \square G_2 \square \cdots \square G_r = (G_1 \square G_2 \square \cdots \square G_{r-1}) \square G_r.$$

Un caso particular é o do *grafo hipercubo* Q_r, que é o produto cartesiano de r copias de K_2. Temos que Q_r é un grafo r-regular de orde 2^r, que se pode identificar co grafo que ten por conxunto de vértices as r-tuplas $(x_1, \ldots, x_r)$, con $x_i \in \{0, 1\}$, e dous vértices son adxacentes se, e soamente se, teñen exactamente $r - 1$ compoñentes iguais.

6. *Produto categórico* de G_1 e G_2. É o grafo $G_1 \times G_2 = (V_1 \times V_2, A')$, onde A' está definido como segue: se $u, u' \in V_1$ e $v, v' \in V_2$, tense que $(u, v) \sim (u', v')$ se, e soamente se, $uu' \in A_1$ e $vv' \in A_2$.

Outro grafo que ten certa importancia é o chamado *grafo de Petersen*, que ten 10 vértices e 15 arestas. Trátase dun grafo 3-regular no que dous vértices adxacentes non teñen veciños en común, pero no que dous vértices non adxacentes sempre teñen exactamente un veciño en común. Donald Knuth afirmou que o grafo de Petersen é *unha configuración notable que serve como contraexemplo a moitas predicións optimistas sobre que podería ser certo nun grafo en xeral.*



Grafo de Petersen

7.2. Conexión e distancia

O obxectivo desta sección é formalizar algunhas das nocións máis habituais en grafos. Por un lado, a idea de *conexión*, é dicir, a posibilidade de poder ir dun vértice a outro a través dun camiño no grafo. Por outro lado, a *distancia*, isto é, o número de arestas que cómpre recorrer para ir dun vértice a outro; por exemplo, diremos que vértices adxacentes que comparten unha aresta están a distancia 1.

Definición 7.8. En V, considérase a seguinte relación de equivalencia: uRv se, e soamente se, hai algún camiño de u a v en G.
As *compoñentes conexas* dun grafo G son os subgrafos inducidos polas clases de equivalencia da relación anterior. Un grafo é *conexo* se ten unha única compoñente conexa.

Comezamos facendo algunhas observacións sobre as nocións de recorrido, sendeiro, circuíto e camiño, que están intimamente ligadas entre si.

Proposición 7.2. Todo $u-v$ recorrido contén un $u-v$ camiño. Ademais, se u, v son dous vértices de xeito que hai dous $u-v$ camiños diferentes, entón G contén polo menos un ciclo.

Demostración. Se $u = v$, o recorrido contén o camiño de lonxitude 0 formado polo vértice u. Se $u \neq v$, imos probar o resultado por indución sobre a lonxitude k do recorrido, onde $k \geq 1$. Para $k = 1$ o resultado é trivialmente certo, xa que un recorrido de lonxitude 1 é un camiño. Consideramos agora un $u - v$ recorrido de lonxitude k, $R = u_0, u_1, \ldots, u_k$, onde $u_0 = u$ e $u_k = v$. Se R non repite vértices, acabamos. En caso contrario, $u_i = j_j$ para algún par de subíndices $0 \leq i < j \leq k$. Polo tanto, $R' = u_0, u_1, \ldots, u_i, u_{j+1}, \ldots, u_k$ é un $u - v$ recorrido de lonxitude menor que k, polo que contén un $u - v$ camiño por hipótese de indución.
Para a segunda parte, consideramos dous $u - v$ camiños diferentes, $x_0, x_1, \ldots, x_a$ e $y_0, y_1, \ldots, y_b$, onde $x_0 = y_0 = u$ e $x_a = y_b = v$. Por ser diferentes, existe un subíndice k, con $k \geq 1$, de xeito que $x_k \neq y_k$ e $x_i = y_i$ para todo $i < k$. O recorrido, $x_k, x_{k+1}, \ldots, x_a, y_{b-1}, \ldots, y_k$ contén un camiño $x_k, z_1, \ldots, z_r, y_k$ que non contén x_{k-1}. Por ser $x_{k-1}x_k$ e $x_{k-1}y_k$ arestas do grafo, $x_k, z_1, \ldots, z_r, y_k, x_{k-1}, x_k$ é un ciclo de G. □

Os ciclos de lonxitude impar desempeñarán un papel importante á hora de caracterizar os grafos bipartitos. Como en moitos casos nos interesará atopar ciclos de lonxitude impar nos grafos, convén ter o seguinte resultado, que nos di que é suficiente con achar un recorrido pechado de lonxitude impar.

Proposición 7.3. Todo recorrido pechado de lonxitude impar contén un ciclo de lonxitude impar. Cómpre ter en conta que o resultado, en cambio, non é certo para recorridos de lonxitude par.

Demostración. Demostrámolo por indución sobre a lonxitude do recorrido, que denotamos por k, onde $k \geq 3$. Se $k = 3$ é certo, xa que os recorridos pechados de lonxitude 3 son ciclos. Se $k \geq 5$ é impar e supoñemos que o resultado é certo para recorridos pechados de lonxitude impar menor que k, podemos considerar un recorrido pechado de lonxitude k impar. Sexa $R = u_0, u_1, \ldots, u_k$, onde $u_0 = u_k$. Se os vértices son todos diferentes xa temos un ciclo de lonxitude k impar. En caso contrario, $u_i = u_j$ para algúns $0 \leq i < j \leq k - 1$. Consideramos agora os recorridos pechados $R_1 = u_0, u_1, \ldots, u_i, u_{j+1}, \ldots, u_k$ e $R_2 = u_i, u_{i+1}, \ldots, u_j$. Os dous recorridos teñen lonxitude polo menos un e a suma das dúas lonxitudes é k, un impar. Polo tanto, un dos

dous ten lonxitude impar e, pola hipótese de indución, contén un ciclo de lonxitude impar. □

Pasamos agora a definir *distancia* e a establecer algunhas das súas propiedades.

Definición 7.9. Sexan $u, v \in V$. A *distancia* de u a v defínese como

$$d(u,v) = \text{mín}\{k \mid \text{ hai un } u-v \text{ camiño de lonxitude } k\}.$$

Dicimos que $d(u,v) = \infty$ se u e v están en diferentes compoñentes conexas.

A distancia cumpre as seguintes propiedades.

(a) $d(u,v) \geq 0$ e $d(u,v) = 0$ se, e soamente se, $u = v$.

(b) $d(u,v) = d(v,u)$.

(c) Para todo $w \in V$, $d(u,v) \leq d(u,w) + d(w,v)$. Esta propiedade coñécese como desigualdade triangular.

Definición 7.10. O *diámetro* dun grafo G é

$$D(G) = \text{máx}\{d(u,v) \mid u, v \in V\}.$$

A *excentricidade* dun vértice u é $e(u) = \text{máx}\{d(u,v) \mid v \in V\}$. O *radio* de G, que se denota por $r(G)$ é o mínimo das excentricidades. Un vértice u que cumpre $e(u) = r(G)$ chámase *central*.

Proposición 7.4. Tense que $r(G) \leq D(G) \leq 2r(G)$, é dicir, o diámetro sempre está entre o radio e o dobre do radio.

Demostración. É unha consecuencia inmediata da desigualdade triangular. □

Exemplo. Na cultura popular, hai unha famosa teoría, proposta polo escritor húngaro Frigyes Karinthy en 1929, que se coñece como *a teoría dos seis graos de separación*. Sostén que unha persoa arbitraria está conectada a outra calquera do planeta a través dunha cadea de coñecidos composta por cinco intermediarios, unindo a ambas persoas con seis arestas. Na linguaxe que estamos a empregar, isto querería dicir que o diámetro do grafo formado por tódalas persoas do planeta, con dúas delas conectadas por un aresta cando se coñecen, ten diámetro 6.

Imos agora empregar os resultados anteriores para establecer unha das primeiras proposicións importantes desta sección.

Proposición 7.5. Un grafo é bipartito se, e soamente se, non contén ningún ciclo de lonxitude impar.

Demostración. Se un grafo é bipartito, os vértices dun ciclo son alternativamente das dúas partes estables, de onde deducimos que o ciclo ten lonxitude par (polo que non pode haber ciclos de lonxitude impar).
Sexa agora G un grafo sen ciclos de lonxitude impar. Fixamos un vértice u e consideramos

$$X = \{z \in V \mid d(u,z) \text{ é par}\}, \quad Y = \{z \in V \mid d(u,z) \text{ é impar}\}.$$

Se o grafo non é conexo, fixamos un vértice de cada compoñente conexa. É obvio que os conxuntos X e Y son non baleiros xa que o grafo é non trivial; ademais, a súa unión é

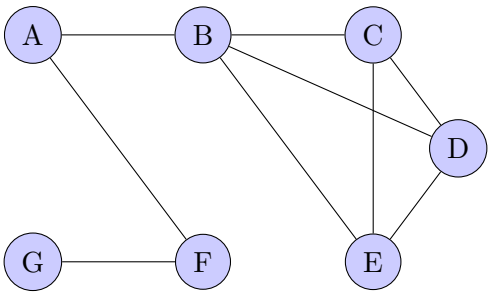
V e a súa intersección é baleira. Sexa $a = vw \in A$. Afirmamos que un dos vértices está en X e o outro en Y. Consideramos para iso un camiño de lonxitude $d(u, v)$ entre u e v, e un camiño de lonxitude $d(u, w)$ entre u e w. Se $v, w \in X$, consideramos o recorrido formado polo $u - v$ camiño, a aresta vw e o $w - u$ camiño obtido ao cambiar o sentido do $u - w$ camiño. Deste xeito obtemos un recorrido pechado de lonxitude impar que contén entón un ciclo de lonxitude impar, o que é unha contradición. O caso no que $v, w \in Y$ é análogo. □

Definición 7.11. Un conxunto de vértices $S \subseteq V$ é *separador* se $G - S$ ten máis compoñentes conexas que G. Analogamente, un conxunto de arestas $B \subseteq A$ é *separador* se $G - B$ ten máis compoñentes conexas que G.

Proposición 7.6. Nun grafo conexo, un conxunto $S \subseteq V$ é separador se, e soamente se, hai dous vértices $u, v \notin S$ tal que todo $u - v$ camiño contén algún vértice de S. Analogamente, un conxunto $B \subseteq A$ é separador se, e soamente se, hai dous vértices u, v tal que todo $u - v$ camiño contén algunha aresta de B.

Definición 7.12. Un vértice v tal que $\{v\}$ é separador chámase *vértice de corte*. Unha aresta a tal que $\{a\}$ é separador chámase *aresta ponte*

Exemplo. No seguinte grafo, o vértice B é un vértice de corte, porque a súa eliminación separa o grafo en dúas compoñentes conexas. Os vértices A e F tamén son vértices de corte. Pola súa banda, a aresta AB é unha aresta ponte, como tamén o son AF e FG.



É unha observación doada que unha aresta é ponte se, e soamente se, non hai ningún ciclo que a conteña. Se un grafo conexo de orde polo menos 3 ten algunha aresta ponte, entón ten algún vértice de corte.

Proposición 7.7. Sexa $G = (V, A)$ un grafo conexo de orde n e medida m.

(a) Se $u \in V$, entón o grafo $G - u$ ten como moito $g(u)$ compoñentes conexas.

(b) Se $a \in A$, o grafo $G - a$ ten como moito dúas compoñentes conexas.

(c) Cúmprese que $m \geq n - 1$.

Demostración. (a) Se $g(u) = d$, sexan $u_1, \ldots, u_d$ os vértices adxacentes a u. Se x é un vértice de $G - u$, hai un $u - x$ camiño en G que comeza cunha aresta uu_i, é dicir, hai un $u_i - x$ camiño en $G - u$. Polo tanto, x está na mesma compoñente conexa que u_i en $G - u$, de onde se deduce que $G - u$ ten como moito d compoñentes conexas.

(b) Supoñamos que $a = uv$. Se x é un vértice calquera de G, hai polo menos un $u-x$ camiño en G. Se o camiño non contén a, entón x está na mesma compoñente conexa que u en $G - a$. Se contén a, comezará pola aresta $a = uv$, de xeito que hai un $v-x$ camiño en G que non contén a. É dicir, x está na mesma compoñente conexa que v en $G - a$. Polo tanto, $G - a$ ten como moito dúas compoñentes conexas, a que contén u e a que contén v.

(c) Procedemos por indución no número de vértices n. Se $n = 1$ é certo. Supoñamos agora que $n \geq 2$ e o resultado é certo para grafos de orde n, con $n \geq 2$; sexa u un vértice calquera. O grafo $G-u$ ten k compoñentes conexas, $G_1, G_2, \ldots, G_k$, onde $1 \leq k \leq g(u)$. Se G_i é un grafo de orde n_i e medida m_i, entón $\sum_{i=1}^{k} n_i = n-1 < n$ e $\sum_{i=1}^{k} m_i = m - g(u)$. Como por hipótese de indución $m_i \geq n_i - 1$, tense

$$\begin{aligned} m &= \sum_{i=1}^{k} m_i + g(u) \geq \sum_{i=1}^{k} (n_i - 1) + g(u) \\ &= \sum_{i=1}^{k} n_i - k + g(u) = n - 1 + (g(u) - k) \\ &\geq n - 1. \end{aligned}$$

□

Proposición 7.8. Sexa $G = (V, A)$ un grafo conexo non trivial, e sexa $u \in V$ e $a \in A$.

(a) O vértice u é de corte se, e soamente se, existen $x, y \in V - u$ de xeito que u pertence a calquera $x - y$ camiño.

(b) A aresta a é ponte se, e soamente se, existen $x, y \in V$ de xeito que a pertence a calquera $x - y$ camiño.

(c) A aresta a é ponte se, e soamente se, non pertence a ningún ciclo.

Demostración. (a) Demostraremos que u non é vértice de corte se, e soamente se, para calquera par de vértices $x, y \in V - \{u\}$ hai polo menos un $x-y$ camiño que non contén u. Se u non é vértice de corte, $G - u$ é conexo, e, polo tanto, para dous vértices x, y de $G - u$ hai un camiño que os conecta, o que necesariamente quere dicir que non pasa por u. Reciprocamente, se para calquera par de vértices $x, y \in V - \{u\}$ hai un $x - y$ camiño que non contén u, entón hai un camiño en $G - u$ para todo par de vértices x, y de $G - u$, que é a definición de que $G - u$ sexa conexo. Polo tanto, u non é vértice de corte de G.

(b) Imos ver que a non é aresta ponte se, e soamente se, para todo par de vértices x, y de $G-a$ hai polo menos un $x-y$ camiño en $G-a$. Supoñamos primeiro que a non é aresta ponte. Como os vértices de $G - a$ son os mesmos que os vértices de G, temos que, para todo par de vértices x, y de G hai polo menos un $x - y$ camiño en G que non contén a. Reciprocamente, se para toda parella de vértices x, y existe un $x - y$ camiño que non contén a, entón haberá un $x - y$ camiño en $G - a$, o que quere dicir que $G - a$ é conexo e a non é aresta ponte.

(c) Imos ver que a non é aresta ponte se, e soamente se, a é dalgún ciclo. Sexa $a = uv$ unha aresta de G e sexa G' a compoñente conexa que a contén. Se $a = uv$ non é aresta ponte de G, entón $G' - a$ é conexo, polo que existe un $u - v$ camiño en

$G' - a$, isto é, un $u - v$ camiño en G' que non contén a. Se engadimos a aresta a ao camiño anterior obtemos un ciclo en G', que polo tanto tamén está en G, e que contén a aresta a. Para ver o recíproco, supoñamos que a está nalgún ciclo. O ciclo só contén elementos de G'. Fixamos agora x, y vértices en $G' - a$. Como G' é conexo, existe polo menos un camiño que os conecta en G'. Se o camiño non contén a, temos un $x - y$ camiño en $G' - a$. Se contén a, podemos substituír a aresta a pola outra parte do ciclo que contén a e que conecta os vértices u e v. Deste xeito, obtense un $x - y$ recorrido en $G' - a$ que contén un $x - y$ camiño en $G'a$. Polo tanto, hai un $x - y$ camiño en $G' - a$, o que demostra que $G' - a$ é conexo e que, polo tanto, a non é aresta ponte de a.

□

Imos introducir agora os conceptos de *vértice-conectividade* e *aresta-conectividade*.

Definición 7.13. Sexan $k, l \geq 1$ enteiros. O grafo G é *k-conexo* se para todo $S \subset V$ con $|S| \leq k - 1$ o grafo $G - S$ é conexo e non trivial. Se G non é conexo ou é trivial, dicimos que é 0-conexo. O máximo k tal que G é conexo chámase *(vértice) conectividade* e escríbese $\kappa(G)$. Analogamente, o grafo G é *l-aresta conexo* se para todo $B \subseteq A$ con $|B| \leq l-1$ o grafo $G-B$ é conexo e non trivial. Se G é non conexo ou trivial, dicimos que é 0-aresta conexo. O máximo l tal que G é l-aresta conexo chámase *aresta conectividade* e escríbese $\lambda(G)$.

Para enunciar a seguinte proposición, recordemos que $\delta(G)$ é o menor dos graos dun grafo.

Proposición 7.9 (Whitney)**.** Se G é un grafo calquera, tense que

$$\kappa(G) \leq \lambda(G) \leq \delta(G).$$

Demostración. Se G é un grafo trivial ou non conexo, entón $\kappa(G) = \lambda(G) = 0$ e $\delta(G) \geq 0$. Supoñamos entón que G é conexo e non trivial, e sexa u un vértice con grao mínimo δ, de xeito que queda illado ao suprimir as δ arestas incidentes a u. Polo tanto, $\lambda(G) \leq \delta(G)$.
Para a outra desigualdade, sexa S un conxunto de arestas de cardinal $r = \lambda(G)$, de xeito que $G - S$ non sexa conexo. Se $S = \{a_1, \ldots, a_r\}$, a aresta a_r é aresta ponte do grafo conexo $G - \{a_1, \ldots, a_{r-1}\}$ xa que, se non fose conexo, teriamos que $\lambda(G) \leq r - 1$. Polo tanto, $G - S = (G - \{a_1, \ldots, a_{r-1}\}) - a_r$ ten exactamente dúas compoñentes conexas. Sexa $a_r = xy$. Para cada aresta a_i, con $1 \leq i \leq r - 1$, escollemos un vértice u_i incidente con a_i tal que $u_i \neq x, y$. O conxunto $W = \{u_1, \ldots, u_{r-1}\}$ ten cardinal como moito $r-1$, xa que pode pasar que escollamos un mesmo vértice para arestas diferentes. O grafo $G-W$ ten orde polo menos 2, xa que x, y son vértices del. Se non fose conexo, entón $\kappa(G) \leq |W| \leq r - 1 < r = \lambda(G)$. Se é conexo de orde 2, entón $G - (W \cup \{x\})$ é o grafo trivial e tense que $\kappa(G) \leq (r - 1) + 1 = r = \lambda(G)$.
Finalmente, supoñamos que $G - W$ é conexo de orde polo menos 3, e que existe entón un vértice z diferente de x e y. □

O seguinte resultado, coñecido como Teorema de Menger, é un dos principais resultados sobre conectividade en grafos. Relaciona o número de vértices que hai que quitar para desconectar dous vértices co número de camiños internamente disxuntos entre eses vértices. A demostración é bastante complexa, polo que a imos omitir.

Teorema 7.1 (Menger)**.** Dados dous vértices u e v non adxacentes, sexa $s(u,v)$ o mínimo número de vértice que hai que eliminar para que u e v queden en compoñentes conexas diferentes, e sexa $c(u,v)$ o máximo número de $u-v$ camiños internamente disxuntos. Entón, $s(u,v) = c(u,v)$.

En particular, un grafo é k-conexo se, e soamente se, para cada parella de vértices u, v existen k $u-v$ camiños internamente disxuntos.

7.3. Grafos eulerianos e hamiltonianos

O problema dos grafos eulerianos ten a súa orixe nunha situación da vida cotiá. Königsberg, a actual Kaliningrado, era unha cidade de Prusia que tiña sete grandes pontes: a ponte do ferreiro, a ponte *conectora*, a porte verde, a ponte do mercado, a ponte de madeira, a ponte alta e a ponte da mel. O problema que se formulaba era o seguinte: é posible atravesar tódalas pontes pasando unha única vez por cada unha delas? Para formular e responder este tipo de cuestións convén introducir a seguinte terminoloxía.

Definición 7.14. Sexa G un grafo conexo. Un *circuíto euleriano* é un recorrido pechado que pasa exactamente unha vez por cada aresta. Un grafo é *euleriano* se ten algún circuíto euleriano.

Proposición 7.10. Un grafo G é euleriano se, e soamente se, é conexo e todos os seus vértices teñen grao par.

Demostración. Consideremos un circuíto euleriano do grafo G

$$u_0, a_1, u_1, a_2, u_2, a_3, u_3, \ldots, u_{m-2}, a_{m-1}, u_{m-1}, a_m, u_m,$$

onde $u_0 = u_m$ e $A = \{a_1, \ldots, a_m\}$. Como G é conexo e non trivial, todo vértice é incidente polo menos a unha aresta, de xeito que todo vértice do grafo pertence ao circuíto. Hai tantas arestas incidentes nun vértice u como o dobre do número de veces que aparece o vértice na sucesión $u_0, u_1, \ldots, u_{m-1}$, xa que no circuíto aparecen tódalas arestas unha vez e só unha, e todo vértice u_i é incidente ás dúas arestas veciñas a_i e a_{i+1}, excepto o vértice $u_0 = u_m$ que é incidente a a_1 e a_{m-1}. Concluímos entón que todo vértice ten grao par.
Para ver o recíproco, imos demostrar que existe unha partición $\{A_i \mid i \in [r]\}$ do conxunto de arestas de xeito que o subgrafo xerado por A_i é un ciclo, para todo $i \in [r]$. Imos demostralo por indución sobre m, con $m \geq 3$. Se G é un grafo conexo con 3 arestas e no que todos os vértices teñen grao 3, ten que ser o grafo ciclo C_3, e a partición do conxunto de arestas ten unicamente unha parte que as contén todas. Supoñamos agora que $m \geq 4$ e que todos os vértices teñen grao par. O grafo contén polo menos un ciclo, C', e sexa A' o conxunto das arestas do ciclo C'. Consideramos o grafo G' xerado por $A - A'$. Todos os vértices de G' teñen grao par. Por hipótese de indución, cada un dos conxuntos de arestas das compoñentes conexas non triviais de G' admiten unha partición en partes inducen ciclos. A partición formada por tódalas partes obtidas, xuntamente co conxunto A', é unha partición de A que cumpre as condición do enunciado.
A partir desa partición podemos construír agora un circuíto euleriano. Sabemos que $A = \cup_{i\in[r]} A_i$ e $A_i \cap A_j = \emptyset$ se $i \neq j$. As arestas de A_1 determinan un ciclo C_1 que comeza e acaba nun vértice u e contén as arestas de A_1 unha vez (e soamente unha). Como G é conexo, polo menos unha aresta $a_1 \in A - A_1$ ten que ser incidente a un vértice u_1 do ciclo C_1. Supoñamos que $a_1 \in A_{i_2}$ e consideremos o circuíto C_2 que consiste en

recorrer o circuíto C_1 ata arribar ao vértice u_1, a continuación o ciclo inducido por A_{i_2} que comeza e acaba en u_1 e despois o que queda de circuíto C_1. Obtemos un circuíto que contén as arestas de $A_1 \cup A_{i_2}$. Como o grafo é conexo, polo menos unha aresta $a_2 \in A - (A_1 \cup A_{i_2})$ ten que ser incidente a un vértice u_2 de C_2. Supomos agora que $a_2 \in A_{i_3}$ e construímos un circuíto C_3 que contén as arestas de $A_1 \cup A_{i_2} \cup A_{i_3}$ e iteramos o proceso ata ter un circuíto que contén tódalas arestas de G. □

O método anterior pódese empregar para construír un ciclo euleriano nun grafo G no que todos os vértices teñen grao par. Outra opción moi similar é o coñecido como *algoritmo de Fleury*, que consiste en ir escollendo arestas que non desconecten o grafo, sempre e cando sexa posible realizar unha elección alternativa.

Definición 7.15. Un *sendeiro euleriano* nun grafo conexo G é un recorrido que pasa exactamente unha vez por cada aresta e que comeza e acaba en vértices diferentes.

Pola proposición anterior, sabemos que un grafo G ten un sendeiro euleriano se, e soamente se, é conexo e ten exactamente dous vértices de grao impar. Nestes casos, ás veces fálase de *grafo semieuleriano*

Definición 7.16. Dicimos que un ciclo ou un camiño nun grafo G son *hamiltonianos* se conteñen todos os vértices de G. Un grafo é *hamiltoniano* se ten algún ciclo hamiltoniano.

Proposición 7.11. Sexa G un grafo hamiltoniano e $S \subseteq V$ un conxunto non baleiro con $|S| = s$. Entón, o grafo $G - S$ ten como moito s compoñentes conexas.

En particular, os grafos hamiltonianos son 2-conexos.
De cara a establecer os dous resultados principais sobre grafos hamiltonianos, precisamos o seguinte resultado.

Proposición 7.12. Sexan G un grafo de orde n e u, v vértices non adxacentes. Se $g(u) + g(v) \geq n$, entón o grafo G é hamiltoniano se, e soamente se, o grafo $G + uv$ tamén o é.

Os dous principais resultados que dan condicións suficientes para que un grafo sexa hamiltoniano son os seguintes. Omitimos as correspondentes demostracións.

Teorema 7.2 (Ore)**.** Sexa G un grafo de orde n tal que, para calquera parella de vértices u e v non adxacentes cúmprese que $g(u) + g(v) \geq n$. Entón G é hamiltoniano.

Teorema 7.3 (Dirac)**.** Sexa G un grafo de orde n tal que para todo vértice u cúmprese que $g(u) \geq n/2$. Entón G é hamiltoniano.

Exemplo. O grafo completo K_n sempre é hamiltoniano. É euleriano se, e soamente se, n é impar, xa que todos os seus vértices teñen grao $n - 1$.
O grafo bipartito completo $K_{m,n}$ é euleriano se, e soamente se, m e n son ambos pares. É hamiltoniano se, e soamente se, $m = n$, xa que calquera ciclo que ten ir alternando un vértice de cada unha das partes estables, polo que ten que ter os mesmos elementos en cada unha delas. En particular, isto amosa que os límites que proporciona o teorema de Dirac son axustados: no grafo $K_{n,n+1}$, que ten orde $2n + 1$, todos os vértices teñen orde n ou $n + 1$, pero ese non é bipartito.

7.4. Árbores

No estudo dos grafos, un dos tipos máis importantes son as *árbores*, que aparecen en moitos contextos diferentes e que cumpren diferentes propiedades que iremos discutindo ao longo desta sección.

Definición 7.17. Un grafo G é unha *árbore* se é conexo e acíclico. Un grafo acíclico chámase *bosque*. Nunha árbore (ou nun bosque) os vértices de grao 1 chámase *follas*.

Antes de comezar a desenvolver as súas propiedades, imos establecer algúns resultados.

Proposición 7.13. Se G é un grafo acíclico de orde n e medida m, entón $m \leq n-1$. En particular, un grafo con todos os vértices de grao maior ou igual que 2 contén polo menos un ciclo.

Demostración. Imos resultar o resultado por indución en n. Se $n = 1$ o resultado é certo. Supoñamos que $n \geq 2$ e que o resultado se cumpre para grafos de orde menor a n. Consideremos un grafo acíclico G de orde n, con $n \geq 2$. Se a medida de G é 0, a desigualdade é certa. Se a medida é polo menos 1, collemos unha aresta calquera a. Como G é acíclico, a é unha aresta ponte de G. Polo tanto, o grafo $G-a$ ten polo menos dúas compoñentes conexas que son grafos acíclicos. Se $G_1, \ldots, G_k$ son as compoñentes conexas de $G-a$ e G_i ten orde n_i e medida m_i, entón $n_i < n$; por hipótese de indución, $m_i \leq n_i - 1$. Sumando todo, quédanos que

$$m = \sum_{i=1}^{k} m_i + 1 \leq \sum_{i=1}^{k} (n_i - 1) + 1 = \sum_{i=1}^{k} n_i - k + 1 = n - k + 1 \leq n - 1.$$

Se os vértices son todos de grao maior ou igual que 2, $m \geq \frac{1}{2}(2n) = n > n-1$, polo que o grafo non pode ser acíclico. □

Do anterior resultado tamén se deduce que un grafo 2-regular é unión de ciclos e que os grafos conexos 2-regulares son precisamente os grafos ciclo.
A seguinte proposición resume as propiedades principais das árbores.

Proposición 7.14. Sexa $T = (V, A)$ unha árbore de orde n e medida m. Entón:

(a) $m = n - 1$.

(b) Se $n \geq 2$, T ten polo menos unha folla.

(c) T é bipartito.

(d) Toda aresta é ponte.

(e) Todo vértice u de grao maior ou igual que 2 é de corte, e $T - u$ ten $g(u)$ compoñentes conexas.

(f) Para todo $u, v \in V$, hai un único $u - v$ camiño.

Demostración. (a) Calquera grafo conexo cumpre que $m \geq n - 1$, mentres que os grafos acíclicos cumpren que $m \leq n - 1$. Polo tanto, $m = n - 1$.

(b) Temos que $m = n - 1$ e como o grafo é conexo non hai vértices de grao 0. Sexa f o número de vértices de grao 1. Empregando o lema do apertón de mans temos que

$$2n - 2 = 2m = f + \sum_{u|g(u)\neq 1} g(u) \geq f + 2(n - f) = 2n - f,$$

polo que $f \geq 2$.

(c) Unha árbore non ten ciclos polo que, en particular, non ten ciclos de lonxitude impar, o que quere dicir que o grafo é bipartito.

(d) Se a aresta non fose ponte, ao quitala habería un camiño conectando os dous vértices; ao engadirmos a aresta, estariamos obtendo un ciclo, que é unha contradición co feito de que T é unha árbore.

(e) Sexan v e w dous vértices adxacentes a u. Se houbese un camiño que os conectase sen pasar por u, ao engadirmos este vértice xunto coas arestas vu e uw estariamos a fabricar un ciclo. Como cada un dos vértices adxacentes a u queda en compoñentes conexas diferentes, tense o enunciado.

(f) Se houbese máis dun camiño diferente, sería posible obter un ciclo.

□

A seguinte proposición permite ter diferentes caracterizacións alternativas das árbores.

Proposición 7.15 (Caracterización das árbores)**.** Se $G = (V, A)$ é un grafo de orde n e medida m, entón as seguintes condicións son equivalentes:

(a) G é unha árbore;

(b) G é acíclico e $m = n - 1$;

(c) G é conexo e $m = n - 1$;

(d) G é conexo e toda aresta é ponte;

(e) para todo $u, v \in V$, existe un único camiño para ir de u a v;

(f) G é acíclico e ao engadirmos unha aresta créase exactamente un ciclo.

Demostración. Tódalas implicacións son de tipo estándar. □

Un bosque de orde n e k compoñentes conexas ten medida $n - k$. Nun grafo acíclico de orde n e medida m cúmprese que $m \leq n - 1$.

Definición 7.18. Unha árbore xeradora dun grafo G é un subgrafo xerador de G que é unha árbore.

Proposición 7.16. Un grafo G ten (polo menos) unha árbore xeradora se, e soamente se, G é conexo.

Demostración. Se un grafo G ten unha árbore xeradora ten que ser conexo, xa que para todo par de vértices hai un camiño na árbore que os conecta e, polo tanto, un camiño que os conecta no grafo G. Supoñamos agora que G é conexo. Consideremos un subgrafo H conexo e xerador de G de medida mínima. Se H non é unha árbore, H contén algún ciclo, polo que podemos coller unha aresta a de dito ciclo e considerar o

subgrafo $H' = H - a$. O subgrafo H' é conexo xa que a non é aresta ponte, é xerador (xa que ten o mesmo conxunto de vértices) e de medida máis pequena que H. Isto é unha contradición coa suposición de que H era o subgrafo conexo xerador de H de medida mínima. □

O seguinte resultado permite determinar o número de árbores xeradoras para o grafo completo K_n.

Proposición 7.17 (Cayley)**.** Hai n^{n-2} árbores diferentes con conxunto de vértices $V = [n]$.

De cara a probar este resultado, imos introducir as coñecidas como *sucesións de Prüfer* dunha árbore. Se T é unha árbore de orde $n \geq 3$ con conxunto de vértices $V = [n]$, a *sucesión de Prüfer de* T é a palabra

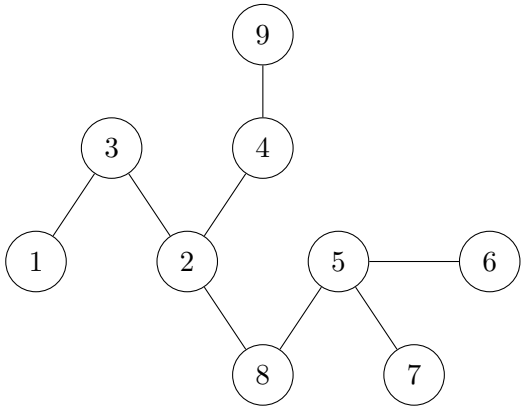
$$\mathcal{P}(T) = (y_1, y_2, \ldots, y_{n-2})$$

de $n-2$ números do conxunto $V = [n]$ definida recursivamente do seguinte xeito:

(a) y_1 é o único vértice adxacente á folla x_1 de valor mínimo da árbores $T_1 = T$;

(b) y_k é o único vértice adxacente á folla x_k de valor mínimo da árbore $T_k = T_{k-1} - x_{k-1}$ para todo k con $2 \leq k \leq n-2$.

Exemplo. Consideremos a seguinte árbore de 9 vértices e 8 arestas.



Imos ver como atopar a sucesión de Prüfer da árbore que se amosa no gráfico.

(a) A folla de menor valor é o vértice 1, e o vértice adxacente é o 3.

(b) Eliminado o vértice 1, a folla de menor valor é o vértice 3, adxacente ao 2.

(c) No seguinte paso, as follas son o 6, o 7 e o 9. O vértice adxacente ao 6 é o 5.

(d) Agora, as follas son o 7 e o 9. O vértice adxacente ao 7 volve ser o 5.

(e) As follas son o 5 e o 9. O vértice adxacente ao 5 é o 8.

(f) Seguimos a ter dúas follas, o 8 e o 9. O vértice adxacente ao 8 é o 2.

(g) Finalmente, xa só cos vértices 2, 4 e 9, as follas son o 2 e o 9, e o vértice adxacente ao 2 é o 4.

Polo tanto, a sucesión de Prüfer da árbore é a $(3, 2, 5, 5, 8, 2, 4)$.

Imos discutir agora o proceso inverso, sobre como reconstruír unha árbore a partir da súa sucesión de Prüfer. Supoñamos que $T = (V, A)$, con $V = [n]$, e pomos $(y_1, y_2, \ldots, y_{n-2})$ para a súa súa sucesión de Prüfer. Para determinar o conxunto de arestas $A = \{a_1, \ldots, a_{n-1})\}$ procedemos recursivamente.

(a) Pomos $a_1 = x_1y_1$, onde $x_1 = \text{mín}([n] - \{y_1, \ldots, y_{n-2}\})$;

(b) Temos que $a_k = x_ky_k$, sendo $x_k = \text{mín}([n] - \{x_1, \ldots, x_{k-1}, y_k, \ldots, y_{n-2})$, se $2 \leq k \leq n-2$;

(c) $a_{n-1} = x_{n-1}n$, onde $x_{n-1} = \text{mín}([n] - \{x_1, \ldots, x_{n-2}\})$.

Exemplo. Imos explicar como obter a árbore correspondente á árbore $(3, 2, 5, 5, 8, 2, 4)$.

(a) Tense que $x_1 = 1$, polo que a primeira aresta é a 13.

(b) Do mesmo xeito, $x_2 = \text{mín}([9] - \{1, 2, 5, 5, 8, 2, 4\}) = 3$, polo que a segunda aresta é 23.

(c) Temos que $x_3 = \text{mín}([9] - \{1, 3, 5, 5, 8, 2, 4\}) = 6$, o que quere dicir que a terceira aresta é 56.

(d) Temos que $x_4 = \text{mín}([9] - \{1, 3, 6, 5, 8, 2, 4\}) = 7$, polo que a cuarta aresta é 57.

(e) Analogamente, $x_5 = 5$ e a quinta aresta é 58.

(f) Tense que $x_6 = 8$ e a sexta aresta é 28.

(g) Finalmente, $x_7 = 2$ e a penúltima aresta é 24.

(h) Para o último paso, $x_8 = 8$, polo que a aresta final é a 49.

Podemos finalmente dar a proba do teorema de Cayley.

Demostración. Como se trata dun proceso reversible, temos unha bixección entre as árbores xeradoras de K_n e as palabras de lonxitude $n-2$ formadas cos números do 1 ao n. Como temos n^{n-2} palabras deste xeito, o teorema de Cayley queda probado. □

Para estender estes resultados a grafos máis xerais, temos o chamado como *teorema de Kirchhoff*. Trátase dun enunciado máis complicado, do que daremos unha breve idea.

Definición 7.19. A matriz $D = (d_{ij})$ de graos dun grafo G con conxunto de vértices $\{u_1, \ldots, u_n\}$ é a matriz diagonal tal que o elemento i-ésimo da diagonal é $d_{ii} = g(u_i)$. Unha matriz de *incidencia orientada* dun grafo G de orde $n \geq 2$ e medida $m \geq 1$ é unha matriz $n \times m$ que se obtén cambiando en cada columna da matriz de incidencia un 1 por un -1.

Proposición 7.18. Sexa A a matriz de adxacencia, M a de incidencia, N unha matriz de incidencia orientada e D a matriz de graos dun grafo, obtidas a partir dunha orientación do conxunto de vértices e de arestas. Entón, cúmprense as seguintes igualdades matriciais:

(a) $MM^t = D + A$.

(b) $NN^t = D - A$.

Estes resultados permiten facer a seguinte definición.

Definición 7.20. A matriz $Q = NN^t = D - A$ chámase *matriz laplaciana* de G.

O seguinte resultado é o coñecido como teorema de Kirchoff ou *matrix tree theorem*.

Proposición 7.19 (Teorema de Kirchhoff)**.** O número de árbores xeradoras dun grafo G é igual ao valor absoluto do determinante de calquera matriz que se obtén ao suprimir unha fila ou unha columna da matriz laplaciana Q.

De cara a diferentes aplicacións, é importante contar con algoritmos que permitan atopar árbores xeradoras. Os máis coñecidos son o *algoritmo de Prim* e o *algoritmo de Kruskal*. O primeiro baséase na elección de vértices e o segundo na elección de arestas. Estes procedementos son máis importantes no contexto dos chamados *grafos ponderados*, nos que se lle asigna un peso a cada unha das arestas.

7.5. Planaridade

Definición 7.21. Unha *representación plana* dun grafo G é unha representación do grafo no plano de xeito que identificamos cada vértice cun punto do plano, e cada aresta cunha liña continua que une os vértices correspondentes de xeito que as arestas non se cortan. Un grafo é *planar* se admite unha representación plana.

Se temos unha representación plana dun grafo, os puntos que representan os vértices e as arestas delimitan diferentes rexións do plano. Unha *cara* é unha rexión conexa maximal do plano que non contén ningún punto utilizado na representación dun vértice ou dunha aresta.
O seguinte resultado coñécese como fórmula de Euler.

Proposición 7.20 (Fórmula de Euler)**.** Se c é o número de caras dunha representación plana dun grafo conexo de orde n e medida m.

(a) Cúmprese que $c + n = m + 2$.

(b) Se c é o número de caras dunha representación plana dun grafo de orde n e medida m con exactamente k compoñentes conexas, entón $c + n = m + k + 1$.

(c) Se G é un grafo planar de orde n, con $n \geq 3$, e medida m, entón $m \leq 3n - 6$.

Demostración. (a) Imos proceder por indución sobre o número de arestas do grafo. Se o grafo non ten ningunha aresta, é o grafo trivial, polo que ten unha cara e un vértice e a fórmula cúmprese. Supoñamos agora que temos un grafo conexo de medida m, con $m \geq 1$, e que o resultado é certo para grafos de medida menor que m. Se o grafo non ten ciclos trátase dunha árbore, que ten unha única cara e $m = n - 1$, polo que o resultado é certo. Se o grafo ten algún ciclo, consideramos unha aresta a dun ciclo. O grafo $G - a$ é conexo de medida $m - 1$. Por hipótese de indución, se o número de caras de $G - a$ é c', temos que $c' + n = m - 1 + 2$. Por outro lado, o número c de caras do grafo cumpre que $c = c' + 1$. Volvendo á ecuación anterior, obtemos que $c + n = m + 2$.

(b) Se o grafo G ten k compoñentes conexas, que chamamos G_i, para cada unha delas cúmprese que $c_i+n_i = m_i+2$. Tense que $c = \sum_{i=1}^{k} c_i-(k-1)$, polo que, sumando tódalas igualdades, chegamos a

$$c = \sum_{i=1}^{k}(m_i + 2 - n_i) - (k-1) = m + 2k - n - (k-1).$$

A partir de aquí, o resultado é evidente.

(c) Supoñamos en primeiro lugar que o grafo G é conexo. Se a medida é como moito 3, entón é certo. Supoñamos entón que $m \geq 4$. Se temos unha representación plana de G, entón $c + n = m + 2$. Por outro lado, se numeramos as caras da representación plana de 1 a $c-$ e f_i representa o número de arestas que limitan a cara i, temos que

$$3c \leq \sum_{i=1}^{c} f_i \leq 2m,$$

xa que cada cara está limitada por, polo menos, tres arestas, e cada aresta limita con, como moito, dúas caras. Polo tanto, $3(m + 2 - n) \leq 2m$, de onde se obtén que $m \leq 3n - 6$. Se o grafo é plano e non conexo, podemos engadir arestas entre as diferentes representacións planas das compoñentes conexas, obtendo unha representación plana dun grafo G' conexo, de orde n e de medida $m' \geq m$, que cumpre $m' \leq 3n - 6$. Polo tanto, $m \leq 3n - 6$.

□

Proposición 7.21. Un grafo planar ten polo menos un vértice de grao como moito 5.

Demostración. Supoñamos que o grafo ten orde n e medida m. Se fose planar e todo vértice tivese grao polo menos 6, entón

$$6n \leq \sum_{u \in V} g(u) = 2m \leq 6n - 12,$$

que é unha contradición. □

Proposición 7.22. Os grafos K_5 e $K_{3,3}$ non son planares.

Dicimos que un grafo G é contraíble a H se H se pode obter a partir de G por medio de sucesivas contraccións de arestas.

Proposición 7.23 (Kuratowski)**.** Un grafo G é un grafo planar se, e soamente se, non contén ningún subgrafo contraíble nin a K_5 nin a $K_{3,3}$.

7.6. Coloración de grafos

Definición 7.22. Unha *coloración* dun grafo G é unha asignación de cores aos vértices de G, de xeito que vértices adxacentes reciben colores diferentes. O mínimo número de cores que fan falta para colorear G é o chamado *número cromático* de G, e escríbese como $\chi(G)$.

Claramente, se $|V(G)| = n$, entón $\chi(G) \leq n$, e alcánzase o valor de n para K_n. Pomos $w(G)$ para a medida da maior clique (subgrafo completo) e $\alpha(G)$ para a medida do maior conxunto independente. Diremos un grafo G é *k-crítico* (respecto ao número cromático) se $\chi(G) = k$, pero $\chi(G - e) < k$ para todo aresta e. Se $\chi(G) = k$, entón G contén un subgrafo k-crítico.

Exemplo. Un grafo ten número cromático 1 se, e soamente se, non ten ningunha aresta. Un grafo ten número cromático 2 se, e soamente se, ten polo menos unha aresta e é bipartito.

Exemplo. O número cromático do grafo completo K_n é $\chi(K_n) = n$, xa que non pode haber dous vértices da mesma cor por estaren unidos cunha aresta.
O número cromático do ciclo C_n é $\chi(C_n) = 2$ se n é par, por tratarse dun grafo bipartito, e $\chi(C_n) = 3$ se n é impar: podemos numerar os vértices do 1 ao $n = 2k + 1$ e pintar dunha cor todos os impares ata $2k - 1$, doutra cor o $2k + 1$, e dunha terceira cor todos os pares.

Para o seguinte resultado, recordemos que $\Delta(G)$ é o maior dos graos de G. É un exercicio sinxelo demostrar que se G ten grao máximo Δ, entón G pódese pintar con $(\Delta + 1)$ cores.

Proposición 7.24 (Brooks)**.** Se G é un grafo conexo non isomorfo a un grafo completo ou a un ciclo impar, entón

$$\chi(G) \leq \Delta(G).$$

Un problema que historicamente atraeu a atención de moitos matemáticos é o da coloración dos grafos planares. Esta cuestión está relacionada co número de cores que fan falta para pintar un mapa de xeito que dúas rexións adxacentes sexan de cores diferentes. Desde mediados do século XIX conxecturouse que con catro cores era suficiente. Porén, ese resultado resistiuse ao estudo da comunidade matemática, e durante moitos anos o mellor resultado dispoñible foi o teorema de Heawood, que afirma que dúas cores son suficientes.

Proposición 7.25 (Heawood)**.** Todo grafo planar é 5-coloreable.

Demostración. Procedemos por indución sobre n, o número de vértices do grafo. Se $n \leq 5$ é claramente certo, así que supoñamos que $n \geq 6$ e que o resultado é certo para grafos de menos de n vértices. Sexa u un vértice de grao como moito 5. Por hipótese de indución, o grafo $G - u$ é 5-coloreable, xa que é planar de orde $n - 1$. Se $g(u) \leq 4$, entón o grafo é 5-coloreable, xa que lle podemos asignar un color diferente ao dos 4 vértices adxacentes a u. Se $g(u) = 5$ e os 5 vértices adxacentes a u teñen asignados como moito 4 cores diferentes, entón tamén podemos rematar. Finalmente, supoñamos que $g(u) = 5$ e que a coloración de $G - u$ asígnalle 5 cores distintas aos vértices adxacentes a u. Numeramos os vértices adxacentes a u como v_1, v_2, v_3, v_4 e v_5, que teñen cores 1, 2, 3, 4 e 5, e consideramos que as arestas uv_1, uv_2, uv_3, uv_4 e uv_5 están en sentido antihorario na representación plana do grafo. Sexa G_{ij} o subgrafo de G inducido polos vértices de cor i e j, con $i \neq j$. Se v_1 e v_3 son de diferentes compoñentes conexas en G_{13}, podemos intercambiar as cores 1 e 3 nos vértices da compoñente conexa de v_1. Se están na mesma compoñente conexa, hai un camiño de v_1 a v_3 en $G - u$ formado polos vértices de G_{13}. Nese caso, v_{24} non poden ser da mesma compoñente conexa en G_{24}, xa que en caso contrario habería un grafo contraíble a G_5, o formado por v_1, v_2, v_3, v_4 e u. Polo tanto, podémoslle asignar unha cor diferente ás 4 cores asignadas aos 5 vértices adxacentes a u. □

No ano 1979 completouse a demostración do teorema das catro cores, que afirma que catro cores son suficientes para pintar calquera grafo planar. No proceso de proba, os ordenadores desenvolveron un papel crucial.

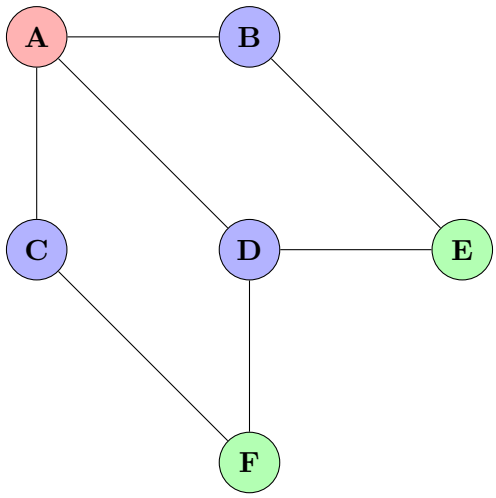
Capítulo 8

Algoritmos en grafos

O obxectivo desta parte final do tema é discutir algúns algoritmos en grafos. En todo momento, G denota un grafo, n o seu número de vértices e m o número de arestas.

8.1. Distancias en grafos: busca en anchura

O algoritmo BFS ou busca en anchura é un algoritmo que se emprega en grafos para atopar a distancia entre dous vértices. Hai un algoritmo similar, que se coñece como DFS ou busca en profundidade, que se usa co mesmo propósito e que é similar en canto á complexidade.
No algoritmo BFS selecciónase un vértice inicial e vanse visitando tódolos demais en función da distancia ao vértice inicial (isto é, primeiro visítanse os que están a distancia 1, logo os que están a distancia 2 e así sucesivamente). Isto permite determinar as distancias ao vértice inicial. A complexidade do BFS é $\mathcal{O}(m+n)$, isto é, é lineal na suma do número de vértices e arestas.
Imos considerar o seguinte exemplo para ilustrar o algoritmo.



O BFS explora o grafo nivel por nivel.

(a) O vértice inicial é o A (en vermello), que se considera que está a distancia 0.

(b) A primeira *capa* está formada polos vértices B, C e D (en azul), todos eles a distancia 1.

(c) A segunda *capa* está formada polos vértices E e F (en verde), ambos a distancia 2.

Durante cada iteración do BFS, os vértices fronteira son os vértices do seguinte nivel que aínda non foron visitados. O algoritmo continúa ata que todos os vértices son explorados.

De cara á súa implementación adoita empregarse unha *cola*, na que se van introducindo os vértices veciños a aqueles que visitamos, e despois vanse explorando en función do tempo que levan na cola (isto é, un vértice explórase antes ca outro se leva máis tempo na cola). Cando se explora un vértice que está a distancia d, a todos aqueles veciños seus que aínda non foron introducidos na cola asígnaselle a distancia $d + 1$.

Imos mencionar algunhas das aplicacións do algoritmo BFS.

- Determinar se un grafo é conexo. Se, partindo dun vértice inicial é posible chegar a tódolos demais, entón o grafo é conexo. En caso contrario, hai máis dunha compoñente conexa.

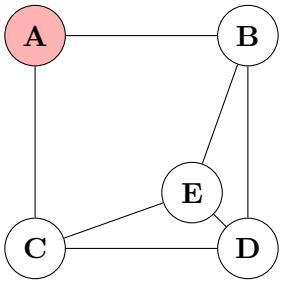
- Existencia de ciclos. Un grafo contén un ciclo se, durante un recorrido do grafo, atopamos un vértice que ten veciños que xa foron visitados.

- Determinar se un grafo ten número cromático 2. Para iso, píntase o vértice inicial dunha cor, por exemplo, de azul. Tódolos seus veciños píntanse de vermello, e os veciños destes de azul, e así sucesivamente. Se ao longo da busca chega un momento no que observamos que dous vértices adxacentes teñen a mesma cor, iso quererá dicir que o grafo non é bipartito.

8.2. Distancias en grafos ponderados: algoritmo de Dijkstra

Unha extensión do algoritmo BFS que se emprega cando as arestas teñen pesos é o algoritmo de Dijkstra. Este algoritmo atopa o camiño máis curto nun grafo, comezando nun vértice que se marco como inicial e visitando tódolos demais vértices do grafo. O algoritmo vai gardando as distancias aos vértices ao longo do recorrido, e vainos visitando en orde crecente segundo a distancia ao vértice inicial. Para a súa implementación cómpre empregar unha *cola de prioridade*, na que a cada vértice que se garda asígnaselle a distancia ao inicial e vanse visitando en orde crecente de distancia; polo tanto, cada vez que imos a un vértice, temos que introducir na cola de prioridade outro vértice, e facer iso ten un custo logarítmico, xa que inserir un elemento nunha lista ordenada equivale a unha busca binaria. Polo tanto, o custo asintótico do algoritmo de Dijkstra é $\mathcal{O}(n + m \log m)$, porque o algoritmo visita tódolos vértices do grafo e para cada aresta engade como moito unha distancia á cola de prioridade. Segundo como sexa a implementación, o custo pódese ver como $\mathcal{O}(n + m \log n)$, pero asintoticamente é o mesmo, xa que $\mathcal{O}(\log n) = \mathcal{O}(\log m)$.

Imos considerar o seguinte exemplo para ilustrar o algoritmo.



Consideremos que os pesos das arestas son os seguintes: a aresta AB ten peso 4; a aresta AC, peso 1; a aresta BD, 2; a aresta BE, 5; a aresta CD, 2; a aresta CE, 6; e a aresta DE ten peso 1. Imos ir explicando o proceso paso a paso.

1. Comezamos no vértice inicial, que ten distancia 0. Introducimos na cola de prioridade os vértices B e C, que están a distancia 4 e 1, respectivamente. Polo tanto, o seguinte vértice a visitar é o 1, que está xa a distancia 1.

2. Desde o vértice C, actualizamos as distancias: a distancia a D é $1 + 2 = 3$ e a distancia a E é $1 + 6 = 7$. O seguinte vértice a visitar é o D, porque entre os que está na cola é o que está a menor distancia do inicial, 3.

3. Desde o vértice D, actualizamos a distancia a E, que pasa a ser é $\text{mín}\{7, 3{+}1\} = 4$. En cambio, a distancia a B segue a ser 4, xa que $\text{mín}\{4, 3 + 5\} = 8$. O seguinte vértice a visitar é o B (tanto B como E están a distancia 4, collemos o B porque foi o primeiro en introducirse na cola).

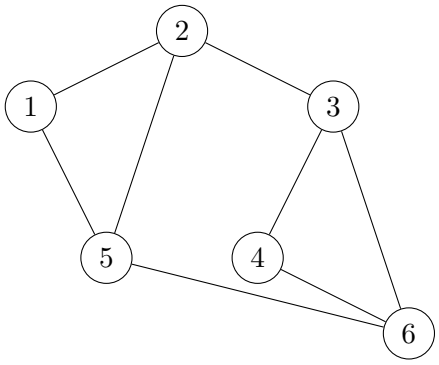
4. Desde o vértice B non se melloran as distancias a ningún dos vértices que faltan por visitar (neste caso o D). O seguinte vértice a visitar é o D, que xa é o último, é o E, a distancia 4.

5. As distancias aos vértices (A, B, C, D, E) son, polo tanto $(0, 4, 1, 3, 4)$.

En caso de desexalo, poderiamos ter gardado tamén o camiño a un dos vértices en concreto.
Finalmente, se queremos permitir pesos negativos, hai que modificar o algoritmo; é o que se coñece como algoritmo de Bellman–Ford. O custo deste tipo de algoritmos é $\mathcal{O}(n^3)$, mentres que o Dijkstra, no caso no que $m = \mathcal{O}(n^2)$ ten custo $\mathcal{O}(n^2 \log n)$, polo que sempre que sexa posible é conveniente usar o algoritmo de Dijkstra.

8.3. Arbore xeradora mínima: algoritmo de Kruskal

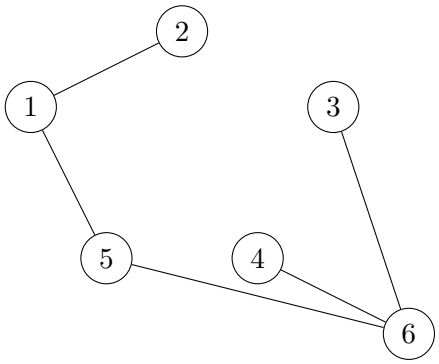
En árbores con pesos, hai diferentes algoritmos para atopar unha árbore xeradora de peso mínimo. Os principais son os de Kruskal e Prim. No algoritmo de Kruskal, comezamos unicamente cos vértices do grafo sen considerar ningunha das arestas. A continuación, procedemos aresta por aresta, en orde crecente de peso, e ímolas engadindo á árbore se non producen un ciclo.
Imos considerar o seguinte exemplo.



O peso de cada unha das seguintes arestas vén dado pola seguinte táboa.

Arestas	**Pesos**
5-6	2
1-2	3
3-6	3
1-5	5
2-3	5
2-5	6
4-6	7
3-4	9

Comezamos a engadir as primeiras arestas sen que se produzan ciclos: a 5-6, a 1-2, a 3-6 e a 1-5. A quinta aresta a engadir, que é a 2-3, produciría un ciclo, polo que non a consideramos. O mesmo sucede coa 2-5. Logo, a seguinte aresta que engadimos é a 4-6, o que deixa o grafo como segue.



O custo total da árbore é $2 + 3 + 3 + 5 + 7 = 20$.
Imos analizar agora o custo do algoritmo. Inicialmente hai que ordenar as arestas, que ten custo $\mathcal{O}(m \log m)$. A continuación, cada vez que seleccionamos unha aresta, cómpre determinar se forma ciclos ou non. O custo de cada comprobación é $\mathcal{O}(\log n)$. Polo tanto, o custo desta fase do algoritmo é $\mathcal{O}(m \log n)$.
A priori, non é evidente xustificar por que o algoritmo de Kruskal funciona sempre. Trátase dun *algoritmo voraz*, no que en cada paso se escolle a mellor opción nese momento. Supoñamos que a aresta de peso menor non se incluíse na árbore xeradora. Nese caso, sempre sería posible eliminar unha aresta da árbore e cambiala pola que ten peso menor, obtendo así unha árbore *mellor*.
O algoritmo de Prim é similar, pero considera vértices en lugar de arestas. Os pasos que segue son os seguintes:

1. Escóllese un vértice inicial de xeito arbitrario.
2. En cada paso, engádese unha aresta de peso mínimo entre aquelas que saen dos vértices xa seleccionados e que non formen ciclos. Isto implica tamén a elección dun novo vértice.
3. Repetimos o paso anterior ata ter incorporado tódolos vértices.

Capítulo 9

Álxebras de Boole

9.1. Álxebras de Boole: definicións

As álxebras de Boole constitúen unha área das matemáticas. Foron introducidas por George Boole no marco da lóxica e tiveron unha gran relevancia no desenvolvemento da teoría da computación ao longo do século XX. A definición formal de álxebra de Boole é a seguinte.

Definición 9.1. Sexa $(A, +, \cdot, 0, 1, \bar{\ })$ un conxunto A con dúas operacións internas, $+$ e $\cdot$, elementos $0, 1 \in A$ e unha aplicación $\bar{\ } : A \to A$ chamada *complemento* ou *inversión*, e de xeito que se cumpren as seguintes propiedades:

(a) $+$ e $\cdot$ son *asociativas*.

(b) $+$ e $\cdot$ son *conmutativas*.

(c) O 0 é un elemento neutro para $+$ e o 1 é un elemento neutro para $\cdot$.

(d) A operación $\bar{\ }$ cumpre que $a + \bar{a} = 1$ e $a \cdot \bar{a} = 0$ para todo $a \in A$.

(e) A operación $+$ é distributiva con respecto de $\cdot$ e viceversa.

O exemplo principal que xa traballamos ao longo do curso obtense a partir dun conxunto X, considerando $(\mathcal{P}(X), \cup, \cap, X, \emptyset, \bar{\ })$. O feito de que sexa unha álxebra de Boole derívase das propiedades da unión, da intersección e do paso ao complementario que se traballaron ao estudarmos a teoría de conxuntos.

Exemplo. Sexa $A = \{0, 1\}$ coas operacións suma e produto dadas por $a + b = 1$ se unha das variables é 1 e 0 en caso contrario, e $a \cdot b = 1$ se $a = b = 1$ e 0 en caso contrario. Ademais, definimos $\bar{0} = 1$ e $\bar{1} = 0$. Isto dota ao conxunto A coa estrutura de álxebra de Boole.

Proposición 9.1. Sexa $(A, +, \cdot, 0, 1, \bar{\ })$ unha álxebra de Boole. Cúmprense entón as seguintes propiedades.

(a) **Idempotencia.** Se $a \in A$, entón $a + a = a$ e $a \cdot a = a$.

(b) Se $a \in A$, $a + 1 = a$ e $a \cdot 0 = 0$.

(c) **Absorción**. Se $a, b \in A$, entón $a + (a \cdot b) = a$ e $a \cdot (a + b) = a$.

(d) Se $a \in A$ e $b \in A$ cumpre que $a + b = 1$ e $a \cdot b = 0$, entón $b = \bar{a}$.

(e) **Leis de Morgan**. Se $a, b \in A$, $\overline{a+b} = \bar{a} \cdot \bar{b}$ e $\overline{a \cdot b} = \bar{a} + \bar{b}$.

(f) Se $a \in A$, $\bar{\bar{a}} = a$.

(g) Se $a, b \in A$, $a + (\bar{a} \cdot b) = a + b$ e $a \cdot (\bar{a} + b) = a \cdot b$.

9.2. Funcións booleanas

Definición 9.2. Dada unha álxebra de Boole A, unha función booleana sobre A en n variables é unha aplicación

$$f \colon A \times \ldots \times A \longrightarrow A.$$

A continuación, imos introducir notación que precisaremos ao longo do tema e que é especialmente frecuente no eido da lóxica.

Definición 9.3. Sexa A unha álxebra de Boole e $x \in A$. Escribimos $\neg x := \bar{x}$ para o complementario de x. De xeito similar, pomos $x \vee y := x + y$ e $x \wedge y := x \cdot y$.

Estes símbolos empréganse con frecuencia na lóxica proposicional. Se p é unha certa proposición, entón $\neg p$ representa a negación de p e lese *non p*. Por outra banda, $p \wedge q$ lese *p e q*, e esixe que sucedan tanto p como q; $p \vee q$ lese *p ou q* e esixe que suceda ou p ou q (unha delas ou ambas); finalmente $p \bar{\vee} q$ lese *p ou q, pero non os dous.*

p	q	$p \wedge q$	$p \vee q$	$p \bar{\vee} q$
1	1	1	1	0
1	0	0	1	1
0	1	0	1	1
0	0	0	0	0

Exemplo. Consideramos a función booleana $f \colon A \times A \times A \to A$ definida por $f(x, y, z) = (x + \bar{y}) \cdot z$. A *táboa da verdade* de f é un cadro no que se indica canto vale a función f segundo os valores das outras variables. Neste caso, como hai dúas opcións para os valores de x, y e z, hai un total de $2^3 = 8$ posibilidades. Iso quere dicir que a táboa constará de 8 filas; para cada elección dos valores, $f(x, y, z)$ pode ser ou 0 ou 1.

x	y	z	$\neg y$	$x \vee \neg y$	$(x \vee \neg y) \wedge z$
0	0	0	1	1	0
0	0	1	1	1	1
0	1	0	0	0	0
0	1	1	0	0	0
1	0	0	1	1	0
1	0	1	1	1	1
1	1	0	0	1	0
1	1	1	0	1	1

Imos ver agora outro exemplo, neste caso de catro variables, dado por $g(x, y, z, w) = x \cdot y + \bar{z} \cdot w$. Ao igual que no caso anterior, podemos facer a táboa da verdade correspondente, que neste caso terá 16 filas correspondentes ás $2^4 = 16$ posibilidades diferentes.

x	y	z	w	$x \wedge y$	$\neg z$	$\neg z \wedge w$	$(x \wedge y) \vee (\neg z \wedge w)$
0	0	0	0	0	1	0	0
0	0	0	1	0	1	1	1
0	0	1	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	0	0	1	0	0
0	1	0	1	0	1	1	1
0	1	1	0	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	1	0	0
1	0	0	1	0	1	1	1
1	0	1	0	0	0	0	0
1	0	1	1	0	0	0	0
1	1	0	0	1	1	0	1
1	1	0	1	1	1	1	1
1	1	1	0	1	0	0	1
1	1	1	1	1	0	0	1

Un dos resultados máis importantes no estudo das funcións booleanas é o seguinte, coñecido como teorema de Shannon. Antes de presentalo, e a modo de notación, introducimos o concepto de *literal* para denotar unha variable ou unha variable negada.

Proposición 9.2 (Teorema de Shannon)**.** Calquera función booleana pódese escribir en *forma normal disxuntiva* como suma de produtos de literais e en *forma normal conxuntiva* como produto de sumas de literais.

A demostración do resultado é inmediata e pódese realizar de xeito construtivo. Imos traballar algúns exemplos que ilustran como obter tamén de xeito práctico as formas normais correspondentes.

Exemplo. A expresión $a + b$ é a forma normal disxuntiva. Porén, iso escríbese tamén como

$$a + b = (a \cdot \bar{b}) + (\bar{a} \cdot b) + (\bar{a} \cdot \bar{b}).$$

De xeito similar, a expresión $a \cdot b$ é unha forma normal conxuntiva. A expresión escríbese como

$$a \cdot b = (\bar{a} + \bar{b}) \cdot (\bar{a} + b) \cdot (a + \bar{b}).$$

Imos agora traballar como converter calquera función booleana a forma normal disxuntiva ou conxuntiva.

Exemplo. Consideramos a función booleana dada pola seguinte táboa.

x	y	z	$g(x, y, z)$
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	0

Para a forma normal disxuntiva, observamos que os valores sobre os que a función vale 1 son o $(1,1,0)$, o $(1,0,0)$ e o $(0,1,0)$, que se corresponden con $x \cdot y \cdot \bar{z}$, $x \cdot \bar{y} \cdot \bar{z}$ e $\bar{x} \cdot y \cdot \bar{z}$, respectivamente. Polo tanto, a forma normal disxuntiva é

$$g(x,y,z) = x \cdot y \cdot \bar{z} + x \cdot \bar{y} \cdot \bar{z} + \bar{x} \cdot y \cdot \bar{z}.$$

Para obter a forma normal conxuntiva o que facemos é considerar os valores sobre os que a función vale 0: neste caso temos o $(1,1,1)$, o $(1,0,1)$, o $(0,1,1)$, o $(0,0,1)$ e o $(0,0,0)$. Para cada un deles, consideramos a suma das variables, como $\bar{x} + \bar{y} + \bar{z}$ no primeiro caso, e logo tomamos o produto de todos eles:

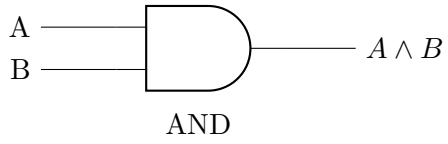
$$g(x,y,z) = (\bar{x} + \bar{y} + \bar{z}) \cdot (\bar{x} + y + \bar{z}) \cdot (x + \bar{y} + \bar{z}) \cdot (x + y + \bar{z}) \cdot (x + y + z).$$

9.3. Portas lóxicas

Definición 9.4. As portas lóxicas son circuítos, polo xeral electrónicos, que simulan as operacións lóxicas.

Imos discutir os casos máis comúns.

- **Porta AND.** O primeiro é un dos exemplos máis habituais, coa función AND, que se corresponde coa operación produto.

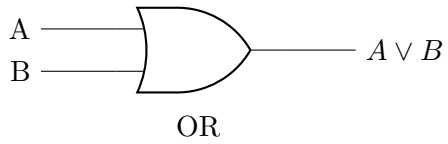


AND

Podemos representar a porta lóxica mediante a seguinte táboa da verdade, que amosa cal é a saída en función da entrada.

A	B	$A \wedge B$
1	1	1
1	0	0
0	1	0
0	0	0

- **Porta OR.** A seguinte porta lóxica representa a chamada *porta OR* (suma).

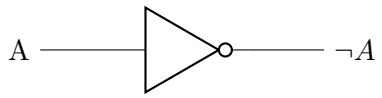


OR

A táboa da verdade correspondente é a seguinte.

A	B	$A \vee B$
1	1	1
1	0	1
0	1	1
0	0	0

- **Porta NOT.** Esta porta lóxica non require dúas entradas, senón unicamente unha, e produce a negación desa variable.

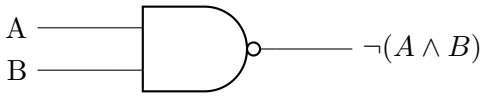


NOT

A táboa da verdade só ten dúas filas neste caso.

A	$\neg A$
1	0
0	1

- **Porta NAND.**

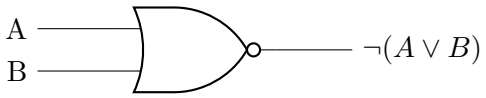


NAND

Esta porta lóxica corresponde a aplicar primeiro a AND e logo a NOT.

A	B	$\neg(A \wedge B)$
1	1	0
1	0	1
0	1	1
0	0	1

- **Porta NOR.**

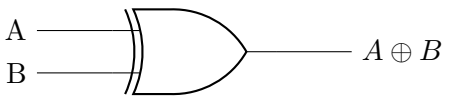


NOR

Esta porta lóxica corresponde a aplicar primeiro a OR e logo a NOT.

A	B	$\neg(A \wedge B)$
1	1	0
1	0	0
0	1	0
0	0	1

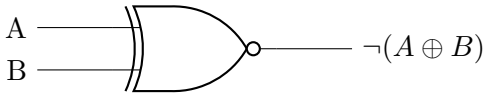
- **Porta XOR.**



XOR

A	B	$\neg(A \wedge B)$
1	1	0
1	0	1
0	1	1
0	0	0

- **Porta XNOR.**



XNOR

A	B	$\neg(A \wedge B)$
1	1	1
1	0	0
0	1	0
0	0	1

9.4. Minimización de circuítos

O obxectivo desta última parte é explicar como os diagramas de Karnaugh se poden empregar para simplificar funcións booleana ata chegar a unha forma mínima. Isto é importante, por exemplo, para a implementación electrónica, xa que queremos empregar o menor número posible de portas lóxicas.
A modo de exemplo, consideremos a función de dúas variables dada por

x	y	$f(x,y)$
1	1	1
1	0	0
0	1	1
0	0	0

En forma normal, iso corresponderíase coa función $f(x,y) = x \cdot y + \bar{x} \cdot y$. Porén, esa expresión pódese simplificar e escribila como

$$f(x,y) = x \cdot y + \bar{x} \cdot y = (x + \bar{x}) \cdot y = 1 \cdot y = y.$$

A expresión de $f(x,y)$ como y é *máis simple* que a anterior, polo que, de cara á súa implementación, é preferible.
O proceso que podemos seguir neste caso é o seguinte. No caso de dúas variables, facemos unha táboa 2×2, e cando hai dúas celas adxacentes, podemos reducir unha variable (isto é, buscamos onde sacar factor común). No caso de tres variables, facemos unha táboa 2×4, e observamos que cando hai dúas celas adxacentes podemos reducir unha variable e no caso dos bloques de tamaño catro reducimos dúas variables.
Imos facer un exemplo paso a paso, partindo da seguinte táboa.

x	y	z	$f(x,y,z)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

Agora, construímos o diagrama de Karnaugh correspondente, coas celas marcadas para os valores de $f(A,B,C) = 1$:

$xy\backslash z$	0	1
00	1	1
01	0	1
11	0	0
10	1	1

O seguinte paso é simplificar o de Karnaugh, agrupando os uns:

- O primeiro grupo é o correspondente a y', isto é, o bloque 2×2 no que $y = 0$.
- O segundo grupo é o correspondente a $x = 0$ e $z = 1$, que dá un bloque 2×1.

A expresión booleana simplificada é, polo tanto,

$$f(x,y,z) = \bar{y} + \bar{x} \cdot z.$$