Apunts de Matemàtica Discreta

Curs 2022-2023

Leila Lebtahi - Juan Monterde

Índex

Introducció

L'assignatura **Matemàtica discreta** és una matèria apareguda com a tal en el Nou Pla d'Estudis del Grau de Matemàtiques. En els plans d'estudi anteriors del Títol de Llicenciat en Matemàtiques, aquesta assignatura no hi apareixia, encara que gran part dels seus continguts sí que es tractaven, amb més o menys profunditat, en altres assignatures de primer cicle.

S'ha impartit per primera vegada al curs 2010/2011, el primer any d'implantació del Grau de Matemàtiques, ja que és una assignatura de primer curs, segon quadrimestre.

És una assignatura de 6 crèdits dividida en:

1. una part teòrica, 3 crèdits, a raó de dues hores setmanals,
2. una part pràctica, 2.25 crèdits, consistent en 15 sessions d'una hora i mitja de duració per sessió,
3. quatre sessions de seminaris i tutories reglades que equivalen a 0.75 crèdits.

Hi ha tantes matemàtiques discretes com llibres sobre matemàtica discreta. Cada text té la seua visió del que és aquesta matèria heterogènia. Aquest no podia ser menys.
Ací trobareu quatre introduccions a diferents parts de l'assignatura.

Primer, recordarem tècniques d'enumeració i recompte, per exemple el principi d'inclusió-exclusió. Seguirem amb els típics problemes de combinatòria per a passar a mostrar com l'ajuda de les funcions generatrius permet resoldre, de manera molt elegant, alguns d'aquests problemes.

Segon, estudiarem les tècniques per a trobar el terme general de successions definides per lleis de recurrència o per equacions en diferències finites. Aquestes successions apareixen per exemple en la discretització de processos continus. Aquesta és una de les característiques de la matemàtica discreta: passar del continu al discret.

Tercer, veurem una molt reduïda introducció a la teoria de grafs, una de les parts importants històricament en la matemàtica discreta.

I quart, repassarem nocions d'aritmètica modular per tal de resoldre equacions diofàntiques i acabarem amb una introducció de les aplicacions de la teoria de nombres a la criptografia.

Un darrer comentari sobre el nom de la matèria. L'adjectiu "discreta" aplicat a "matemàtica" té el seu origen en els processos coneguts com a "discretització". Una discretització permet passar, per exemple,

d'una funció contínua a només un conjunt finit, o com a molt numerable, de punts. Les discretitzacions són la tècnica habitual en l'obtenció de solucions aproximades de molts problemes matemàtics, fonamentalment, en equacions diferencials o en derivades parcials. Aixíper exemple, una equació en diferències finites (capítol 2) es pot interpretar com a la discretització d'una equació diferencial. Per extensió, tot allò que tracta de matemàtiques basades en els conjunts numerables (i per tant, també en conjunts finits) és el que ara es pot englobar en el terme "matemàtica discreta".

1. Mètodes d'enumeració i combinatòria

Aprendrem en aquest capítol tècniques bàsiques per a comptar, aplicades a diferents aspectes:

- Comptar els elements d'un conjunt, com per exemple els elements de $A \cap B$ o els de $A \times B$, amb els principis de la suma, del producte i d'inclusió-exclusió.
- Comptar les maneres de seleccionar k objectes de n, amb o sense repetició, i considerant l'ordre o no considerant-lo. És la combinatòria clàssica: permutacions, combinacions i variacions.
- Comptar les formes en què es poden repartir objectes en caixes, per al que emprarem la combinatòria clàssica i també mostrarem, en la segona part del capítol, com l'ajuda de les funcions generatrius permet resoldre, de manera molt elegant, alguns d'aquests problemes.

1.1 Tècniques de recompte

Definició 1.1.1 *Si A és un conjunt, denotarem per $|A|$ el seu cardinal: la quantitat d'elements del conjunt A.*

Dos principis fonamentals per a comptar:

Principi de la suma:

$$\boxed{\text{Si } A \cap B = \emptyset \Rightarrow |A \cup B| = |A| + |B|}$$

Principi del producte:

$$\boxed{|A \times B| = |A| \times |B|}$$

Exemple 1.1 *Volem formar una junta directiva formada per un president, un secretari i un tresorer entre cinc possibles candidats: Anna, Biel, Carles, Daniel i Erika. Quantes possibles juntes directives podem formar si permetem que una persona puga assumir més d'un càrrec?*

Siga $C = \{Anna, Biel, Carles, Daniel, Erika\}$. Si permetem repeticions en els càrrecs, aleshores, ens estan preguntant pel cardinal del conjunt $C \times C \times C$, és a dir:

$$|C \times C \times C| = |C|^3 = 5^3 = 125.$$

I si no es permeten repeticions? És a dir, si, per exemple, ja s'ha triat president, aleshores el secretari es tria només entre les quatre persones restants, i així successivament. En aquest cas,

$$|C \times (C - \{\textit{president}\}) \times (C - \{\textit{president, secretari}\})| = 5 \cdot 4 \cdot 3 = 60.$$

En general, tractarem de comptar de quantes maneres diferents es poden triar k objectes d'un conjunt de n elements. Estudiarem les diferents possibilitats amb exemples il·lustratius per a entendre correctament les diferències que existeixen entre els diferents casos. Començarem amb les variacions i el següent problema:

Determinar quantes paraules formades per 5 bytes es poden construir. O equivalentment quants nombres enters es poden emmagatzemar amb 5 bytes.

El conjunt de les paraules formades per cinc bytes, és a dir, per cinc elements del conjunt $A = \{0, 1\}$ és $A \times A \times A \times A \times A$ i per tant, usant la propietat del cardinal d'un producte, són $2^5 = 32$ paraules. És a dir, ara el que estem comptant són seleccions ordenades de 5 elements (possiblement repetits) d'un conjunt de 2 elements.

Això ens permet plantejar el concepte de **variacions**.

Cas 1. Variacions amb repetició: $VR(n, k) = n^k$.

- Donat un conjunt A de cardinal n, direm variació amb repetició d'ordre k a qualsevol llista **ordenada** que estiga formada per exactament k elements de A **no necessàriament diferents**, convenint que dues variacions amb repetició seran diferents si tenen algun element diferent o fins i tot, tenint-hi els mateixos elements, aquests estan ordenats de diferent manera.
- Una altra manera de definir-les és dient que una variació amb repetició d'ordre k és qualsevol aplicació del conjunt $\{1, 2, 3, \ldots, k\}$ (o de qualsevol conjunt de cardinal k) en el conjunt A.

Ara, modificant el problema:

Donada una carrera amb 162 participants, determinar quants possibles resultats poden produir-se per al podi (or, plata i bronze).

El problema equivalent és calcular el nombre d'aplicacions injectives d'un conjunt de 3 elements en un de 162. En efecte, per al guanyador de l'or hi ha 162 possibilitats (qualsevol corredor); una vegada establit qui ha guanyat l'or, per al guanyador de la medalla de plata hi ha 161 possibilitats; i sabent el guanyador de l'or i la plata tenim 160 resultats possibles per al bronze. D'aquesta manera hi ha $162 \times 161 \times 160$ possibles resultats de la carrera. D'aquesta manera, estem comptant exactament les seleccions ordenades de 3 elements en un conjunt de 162 elements.

Cas 2. Variacions ordinàries o sense repetició: $V(n, k) = \dfrac{n!}{(n-k)!}$.

- Donat un conjunt A de cardinal n, direm variació ordinària o variació sense repetició d'ordre k a qualsevol llista **ordenada** que estiga formada per exactament k elements de A **necessàriament diferents**,

convenint que dues variacions sense repetició seran diferents si tenen algun element diferent o fins i tot tenint els mateixos elements, estan ordenats de diferent manera.

• Una altra manera de definir-les és dient que una variació sense repetició d'ordre k és qualsevol aplicació **injectiva** del conjunt $\{1, 2, 3, \ldots, k\}$ (o de qualsevol conjunt de cardinal k) en el conjunt A.

Permutacions

El cas particular de les variacions és quan $k = n$, és a dir, quan tractem de comptar el nombre d'aplicacions injectives d'un conjunt de n elements en aquest. Per tant és comptar el nombre d'aplicacions bijectives del conjunt $\{1, 2, \ldots, n\}$ en si mateix. I justament el que estem comptant són les diferents maneres d'ordenar un conjunt de n elements. Cada possible ordenació d'un conjunt de n elements és una permutació d'aquests n elements.
Per tant, el nombre de permutacions del conjunt $\{1, 2, \ldots, n\}$ és $n!$.

Introduïm ara una variant en el problema del càlcul de les diferents ordenacions. Suposem que ens plantegen el següent enunciat:

Estudia quants nombres diferents es poden construir reordenant les xifres del nombre 252.

És clar que el problema no es resol calculant el nombre de permutacions de 3 elements (que són 6). No es resol així perquè els nombres obtinguts com a resultat de reordenar les xifres del 252 són: 252, 522, 225. Són solament 3 perquè el nombre 2 està repetit 2 vegades. D'aquesta manera, com les maneres de reordenar els dossos són exactament dos, s'ha de dividir per 2 per a comptar-les només una vegada: $6/2 = 3$.
I generalitzant:

Cas 3. Permutacions amb repetició: $PR^n_{n_1 n_2 \ldots n_s} = \dfrac{n!}{n_1!\, n_2!\, \ldots\, n_s!}$.

• El nombre de permutacions amb repetició de n elements, on hi ha s elements que es repeteixen $n_1 \geq 1$, $n_2 \geq 1$, …, $n_s \geq 1$ vegades respectivament ($n_1 + n_2 + \cdots + n_s = n$), és el nombre $PR^n_{n_1, n_2, \ldots, n_s}$ de diferents ordenacions d'eixa llista amb elements repetits.

L'últim concepte de combinatòria que definirem és el de combinacions. Fa referència al següent problema:

Determinar quants subconjunts de 3 elements té el conjunt $\{1, 2, 3, \ldots, 65\}$.

Si calculem $V(65, 3)$, llavors estem computant, no els subconjunts, sinò les seleccions ordenades de tres elements. D'aquesta manera cada subconjunt de 3 elements l'estem comptant més d'una vegada. Exactament el comptem tantes vegades com maneres diferents hi ha de reordenar-ho, és a dir, 3! vegades. Per exemple, el conjunt $\{1, 2, 3\}$ és el mateix que $\{3, 2, 1\}$. Per tant, el problema es resol calculant $\frac{V(65,3)}{3!}$, per a, efectivament, només comptar cada subconjunt una vegada.
Aquest tipus de problema dóna lloc al cas següent:

Cas 4. Combinacions ordinàries o sense repetició: $C(n, k) = \dfrac{V(n, k)}{k!} = \dfrac{n!}{k!(n-k)!} = \binom{n}{k}$, $0 \leq k \leq n$.

• Donat un conjunt A de cardinal n, direm nombre de combinacions de n elements agafats de k en k, que escrivim $C(n,k)$, al nombre de subconjunts de k elements en A. Escriurem $C(n,k) = \binom{n}{k}$ i es denomina nombre combinatori n sobre k.

Una altra manera de definir-les és dient que una combinació sense repetició d'ordre k és
• el nombre de subconjunts de k elements d'un conjunt de n elements.
• el nombre de seleccions no ordenades de k elements en un conjunt de n elements.

Ara vegem com es pot modificar el problema de les combinacions.

Exemple 1.1.2 *Imagineu, per exemple, que dues persones han de triar cadascuna un gelat entre tres possibles sabors, A, B, C. Per tant, les possibles eleccions són AA, BB, CC, AB, AC, BC. Així, el nombre de combinacions amb repetició de tres elements d'ordre 2 és 6.*

Compliquem-ho encara un poc més.

Exemple 1.1.3 *Suposem que 7 amics acudeixen a una gelateria, que poden triar entre 10 possibles sabors distints i que el gelater té prou memòria per demanar primer què volen tots i després servir-ho tot alhora. Quantes comandes possibles poden fer els 7 amics?*

Imaginem que els sabors són $A, B, C, D, E, F, G, H, I, J$ i que demanen 3 de A, 1 de E, 1 de H i 2 de J. Podem codificar això de la següent manera:

$$\begin{array}{cccccccccccccccccc} A & & B & & C & & D & & E & & F & & G & & H & & I & & J \\ \cdots & | & & | & & | & & | & \cdot & | & & | & & | & \cdot & | & & | & \cdot\cdot \end{array}$$

Si ens fixem en la segona fila de ratlles i punts, observem que a cada possible combinació amb repetició li podem assignar un codi format per $(10-1)$ ratlles i 7 punts, havent-hi en total $10+7-1$ elements del conjunt $\{\cdot, |\}$ en els quals el punt està repetit 7 vegades i la ratlla $10-1=9$. Es tracta doncs ara d'un problema de permutacions amb repetició:

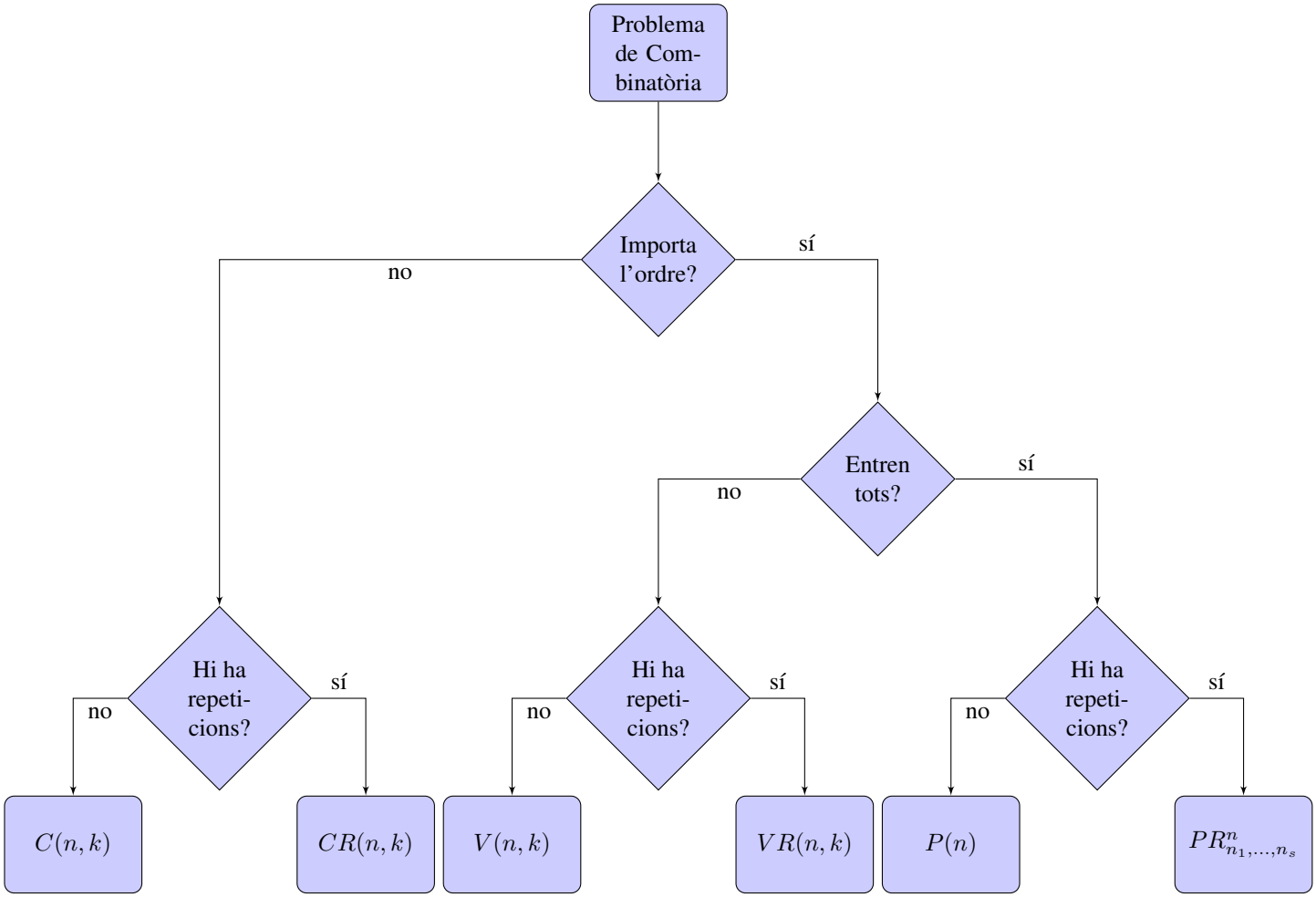
$$PR_{7,9}^{10+7-1} = \frac{(10+7-1)!}{7!\,9!} = \frac{16!}{7!\,9!}.$$

Aquest exemple el podem veure com un problema de comptar les maneres de repartir n objectes indistingibles (els 7 amics) en k caixes diferents (els deu sabors).
Aquest mateix raonament permet calcular la fórmula general.

Cas 5. Combinacions amb repetició: $CR(n,k) = \binom{n+k-1}{k}$.

• Donat un conjunt de cardinal n, definim el nombre de combinacions amb repetició de n elements agafats de k en k al nombre de seleccions no ordenades de k elements (amb possibles repeticions) en un conjunt de n elements.

Resumint els conceptes vistos fins ara, es té:



1.2 El nombre de subconjunts d'un conjunt

Ja hem vist abans (Cas 4) que el nombre de subconjunts de k elements d'un conjunt de n elements és el nombre binomial $\binom{n}{k}$. El que volem calcular ara és el cardinal de la família de conjunts formada per tots els subconjunts d'un conjunt de cardinal n.

1.2.1 *El conjunt potència i el conjunt de les parts d'un conjunt*

En aquesta secció considerem conjunts qualssevol, no necessàriament finits.

Definició 1.2.1 *Siguen X i Y dos conjunts, anomenem conjunt potència al conjunt de totes les aplicacions*

de X en Y, denotat per Y^X o més explícitament:

$$Y^X = \{f/\ f : X \to Y\}$$

Definició 1.2.2 *Donat un conjunt X, anomenem conjunt de les parts de X al conjunt format per tots els seus subconjunts:*

$$\mathcal{P}(X) = \{A \subseteq X\}$$

El conjunt buit, $\emptyset$ i el conjunt total, és a dir, el propi X, són elements trivials de les parts de X.

Definició 1.2.3 *Donat un conjunt X i un subconjunt $A \subseteq X$, anomenem funció característica de A en X a l'aplicació: $\varphi_A : X \to \{0,1\}$ tal que*

$$\varphi_A(x) = \begin{cases} 0 & si\ x \notin A \\ 1 & si\ x \in A \end{cases}.$$

Proposició 1.2.4 *Donat un conjunt X, existeix una aplicació bijectiva entre $\mathcal{P}(X)$ i $\{0,1\}^X$.*

Demostració. És una demostració constructiva. Definim l'aplicació $\psi : \mathcal{P}(X) \to \{0,1\}^X$ tal que $\psi(A) = \varphi_A$. Anem a provar que ψ és una bijecció.

• (ψ injectiva) Suposem que tenim dos subconjunts A i B tal que $\psi(A) = \psi(B)$. Hem de provar que $A = B$. Siga $x \in A$. Sabem que $\varphi_A(x) = 1$; com que $\psi(A)(x) = \psi(B)(x)$, aleshores $\varphi_B(x) = 1$, però això només pot passar si $x \in B$. Per tant, $x \in B$.

Siga ara $x \notin A$. Sabem que $\varphi_A(x) = 0$; per tant, $\varphi_B(x) = 0$, però això només pot passar si $x \notin B$. Per tant, $x \notin B$.

Això prova que $\psi(A) = \psi(B)$ implica que $A = B$, i així ψ és injectiva.

• (ψ suprajectiva) D'altra banda, donada una aplicació $f : \mathcal{X} \to \{0,1\}$, prenem $A = f^{-1}(\{1\})$. Anem a comprovar que $\psi(A) = f$. En efecte, com que $A = \{x \in X$ tal que $f(x) = 1\}$ tenim que

a) si $x \in A$ llavors $f(x) = 1$.

b) si $x \notin A$ llavors $f(x) = 0$ perquè no hi ha una altra possibilitat.

Observem que f dóna les mateixes imatges que φ_A. Per tant $f = \varphi_A = \psi(A)$.

Això vol dir que ψ és suprajectiva. □

Aprofitant que dos conjunts finits sobre els quals existeix una bijecció tenen el mateix cardinal, tenim el següent resultat:

Corol·lari 1.2.5 *Si A és un conjunt finit i $\mathcal{P}(A)$ el conjunt de les parts de A, el nombre de subconjunts de A és $2^{|A|}$, es a dir,*

$$|\mathcal{P}(A)| = 2^{|A|}.$$

Demostració. Per la proposició anterior, $|\mathcal{P}(A)| = |\{0,1\}^A| = VR(\{0,1\}, |A|) = |\{0,1\}|^{|A|} = 2^{|A|}$. □

1.3 El binomi de Newton. Fórmula de Leibniz per a la potència d'un polinomi.

Recordem la fórmula del binomi de Newton:

$$(a+b)^n = \sum_{i=0}^{n} = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n}b^n$$

que es pot demostrar fàcilment per inducció.
Si la particularitzem per a $a = 1$ i $b = x$, tenim que

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n.$$

Com veiem, el coeficient de cada monomi és un nombre combinatori que hem fet servir per a comptar elements d'algun conjunt.
Per exemple, el coeficient de x^7 en $(1+x)^{20}$ és $C(20,7) = \binom{20}{7}$, que és la quantitat de subconjunts de 7 elements que té un conjunt de 20 elements.

Podem aprofitar la fórmula anterior per a trobar diversos resultats.
Per exemple, si substituïm x per 1, s'obté el resultat següent:

$$\textit{Per a tot } n \in \mathbb{N},\ \sum_{i=0}^{n}\binom{n}{i} = 2^n.$$

Podem preguntar-nos ara:

Quants subconjunts de cardinal parell té un conjunt de n elements?

Si en l'equació $(1+x)^n = \sum_{k=0}^{n}\binom{n}{k}x^k$, prenem $x = 1$ i després $x = -1$, s'obté:

$$2^n = \sum_{k=0}^{n}\binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{n}$$

i

$$0 = \sum_{k=0}^{n}(-1)^k\binom{n}{k} = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + (-1)^n\binom{n}{n}.$$

Sumant les dos equacions, arribem a

$$2^n = 2\sum_{\ell=0}^{\lfloor n/2\rfloor}\binom{n}{2\ell} = 2\left(\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \dots\right).$$

La quantitat de subconjunts de cardinal parell d'un conjunt de n elements és 2^{n-1}.

Propietats 1.3.1 (dels coeficients binomials)

$$\binom{n}{k} = \binom{n}{n-k} \quad \textit{per a } n \geq 1 \textit{ y } 0 \leq k \leq n.$$

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \quad \textit{per a } n \geq 2 \textit{ y } 1 \leq k \leq n-1.$$

Ara ens centrarem en una generalització a polinomis del teorema del binomi. Concretament és el desenvolupament de

$$(x_1 + x_2 + \cdots + x_n)^m.$$

Si desenvolupem els productes (en total m factors o parèntesis), per a calcular el coeficient de cada monomi, obtindrem termes com aquest:

$$x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}, \quad \text{amb} \quad \alpha_1 + \alpha_2 + \cdots + \alpha_n = m.$$

Podem procedir de la següent manera:

Hi ha $\binom{m}{\alpha_1}$ maneres de triar els parèntesis dels quals prenem el factor x_1.

Hi ha $\binom{m-\alpha_1}{\alpha_2}$ maneres de triar els parèntesis dels quals prenem el factor x_2.

Procedint-hi d'igual manera fins a acabar amb l'últim factor, tenim que aquest coeficient serà:

$$\binom{m}{\alpha_1}\binom{m-\alpha_1}{\alpha_2}\binom{m-\alpha_1-\alpha_2}{\alpha_3}\cdots\binom{m-\alpha_1-\alpha_2-\cdots-\alpha_{n-1}}{\alpha_n} =$$

$$\frac{m!}{\alpha_1!(m-\alpha_1)!}\cdot\frac{(m-\alpha_1)!}{\alpha_2!(m-\alpha_1-\alpha_2)!}\cdots\frac{(m-\alpha_1-\alpha_2-\cdots-\alpha_{n-1})!}{\alpha_n!} =$$

$$= \frac{m!}{\alpha_1!\alpha_2!\alpha_3!\cdots\alpha_n!} = PR^m_{\alpha_1,\alpha_2,\dots,\alpha_n}.$$

Proposició 1.3.2 *(Fórmula de Leibniz) El desenvolupament en monomis de* $(x_1 + x_2 + \cdots + x_n)^m$ *és*

$$(x_1 + x_2 + \cdots + x_n)^m = \sum_{\alpha_1+\alpha_2+\cdots+\alpha_n=m} \binom{m}{\alpha_1\alpha_2\dots\alpha_n} x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \tag{1.1}$$

on $\alpha_1 + \alpha_2 + \cdots + \alpha_n = m$ *y* $\binom{m}{\alpha_1\alpha_2\dots\alpha_n} = \frac{m!}{\alpha_1!\alpha_2!\alpha_3!\cdots\alpha_n!} = PR^m_{\alpha_1,\alpha_2,\dots,\alpha_n}$*, anomenats coeficients multinomials.*

Aquest resultat el podem considerar també com un problema de comptar les maneres de repartir m objectes en n caixes, de manera que a cada caixa vaja un nombre d'objectes determinat: α_1 objectes a la caixa 1, α_2 a la caixa 2, ... i α_n a la caixa n. Aquests nombres, $\alpha_i, i = 1, 2 \dots, n$, han de sumar m i poden ser zero, és a dir, pot haver-hi en aquest cas caixes que resten buides. El nombre d'aquests repartiments és $PR^m_{\alpha_1,\alpha_2,\dots,\alpha_n}$.

Exemple 1.3.3 *En un restaurant hi ha cinc taules diferents. De quantes formes es poden col·locar deu persones, si en la taula 1 ha d'haver-hi quatre persones, en la 2 tres, en la 3 altres tres, i han de restar buides les taules 4 i 5?*
La resposta és $PR^{10}_{4,3,3,0,0} = \frac{10!}{4!3!3!0!0!} = 4200$.

Exemple 1.3.4 *Demostrar que*

$$\sum_{\alpha_1+\alpha_2+\cdots+\alpha_n=m} \binom{m}{\alpha_1\alpha_2\dots\alpha_n} = n^m.$$

Exemples 1.3.5 *Trobar el coeficient de*

1. x^3y^4z *en el desenvolupament de* $(x+y+z)^8$. *(Sol: 280)*
2. x^3y^5 *en el desenvolupament de* $(3x+4y+2)^{10}$. *(Sol: 278691840)*

1.4 Principi d'inclusió-exclusió

Calcular la quantitat de nombres naturals majors que zero i menors o iguals que 100 que són divisibles per 2 és ben fàcil. Mireu que la condició determina un subconjunt $C_2 = \{2, 4, 6, \ldots, 100\}$ del conjunt $X = \{1, 2, \ldots, 100\}$. La pregunta no és una altra que determinar el cardinal de C_2. Com que, de cada dos naturals consecutius, un d'ells és divisible per 2 i l'altre no, aleshores $|C_2| = \frac{100}{2} = 50$.

Compliquem un poc més la cosa. Ara volem calcular la quantitat de nombres naturals majors que zero i menors o iguals que 100 que són divisibles per 2 o per 5. Si denotem per C_5 el subconjunt de X format pels naturals divisibles per 5, aleshores ens estan demanant pel cardinal de $C_2 \cup C_5$, és a dir, el subconjunt format pels elements que estan en C_2 o en C_5. Hi ha casos molt diversos. Per exemple, el 14 està en C_2 però no en C_5. El 15 està en C_5 però no en C_2. Un darrer cas és el del 20, que pertany alhora a C_2 i a C_5, és a dir, pertany a la intersecció, $C_2 \cap C_5$.
Si la intersecció fòra buida, aleshores el cardinal de la unió, pel principi de la suma, seria la suma dels cardinals. Com que no ho és, hem de llevar, de la suma dels cardinals, els elements que estan en la intersecció, perquè els hem comptat dues vegades. És a dir,

$$|C_2 \cup C_5| = |C_2| + |C_5| - |C_2 \cap C_5|.$$

Recordem que la intersecció de dos conjunts X i Y la denotarem per $X \cap Y$, encara que de vegades també ens podem trobar amb la notació que fa servir el producte per a la intersecció de conjunts XY.
Noteu finalment que el conjunt $C_2 \cap C_5$ no és un altre que el format pels nombres divisibles alhora per 2 i per 5, és a dir, els divisibles per 10. Per tant, $|C_2 \cap C_5| = |C_{10}| = \frac{100}{10} = 10$. Així, la quantitat de nombres naturals majors que zero i menors o iguals que 100 que són divisibles per 2 o per 5 és

$$|C_2 \cup C_5| = |C_2| + |C_5| - |C_{10}| = 50 + 20 - 10 = 60.$$

En general, és a dir, si hem de calcular el cardinal de la unió de n conjunts, tenim el següent enunciat:

Teorema 1.4.1 *(Principi d'inclusió-exclusió)*
Siga X un conjunt i siguen $A_1, A_2, \ldots, A_n$ subconjunts. Llavors

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{I \in \mathcal{P}(\{1,2,\ldots,n\}) - \{\emptyset\}} (-1)^{|I|-1} \left|\bigcap_{i \in I} A_i\right|. \tag{1.2}$$

Demostració. Farem una demostració per inducció sobre n.
Per a $n = 1$, el que tenim d'una banda és

$$\left|\bigcup_{i=1}^{n} A_i\right| = |A_1|$$

i d'altra banda

$$\sum_{I\in\mathcal{P}(\{1\})-\{\emptyset\}} (-1)^{|I|-1} \,|\bigcap_{i\in I} A_i| = (-1)^{1-1} \,|\bigcap_{i\in\{1\}} A_i| = |A_1|.$$

És necessari provar-la per a $n = 2$. En aquest cas el teorema diu que:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

La unió $A_1 \cup A_2$ es pot posar com la unió disjunta

$$A_1 \cup A_2 = (A_1\backslash A_2) \cup (A_2\backslash A_1) \cup (A_1 \cap A_2).$$

Com que $|A_1\backslash A_2| = |A_1| - |A_1 \cap A_2|$ i $|A_2\backslash A_1| = |A_2| - |A_2 \cap A_1|$. Aleshores, fent servir ara el principi de la suma, s'obté l'expressió de l'enunciat.

Suposarem ara que l'equació (1.2) és certa per a $n = k$, es a dir:

$$|\bigcup_{i=1}^{k} A_i| = \sum_{I\in\mathcal{P}(\{1,2,\ldots,k\})-\{\emptyset\}} (-1)^{|I|-1} \,|\bigcap_{i\in I} A_i|.$$

Anem a provar-la per a $n = k + 1$. Mireu primer que

$$|\bigcup_{i=1}^{k+1} A_i| = |(\bigcup_{i=1}^{k} A_i) \cup A_{k+1}| = |\bigcup_{i=1}^{k} A_i| + |A_{k+1}| - |(\bigcup_{i=1}^{k} A_i) \cap A_{k+1}| \tag{1.3}$$

on s'ha fet servir la hipòtesi d'inducció per al cas $n = 2$. Per això era necessàri provar també el cas $n = 2$.

Ara, el que farem es descomposar el conjunt $\mathcal{P}(\{1, 2, \ldots, k, k + 1\})$ en tres subconjunts disjunts:

$$\begin{aligned} S_1 &= \mathcal{P}(\{1, 2, \ldots, k\}) \\ S_2 &= \{\{k + 1\}\} \\ S_3 &= \{X \cup \{k + 1\} : X \in \mathcal{P}(\{1, 2, \ldots, k\}) - \{\emptyset\}\}. \end{aligned}$$

Recordeu que volem que l'expressió

$$\sum_{I\in\mathcal{P}(\{1,2,\ldots,k+1\})-\{\emptyset\}} (-1)^{|I|-1} \,|\bigcap_{i\in I} A_i|$$

coincidisca amb l'expressió de l'equació (1.3).

Per a fer-ho veurem que si separem els índexs I segons estiguen en S_1, S_2 o S_3 obtindrem els tres termes de l'equació (1.3).

$$\sum_{I\in\mathcal{P}(\{1,2,\ldots,k+1\})-\{\emptyset\}} (-1)^{|I|-1}\,|\bigcap_{i\in I} A_i| =$$

$$\sum_{I\in S_1-\{\emptyset\}} (-1)^{|I|-1}\,|\bigcap_{i\in I} A_i| + \sum_{I\in S_2} (-1)^{|I|-1}\,|\bigcap_{i\in I} A_i| + \sum_{I\in S_3} (-1)^{|I|-1}\,|\bigcap_{i\in I} A_i|.$$

La primera suma és, per hipòtesi d'inducció, $\left|\bigcup_{i=1}^{k} A_i\right|$, la segona suma és simplement $|A_{k+1}|$. Vegem la tercera suma. Si $I \in S_3$ aleshores $I = \{j_1, j_2, \ldots, j_s, k+1\}$ amb $\{j_1, j_2, \ldots, j_s\} \subset \{1, 2, \ldots, k\}$ i no buit. Llavors

$$\begin{aligned}(-1)^{|I|-1}\,|\bigcap_{i\in I} A_i| &= (-1)^{s+1-1}\,|A_{j_1}\cap A_{j_2}\cap\ldots\cap A_{j_s}\cap A_{k+1}| \\ &= (-1)^{s}\,|(A_{j_1}\cap A_{k+1})\cap(A_{j_2}\cap A_{k+1})\cap\ldots\cap(A_{j_s}\cap A_{k+1})|\end{aligned}$$

Quan I varia sobre S_3, hem d'avaluar totes les possibilitats de conjunts $\{j_1, j_2, \ldots, j_s\} \subset \{1, 2, \ldots, k\}$ no buits, i això ens permet d'escriure la tercera suma així:

$$\begin{aligned}\sum_{I\in S_3} (-1)^{|I|-1}\,|\bigcap_{i\in I} A_i| &= \sum_{I\in\mathcal{P}(\{1,2,\ldots,k\})-\{\emptyset\}} (-1)^{|I|}|\bigcap_{i\in I}(A_i\cap A_{k+1})| \\ &= -\sum_{I\in\mathcal{P}(\{1,2,\ldots,k\})-\{\emptyset\}} (-1)^{|I|-1}|\bigcap_{i\in I}(A_i\cap A_{k+1}| \\ &= -|\bigcup_{i=1}^{k-1}(A_i\cap A_{k+1})|\end{aligned}$$

En l'últim pas hem fet servir la hipòtesi d'inducció. Finalment, noteu que

$$\bigcup_{i=1}^{k-1}(A_i\cap A_{k+1}) = \left(\bigcup_{i=1}^{k-1} A_i\right)\cap A_{k+1}.$$

□

Tornem a l'exemple introductori d'aquesta secció. En realitat, nosaltres necessitem aplicar el principi d'inclusió-exclusió als complementaris: Si X és un conjunt i si $C_1, C_2, \ldots, C_k$ són subconjunts, aleshores:

$$\begin{aligned}|(X-C_1)\cap(X-C_2)\cap\cdots\cap(X-C_k)| &= |X-(C_1\cup C_2\cup\cdots\cup C_k)| \\ &= |X| - \sum_{1\le i\le k}|C_i| + \sum_{1\le i<j\le k}|C_i\cap C_j| - \\ &\quad - \sum_{1\le i<j<\ell\le k}|C_i\cap C_j\cap C_\ell| + \cdots + \\ &\quad +(-1)^k|C_1\cap C_2\cap\cdots\cap C_k|.\end{aligned}$$

Les notacions alternatives que hem recordat abans per al complementari i per a la intersecció permeten escriure aquesta fórmula d'una manera més condensada:

$$\begin{aligned}|\overline{C_1}\overline{C_2}\dots\overline{C_k}| &= |X| - \sum_{1\le i\le k}|C_i| + \sum_{1\le i<j\le k}|C_iC_j| - \\ &\quad - \sum_{1\le i<j<\ell\le k}|C_iC_jC_\ell| + \cdots + (-1)^k|C_1C_2\dots C_k|.\end{aligned}$$

Apliquem aquest principi per a calcular la quantitat de nombres naturals majors que zero i menors o iguals que 100 que no són divisibles ni per 2, ni per 3, ni per 5:

$$\begin{aligned}&|(X-C_2)\cap(X-C_3)\cap(X-C_5)|\\ &= |X| - |C_2| - |C_3| - |C_5| + |C_2\cap C_3| + |C_2\cap C_5| + |C_3\cap C_5| - |C_2\cap C_3\cap C_5|\\ &= |X| - |C_2| - |C_3| - |C_5| + |C_6| + |C_{10}| + |C_{15}| - |C_{30}|\\ &= 100 - 50 - 33 - 20 + 16 + 10 + 6 - 3 = 26.\end{aligned}$$

1.5 Aplicacions

1.5.1 *Comptant monomis*

Siguen x, y, z tres indeterminades, anomenem *monomi de grau* d a una expressió del tipus $x^a y^b z^c$ amb $a+b+c=d$. Anem a estudiar el següent problema: determinar el nombre de monomis diferents de grau 10 en aquestes tres indeterminades.
Observem que un monomi de grau 10 és per exemple x^8yz que podria també escriure's com a x^7yxz, o de qualsevol altra manera possible, resultat de reordenar les variables. Això mostra que l'ordre de les seleccions no és rellevant.
Com que podem reordenar les variables, podem suposar que cada monomi de grau 10 està escrit com en la definició:

$$x^a y^b z^c \quad \text{amb} \quad a+b+c=10.$$

Per tant és el nombre de seleccions no ordenades de 10 elements en un conjunt de 3 elements. La resposta és: $CR(3,10) = \binom{3+10-1}{10} = \binom{12}{10} = 66$.

Una manera equivalent d'enunciar el problema, posant el punt de vista en els exponents, és preguntar quantes solucions naturals té l'equació

$$x_1 + x_2 + x_3 = 10.$$

Recordeu que aquests monomis apareixien en la Fórmula de Leibniz (v. Eq. (1.1). Allà el problema era trobar el coeficient d'un monomi concret en el desenvolupament. Dit d'una altra manera, quantes vegades apareixia un monomi concret en el desenvolupament. El problema ací és és un altre. El problema ara és comptar quants termes té el sumatori que apareix en la Fórmula de Leibniz.

Doncs bé, ara complicarem un poc més la pregunta. D'aquestes solucions, quantes verifiquen que $x_1 \leq 4, x_2 \leq 4, x_3 \leq 4$?
Aplicarem el principi d'inclusió-exclusió per respondre a la pregunta. El conjunt total, X, és el conjunt de totes les solucions naturals de l'equació $x_1 + x_2 + x_3 = 10$. Per tant, $|X| = 66$.
Per a $i = 1, 2, 3$, definim

$$C_i = \{\text{solucions amb } \ x_i > 4\} = \{\text{solucions amb } \ x_i \geq 5\}.$$

Una manera directa de calcular el cardinal de C_1 és adonar-se que si tenim una solució de l'equació $x_1 + x_2 + x_3 = 10$ amb $x_1 \geq 5$, aleshores, si restem 5 unitats a x_1, també tenim una solució de l'equació $x_1 + x_2 + x_3 = 5$, ara ja sense restriccions. Com ja sabem,

$$|\{\text{solucions naturals de } x_1 + x_2 + x_3 = 5\}| = \binom{3+5-1}{5} = \binom{7}{5} = \binom{7}{2} = 21.$$

Continuem amb l'aplicació del principi d'inclusió-exclusió. Ara toca calcular el cardinal d'interseccions de la forma $C_1 \cap C_2$. Noteu, però, que

$$C_1 \cap C_2 = \{\text{solucions de } x_1 + x_2 + x_3 = 10, \text{ amb } x_1 \geq 5, \text{ i } x_2 \geq 5\} = \{\text{solucions de } x_1 + x_2 + x_3 = 0\}.$$

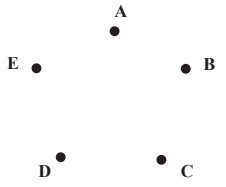
L'única solució és la trivial, per tant, $|C_1 \cap C_2| = 1$.
Finalment, $C_1 \cap C_2 \cap C_3 = \emptyset$. Ja podem escriure la fórmula del principi d'inclusió-exclusió per al nostre cas:

$$\begin{aligned} &|(X - C_1) \cap (X - C_2) \cap (X - C_3)| \\ &= |X| - |C_1| - |C_2| - |C_3| + |C_1 \cap C_2| + |C_1 \cap C_3| + |C_2 \cap C_3| - |C_1 \cap C_2 \cap C_3| \\ &= 66 - 3 \cdot 21 + 3 \cdot 1 = 6. \end{aligned}$$

1.5.2 *Comptant carreteres*

Veurem ara altre exemple d'aplicació del principi d'inclusió-exclusió. Suposem que volem unir amb carreteres cinc poblacions, A, B, C, D i E. La pregunta és:

Quants conjunts de carreteres distints es poden construir que unisquen totes les poblacions?

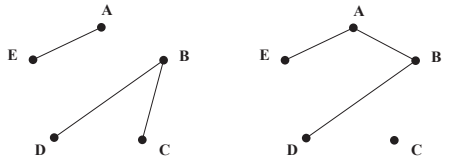


Esquema que representa les cinc poblacions.

Cada carretera està determinada per les dues poblacions que connecta. Així, una carretera és un subconjunt de dos elements del conjunt $\{A, B, C, D, E\}$. El nombre de carreteres possibles és el mateix que el nombre de subconjunts de dos elements, $\binom{5}{2} = 10$. El conjunt de totes les carreteres és

$$X = \{AB, AC, AD, AE, BC, BD, BE, CD, CE, DE\}.$$

Una xarxa viària és un subconjunt del conjunt de carreteres. Per tant, la quantitat de xarxes viàries distintes és la quantitat de subconjunts del conjunt de carreteres, $2^{10} = 1024$.



Dos conjunts diferents de carreteres. A l'esquerra, $\{AE, BC, BD\}$. A la dreta, $\{AE, AB, BD\}$.

Volem també que cap de les poblacions quede aïllada. Noteu que en les dues figures anteriors, hi ha una configuració de les carreteres, la de la dreta, que no verifica la condició addicional. L'altra, la de l'esquerra, encara que no es deixa cap població aïllada, i per tant, és una de les que volem comptar, salta a la vista que té un "defecte". Ja parlarem d'aquest cas més endavant. La pregunta, per tant, és ara:

De les 1024 possibles xarxes viàries, quantes no deixen cap d'elles aïllada?

Per a poder aplicar el principi d'inclusió-exclusió hem de definir els subconjunts adients. El conjunt de carreteres que no deixen aïllada cap població és la intersecció del conjunt de carreteres que no deixen aïllada la població A amb el conjunt de carreteres que no deixen aïllada la població B amb ... el conjunt de carreteres que no deixen aïllada la població E. Per tant, sembla clar que hem de definir C_A com el conjunt de carreteres que deixen aïllada la població A i anàlogament amb les altres poblacions. El que hem de calcular és

$$|(X - C_A) \cap (X - C_B) \cap (X - C_C) \cap (X - C_D) \cap (X - C_E)| = |X - (C_1 \cup C_B \cup C_C \cup C_D \cup C_E)\,|.$$

Haurem de calcular prèviament els cardinals d'alguns subconjunts. El primer de tots és el de C_A. Ara bé, C_A no és altra cosa que el conjunt de carreteres que es poden construir entre les quatre poblacions B, C, D i E. Per tant,

$$|C_A| = 2^{\binom{4}{2}} = 2^6 = 64.$$

El segon cardinal és el de $C_A \cap C_B$. Ara bé, $C_A \cap C_B$ no és altra cosa que el conjunt de carreteres que es poden construir entre les tres poblacions C, D i E. Per tant,

$$|C_A \cap C_B| = 2^{\binom{3}{2}} = 2^3 = 8.$$

Anàlogament,

$$|C_A \cap C_B \cap C_C| = 2^{\binom{2}{2}} = 2^1 = 2.$$

A partir d'ací, la cosa canvia ja que, per exemple, $C_A \cap C_B \cap C_C \cap C_D$ és la família formada per un únic conjunt, el conjunt buit.

$$C_A \cap C_B \cap C_C \cap C_D = \{\emptyset\}.$$

Ja que només queda disponible la població E i per a construir una carretera calen almenys dos punts. Anàlogament per a la darrera intersecció. Per tant,

$$|C_A \cap C_B \cap C_C \cap C_D| = |C_A \cap C_B \cap C_C \cap C_D \cap C_E| = 1.$$

Ara ja podem calcular el que volíem

$$\begin{aligned} & |(X - C_A) \cap (X - C_B) \cap (X - C_C) \cap (X - C_D) \cap (X - C_E)| = \\ = \; & |X - (C_1 \cup C_B \cup C_C \cup C_D \cup C_E)\,| \\ = \; & |X| - 5 \cdot |C_A| + \binom{5}{2}|C_A \cap C_B| - \binom{5}{3}|C_A \cap C_B \cap C_C| + \\ & + \binom{5}{4}|C_A \cap C_B \cap C_C \cap C_D| - |C_A \cap C_B \cap C_C \cap C_D \cap C_E| \\ = \; & 1024 - 5 \cdot 64 + 10 \cdot 8 - 10 \cdot 2 + 5 \cdot 1 - 1 = 768. \end{aligned}$$

Ara que ja hem calculat el nombre de carreteres que no deixen cap població aïllada, recordem que entre eixes 768 hi ha algunes del tipus de la figura anterior, esquerra. Aquestes són carreteres que es diuen disconnexes, perquè les dues poblacions, A i E, estan disconnetades de les altres 3. Un problema adicional consisteix en saber quantes carreteres connexes (amb cinc ciutats) hi ha? Farem el compte mitjançant el següent raonament:

• Per a deixar dues parts inconnexes sense aïllar punts és necessari i suficient dividir les cinc poblacions en un subconjunt de dos elements i un altre de 3 elements.

• El subconjunt de dos elements queda unit mitjançant una carretera, mentre que el nombre de xarxes viàries entre tres poblacions que no deixen poblacions incomunicades és 4.

Per tant les disposicions que deixen les cinc poblacions en parts disconnexes sense deixar punts aïllats té un cardinal de $4\binom{5}{3} = 40$, així doncs les "bones xarxes viàries" que no deixen punts aïllats ni components disconnexes són $768 - 40 = 728$.

En general, per a un nombre n qualsevol de poblacions és difícil el càlcul de les xarxes viàries que no deixen cap component aïllada ni punts aïllats. Aquesta disposició té un nom propi, es diu **graf connex** i ho estudiarem més endavant. Sabem que aquest nombre és menor estrictament que

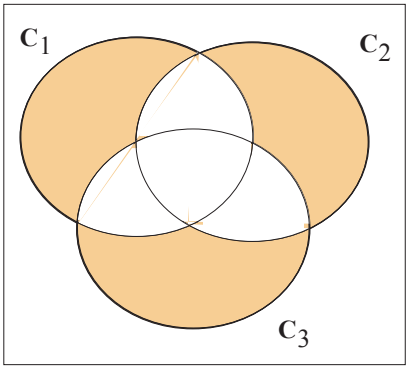
$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} 2^{\binom{n-k}{2}}$$

que és el nombre de xarxes viàries que no deixen punts aïllats.

1.6 Variacions sobre el principi d'inclusió-exclusió

En aplicar el principi d'inclusió-exclusió, hem pogut comptar els elements d'un conjunt que no verificaven cap d'una llista de propietats. De vegades, però, estarem interessats a comptar els elements d'un conjunt que verifiquen una, i només una, de les propietats de la llista. Per exemple,

Quina és la quantitat de nombres naturals majors que zero i menors o iguals que 100 que són divisibles per un, i només per un, dels factors 2, 3 o 5?



Representació gràfica del subconjunt format pels elements que verifiquen una, i només una, de les propietats C_1, C_2 o C_3.

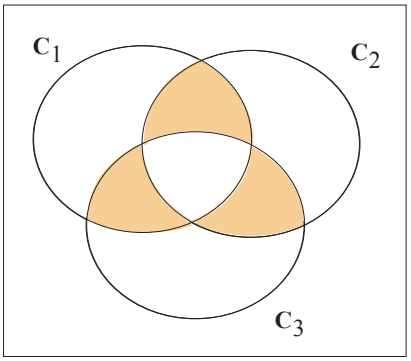
Doncs bé, en el cas de treballar amb tres subconjunts C_1, C_2 i C_3 aleshores, el cardinal del subconjunt dels elements que estan en un, i només en un, dels tres subconjunts és igual a:

$$|C_1| + |C_2| + |C_3| - 2|C_1 \cap C_2| - 2|C_1 \cap C_3| - 2|C_2 \cap C_3| + 3|C_1 \cap C_2 \cap C_3|.$$

Així, per exemple, per calcular la quantitat de nombres naturals majors que zero i menors o iguals que 100 que són divisibles per un, i només per un, dels factors 2, 3 o 5 tindrem que el resultat és

$$50 + 33 + 20 - 2 \cdot 10 - 2 \cdot 6 - 2 \cdot 16 + 3 \cdot 3 = 48.$$

Quina seria ara la fórmula si volguèrem trobar el cardinal del subconjunt dels elements que estan en dos, i només en dos, dels tres subconjunts?

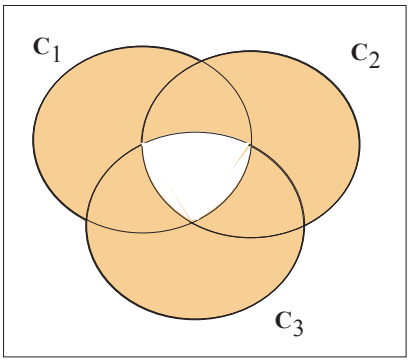


Representació gràfica del subconjunt format pels elements que verifiquen dues,
i només dues, de les propietats C_1, C_2 o C_3.

Doncs bé, la fórmula seria ara la següent:

$$|C_1 \cap C_2| + |C_1 \cap C_3| + |C_2 \cap C_3| - 3|C_1 \cap C_2 \cap C_3|.$$

Quina seria ara la fórmula si volguèrem trobar el cardinal del subconjunt dels elements que estan en, com a molt, dos dels tres subconjunts?



Representació gràfica del subconjunt format pels elements que estan en, com a molt,
dos dels tres subconjunts C_1, C_2 o C_3.

Doncs bé, la fórmula seria ara la següent:

$$|C_1| + |C_2| + |C_3| - |C_1 \cap C_2| - |C_1 \cap C_3| - |C_2 \cap C_3|.$$

Noteu que, gràcies al principi d'inclusió-exclusió, el resultat és el mateix que

$$|C_1 \cup C_2 \cup C_3| - |C_1 \cap C_2 \cap C_3|.$$

1.7 Funcions generatrius

1.7.1 *Nombres binomials generalitzats*

Recordem la relació que hi ha entre els nombres combinatoris i la quantitat de subconjunts d'un determinat cardinal. Per exemple, el coeficient de x^7 en $(1+x)^{20}$ és $\binom{20}{7}$, que és la quantitat de subconjunts de 7 elements que té un conjunt de 20 elements. Aquest era el cas 4, de combinacions ordinàries, dels problemes estudiats al principi. També han aparegut els nombres binomials en un altre dels problemes, concretament en el cas 5, combinacions amb repetició.
El que veurem en aquesta secció és, primer, com els coeficients d'aquesta mena de desenvolupaments són útils per resoldre alguns dels problemes que ja hem vist i, segon, com resoldre alguns de nous i de més complicats. Caldrà primer generalitzar la definició de nombre binomial.

La definició inicial del nombre binomial $\binom{n}{k}$,

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

exigeix que n i k siguen nombres naturals i que $k \leq n$. Ara bé, si simplifiquem factors presents en el numerador i el denominador, tenim que

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!},$$

i aixípodem definir també els nombres combinatoris quan $n \in \mathbb{Z}$ de la següent manera:

Definició 1.7.1 *Donat $n \in \mathbb{Z}$ i $k \in \mathbb{N}$, definim*

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!}.$$

Per exemple,

$$\binom{-3}{2} = \frac{(-3)(-4)}{2!} = \frac{12}{2} = 6,$$

$$\binom{-5}{3} = \frac{(-5)(-6)(-7)}{3!} = \frac{-6\cdot 35}{6} = -35.$$

Els nombres combinatoris que acabem de definir amb n negatiu es poden reduir als usuals:

Proposició 1.7.2 *Si $n, k \in \mathbb{N}$, aleshores*

$$\boxed{\binom{-n}{k} = (-1)^k \binom{n+k-1}{k}.}$$

Demostració.

$$\begin{aligned}
\binom{-n}{k} &= \tfrac{(-n)(-n-1)\ldots(-n-k+2)(-n-k+1)}{k!} \\
&= (-1)^k\ \tfrac{n(n+1)\ldots(n+k-2)(n+k-1)}{k!} \\
&= (-1)^k\ \tfrac{(n+k-1)(n+k-2)\ldots(n+1)n}{k!} \\
&= (-1)^k\ \tfrac{(n+k-1)(n+k-2)\ldots(n+1)n\ (n-1)\ldots\ 2\ 1}{k!\ (n-1)\ldots\ 2\ 1} \\
&= (-1)^k\ \tfrac{(n+k-1)!}{k!\ (n-1)!} \\
&= (-1)^k\ \tfrac{(n+k-1)!}{k!\ (n+k-1-k)!} \\
&= (-1)^k\ \tbinom{n+k-1}{k}.
\end{aligned}$$

□

Recordeu que el nombre combinatori $\binom{n+k-1}{k}$ era el que apereixia en el cas 5. Així, podem "unir" ambdós casos en un únic formalisme. Recordeu que l'única diferència entre ambdós casos era que en el cas 4, de combinacions ordinàries, no permetíem repeticions en la tria, i que en el cas 5, de combinacions amb repetició, síque en permetíem.
En el cas 4, la resposta és el nombre combinatori $\binom{n}{r}$, mentre que en el cas 5, la resposta és, tret del signe, el nombre combinatori $\binom{-n}{r}$. La diferència, per tant, de fer una tria amb repeticions (cas 5) o sense (cas 4) és posar o no un signe en el nombre binomial.

1.7.2 *Desenvolupaments de Taylor*

La noció de polinomis de Taylor associats a una funció derivable s'introdueix en l'assignatura Anàlisi matemàtica I. És possible que encara no s'haja parlat de polinomis de Taylor en aquest punt del curs, però del que sí que s'ha parlat, perquè és de primer quadrimestre, és de sèries, en particular de les sèries geomètriques. Així és gairebé l'únic que ens caldrà saber.
Donada una funció que suposarem infinitament derivable en un entorn de $0 \in \mathbb{R}$, l'anàlisi matemàtica ens instrueix que en un entorn de 0 aquesta funció és "igual" al seu desenvolupament de Taylor:

$$f(x) = \sum_{j=0}^{\infty} \frac{f^{(j)}(0)}{j!}\, x^j = f(0) + \frac{f'(0)}{1!}\, x + \frac{f''(0)}{2!}\, x^2 + \frac{f^{(3)}(0)}{3!}\, x^3 + \cdots + \frac{f^{(n)}(0)}{n!}\, x^n + \cdots$$

Estrictament parlant, caldria dir que la funció convergeix cap al seu desenvolupament de Taylor. Nosaltres no ens preocuparem de les qüestions de convergència, que sabem que es donen en un entorn determinat. Només ens ocuparem de veure formalment els desenvolupaments de les funcions que siguen útils a l'hora de fer comptes.
La fórmula del binomi de Newton aplicada a $(1+x)^n$ es pot entendre com el desenvolupament de Taylor de la funció $f(x) = (1+x)^n$ en el punt $x_0 = 0$. En efecte, si $k \in \{0, 1, 2, \ldots, n\}$,

$$f^{(k)}(0) = n(n-1)\ldots(n-k+1).$$

Les derivades superiors són totes nul·les. Així,

$$f(0) + \frac{f'(0)}{1!}\, x + \frac{f''(0)}{2!}\, x^2 + \frac{f^{(3)}(0)}{3!}\, x^3 + \cdots + \frac{f^{(n)}(0)}{n!}\, x^n$$

és igual que

$$1+\frac{n}{1!}\,x+\frac{n(n-1)}{2!}\,x^2+\frac{n(n-1)(n-2)}{3!}\,x^3+\cdots+\frac{n!}{n!}\,x^n$$

equivalentment

$$\binom{n}{0}+\binom{n}{1}\,x+\binom{n}{2}\,x^2+\binom{n}{3}\,x^3+\cdots+\binom{n}{n}\,x^n.$$

Amb això comprovem que el nombres combinatoris $\binom{n}{k}$, amb $n\in\mathbb{N}$, estan relacionats amb el desenvolupament en sèrie de Taylor de la funció $(1+x)^n$. La qüestió ara és saber si passa el mateix quan $n\in\mathbb{Z}$ (quan n és negatiu).

Estaran també relacionats els nombre binomials $\binom{-n}{k}$ (n positiu) amb el desenvolupament en sèrie de Taylor de la funció $(1+x)^{-n}$?

Tal com ja hem dit, i segurament veureu al llarg d'aquest quadrimestre, en l'assignatura Anàlisi matemàtica I, que el desenvolupament de la funció $(1-x)^{-1}=\dfrac{1}{1-x}$ en $x_0=0$ és

$$\frac{1}{1-x}=1+x+x^2+x^3+\cdots\,.$$

En realitat, aquesta expressió també es pot deduir sense fer servir desenvolupaments de Taylor. La podem deduir alternativament si recordem les progressions geomètriques.
En efecte, la suma de

$$1+x+x^2+x^3+\cdots+x^n=\frac{1-x^{n+1}}{1-x}.$$

Si suposem ara que $|x|<1$ i calculem el límit quan n tendeix a infinit,

$$1+x+x^2+x^3+\cdots=\lim_{n\to\infty}\frac{1-x^{n+1}}{1-x}=\frac{1}{1-x}.$$

Val a dir que les sèries amb què treballarem les considerarem sèries formals, i no ens preocuparem de la seua convergència, encara que sempre es pot demostrar que són convergents en algun interval.

Una tercera "demostració", i mireu que la paraula *demostració* l'hem escrita entre cometes, és la següent:

$$\begin{aligned}(1-x)(1+x+x^2+x^3+\dots) &= 1+x+x^2+x^3+\dots\\ &\quad -x-x^2-x^3-x^4\dots\\ &= 1.\end{aligned}$$

A partir del desenvolupament de $\dfrac{1}{1-x}$ se'n poden deduir molts altres. Per exemple, si canviem x per $-x$, tenim que

$$(1+x)^{-1}=1-x+x^2-x^3+\cdots$$

Si ara derivem ambdós membres, tenim que

$$-(1+x)^{-2} = -1 + 2x - 3x^2 + 4x^3 - \cdots$$

equivalentment

$$(1+x)^{-2} = 1 - 2x + 3x^2 - 4x^3 + \cdots$$

Si substituïm x per x^2 en $(1+x)^{-1}$, tenim que el desenvolupament de $(1+x^2)^{-1}$ és

$$(1+x^2)^{-1} = 1 - x^2 + x^4 - x^6 + \cdots$$

Definició 1.7.3 *Una funció infinitament derivable en el* 0 *es diu que és una funció generatriu d'una successió* $\{a_n\}_{n\geq 0}$ *si*

$$\frac{f^{(n)}(0)}{n!} = a_n$$

per a tot $n \geq 0$.

Les successions de coeficients de tots aquests desenvolupaments de Taylor determinen unívocament les funcions corresponents, i viceversa. Per això, les funcions s'anomenen funcions generatrius de les successions corresponents i viceversa, les successions s'anomenen successions generatrius de les funcions corresponents. Així, la successió

$$1, 1, 1, 1, \ldots$$

és successió generatriu de $(1-x)^{-1}$, la successió

$$1, -1, 1, -1, \ldots$$

és successió generatriu de $(1+x)^{-1}$, la successió

$$1, -2, 3, -4, \ldots$$

és successió generatriu de $(1+x)^{-2}$, la successió

$$1, 2, 3, 4, \ldots$$

és successió generatriu de $(1-x)^{-2}$, la successió

$$1, 0, -1, 0, 1, 0, -1, \ldots$$

és successió generatriu de $(1+x^2)^{-1}$.
D'una altra banda, la successió generatriu de, per exemple, $(1+x)^7$, és

$$\binom{7}{0}, \binom{7}{1}, \binom{7}{2}, \binom{7}{3}, \binom{7}{4}, \binom{7}{5}, \binom{7}{6}, \binom{7}{7}, 0, 0, 0 \ldots$$

Tornem ara a la pregunta del principi:

Quin és el desenvolupament en sèrie de Taylor de la funció $(1+x)^{-n}$ *en el punt* $x_0 = 0$*?*

Proposició 1.7.4 *La funció $(1+x)^{-n}$ és la funció generatriu de la successió de terme general*

$$a_i = \binom{-n}{i}, \qquad \forall i \in \mathbb{N}.$$

Demostració. Noteu primer que per a tot $i \in \mathbb{N}$,

$$f^{(i)}(x) = (-n)(-n-1)\dots(-n-i+1)(1+x)^{-n-i}.$$

Així, el coeficient de x^i en el desenvolupament en sèrie de Taylor de la funció $(1+x)^{-n}$ en el punt $x_0 = 0$ és

$$\frac{f^{(i)}(0)}{i!} = \binom{-n}{i}.$$

□

Quina relació té tot això amb els problemes de recompte?

Quin és el coeficient de x^{10} en $(1+x)^{-20}$? La resposta és simplement

$$\binom{-20}{10} = (-1)^{10}\binom{20+10-1}{10} = \binom{29}{10}.$$

Quin és el coeficient de x^{10} en $(x^2+x^3+x^4+x^5)^4$? En aquest cas, és millor considerar la funció $(x^2+x^3+x^4+\dots)^4$ perquè això podem aplicar els resultats anteriors sobre successions generatrius i perquè el coeficient de x^{10} en ambdues funcions és el mateix.
Cal primer una certa manipulació:

$$\begin{aligned}(x^2+x^3+x^4+\dots)^4 &= (x^2)^4(1+x+x^2+\dots)^4\\ &= x^8((1-x)^{-1})^4\\ &= x^8(1-x)^{-4}\end{aligned}$$

Per tant, el que hem de calcular és el coeficient de $x^{10-8} = x^2$ en $(1-x)^{-4}$ i la resposta és simplement

$$\binom{-4}{2} = (-1)^2\binom{4+2-1}{2} = \binom{5}{2} = 10.$$

Per tant, el coeficient de x^{10} en $(x^2+x^3+x^4+x^5)^4$ és 10.

Tornem al problema de la gelateria. Suposem ara que 10 persones han de triar gelats entre 4 sabors diferents. La pregunta era determinar quantes possibles eleccions podien fer. Doncs bé, si associem a cada sabor el factor

$$1+x+x^2+x^3+\cdots$$

aleshores la resposta la dóna el coeficient de x^{10} (l'exponent correspon al nombre de persones) en el producte

$$(1+x+x^2+x^3+\cdots)(1+x+x^2+x^3+\cdots)(1+x+x^2+x^3+\cdots)(1+x+x^2+x^3+\cdots).$$

Observeu que quan multipliqueu aquests 4 factors apareixeran monomis de la forma

$$x^a\ x^b\ x^c\ x^d$$

on cada factor x^k prové del factor $(1+x+x^2+x^3+\cdots)$ corresponent. Cada monomi es pot interpretar com una de les possibles eleccions en què hi ha a persones que trien el primer sabor, b que trien el segon, c que trien el tercer i d que trien el quart. Com que hi ha 10 persones, aleshores $x^a\ x^b\ x^c\ x^d = x^{10}$. Cada elecció dóna lloc a un x^{10} i, així, el coeficient total de x^{10} és la quantitat total de possibles eleccions.
El coeficient de x^{10} en $(1+x+x^2+x^3+\cdots)^4$ és el terme a_{10} en la successió generatriu de $(1-x)^{-4}$, i aquest terme és

$$a_{10} = \binom{-4}{10}(-1)^{10} = (-1)^{10}\binom{4+10-1}{10} = \binom{13}{10} = \binom{13}{3} = 13\cdot 2\cdot 11 = 286.$$

Ara, amb aquesta tècnica, podem calcular més coses. Per exemple, suposem una altra vegada que 10 persones han de triar gelats entre 4 sabors diferents. Ara, però, sabem que cada sabor és demanat per un nombre parell de persones. La pregunta és la mateixa: Quantes possibles eleccions hi ha?
Noteu que el problema és equivalent al de trobar la quantitat de solucions de l'equació

$$x_1+x_2+x_3+x_4 = 10$$

amb les condicions, $x_k \in \mathbb{N}$ i parell, per a tot $k \in \{1,2,3,4\}$.
Per tal de considerar només les solucions parelles només cal substituir x per x^2 en el raonament anterior. Hem de trobar el coeficient de x^{10} en

$$(1+x^2+x^4+\cdots)^4 = \left(\frac{1}{1-x^2}\right)^4 = (1-x^2)^{-4} = \sum_{k=0}^{\infty}(-1)^k\binom{-4}{k}\,x^{2k}.$$

El coeficient és

$$(-1)^5\binom{-4}{5} = \binom{4+5-1}{5} = \binom{8}{3} = 8\cdot 7 = 56.$$

1.7.3 *Un últim exemple*

Quantes solucions naturals té l'equació $a+2b+c=9$?

Hi ha tantes solucions com indica el coeficient de x^9 en el producte

$$(1+x+x^2+x^3+\cdots+x^9)(1+x^2+x^4\cdots+x^8)(1+x+x^2+x^3+\cdots+x^9).$$

Aquest coeficient es pot calcular de diverses maneres. La més directa és la següent: Hem de calcular el

coeficient de x^9 en el producte

$$\begin{aligned}
(1-x^2)^{-1}(1-x)^{-2} &= \left(\tfrac{1-x^2}{1-x}\right)^2 \tfrac{1}{(1-x^2)^3} \\
&= (1+x)^2 \tfrac{1}{(1-x^2)^3} \\
&= \left(1+2x+x^2\right) \tfrac{1}{(1-x^2)^3} \\
&= \left(1+2x+x^2\right)(1-x^2)^{-3} \\
&= \left(1+2x+x^2\right)\left(\tbinom{-3}{0}(-x^2)^0 + \tbinom{-3}{1}(-x^2)^1 + \tbinom{-3}{2}(-x^2)^2 + \right. \\
&\quad \left. + \tbinom{-3}{3}(-x^2)^3 + \tbinom{-3}{4}(-x^2)^4 + \tbinom{-3}{5}(-x^2)^5 + \dots\right) \\
&= \left(1+2x+x^2\right)\left(\tbinom{-3}{0} - \tbinom{-3}{1}x^2 + \tbinom{-3}{2}x^4 - \tbinom{-3}{3}x^6 + \tbinom{-3}{4}x^8 - \tbinom{-3}{5}x^{10} + \cdots\right).
\end{aligned}$$

L'única manera d'obtenir un x^9 en el producte anterior és quan es multiplica el terme $2x$ del primer producte pel terme $\binom{-3}{4}x^8$ del segon. Per tant, el coefficient que busquem és $2 \cdot \binom{-3}{4} = 30$.

Nota 1.2 *En aquestes últimes pàgines hem vist com calcular quantes solucions naturals té una equació de la forma $ax + by = c$, amb $a, b, c \in \mathbb{N}$, o equacions més complicades. Per calcular també quines són les seues solucions, haurem d'esperar al darrer tema on estudiarem, en la secció 4.4, el que s'anomenen equacions diofàntiques lineals i com calcular-ne les solucions.*

1.8 Annex: Resum de tècniques combinatòries

Abans de passar als exercicis recordem sobre tot el principi del tema.

Variacions amb repetició
El nombre de *variacions amb repetició* de n elements agafats de k en k és

$$VR(n,k) = n^k.$$

Aquest nombre és el mateix que:

- El nombre d'aplicacions de $\mathbb{N}_k$ en $\mathbb{N}_n$, o en general, el nombre d'aplicacions $f : X \to Y$ entre un conjunt, X, amb cardinal k i un altre, Y, amb cardinal n.
- El nombre de paraules de k lletres en un alfabet de n lletres.
- El nombre de seleccions ordenades de k elements (admetent-hi repeticions) d'un conjunt de n elements.

Variacions ordinàries

El nombre de *variacions* de n elements agafats de k en k és

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

Aquest nombre és el mateix que:

- El nombre d'aplicacions injectives de $\mathbb{N}_k$ en $\mathbb{N}_n$, o en general, el nombre d'aplicacions injectives $f : X \to Y$ entre un conjunt, X, amb cardinal k i un altre, Y, amb cardinal n.
- El nombre de paraules de k lletres en un alfabet de n lletres que no tenen cap lletra repetida.
- El nombre de seleccions ordenades de k elements (sense repeticions) d'un conjunt de n elements.

Permutacions

El nombre de permutacions d'un conjunt de n elements és

$$P(n) = n!$$

Aquest nombre és el mateix que:

- El nombre d'aplicacions bijectives de $\mathbb{N}_n$ en $\mathbb{N}_n$, o en general, el nombre d'aplicacions bijectives $f : X \to Y$ entre dos conjunts, X i Y, amb el mateix cardinal, n.
- El nombre d'ordenacions distintes d'un conjunt de n elements.
- El nombre de variacions de n elements agafats de n en n.

Permutacions amb repetició

El nombre de *permutacions amb repetició* d'un conjunt s elements $\{a_1, a_2, \ldots, a_s\}$ en el que l'element a_i es repeteix n_i vegades, amb $n_1 + n_2 + \cdots + n_s = n$, $n_i \geq 1$, és

$$PR(n_1, n_2, \ldots, n_s) = \binom{n}{n_1, n_2, \ldots, n_s} = \frac{n!}{n_1!\, n_2!\, \ldots\, n_s!}$$

Aquest nombre és el mateix que:

- Donar una llista ordenada de longitud n on l'element a_1 es repeteix n_1 vegades, a_2 es repeteix n_2 vegades, i en general, l'element a_i es repeteix n_i vegades ($n_1 + n_2 + \cdots + n_s = n$).
- Distribuir n objectes diferents en s caixes, de manera que la caixa i-èsima reba n_i objectes.
- El nombre d'aplicacions d'un conjunt de n elements en un altre de s elements tal que aquestes aplicacions envien n_1 elements a a_1, n_2 elements a a_2,..., n_s elements a a_s.

Combinacions ordinàries
El nombre de *combinacions* d'un conjunt de n elements agafats de k en k és el nombre combinatori

$$\boxed{C(n,k) = \binom{n}{k} = \frac{n!}{k!(n-k)!}}, \qquad 0 \leq k \leq n.$$

Aquest nombre és el mateix que

- El nombre de subconjunts de k elements que podem formar a partir d'un conjunt que té n elements.
- El nombre de seleccions no ordenades de k elements que es poden fer a partir d'un conjunt de n elements.

Combinacions amb repetició
El nombre de *combinacions amb repetició* de n elements agafats de k en k és

$$CR(n,k) = \frac{(n+k-1)!}{(n-1)!\,k!} = \binom{n+k-1}{k} = \binom{n+k-1}{n-1}.$$

Aquest nombre és el mateix que

- El nombre de seleccions no ordenades (amb elements repetits) de k elements que es poden fer a partir d'un conjunt de n elements.
- El nombre de solucions enteres no negatives de l'equació

$$x_1 + x_2 + \cdots + x_n = k.$$

- El nombre de formes de distribuir k objectes idèntics en n caixes etiquetades.

1.9 Exercicis

1. Recordant el que hem dit en el cas 4, que el nombre de subconjunts de r elements d'un conjunt de n elements és el nombre binomial $\binom{n}{r}$, demostreu la coneguda fórmula recursiva sobre nombres binomials:
$$\binom{n}{r} + \binom{n}{r+1} = \binom{n+1}{r+1}.$$

2. De quantes maneres diferents poden seure sis jugadors de pòquer en una taula circular?
(Sol.: 5!.)

3. De quantes maneres diferents poden seure dotze persones en dues taules circulars de sis seients cadascuna?
   (Sol.: $\frac{1}{2}\binom{12}{6}(5!)^2$.)

4. Quantes paraules diferents es poden formar amb totes les lletres de la paraula SETRILLERES?

5. Suposem que vint persones seuen al voltant d'una taula redona. De quantes maneres diferents podem triar 3 d'aquestes persones de manera que mai dues d'elles siguen veïnes?
   (Sol.: $\binom{20}{3} - 20 \times 16 - 20 = 800$.)

6. Trobeu la quantitat d'enters de 20 dígits en els quals no hi ha dos dígits consecutius iguals.
   (Sol.: 9^{20}.)

7. Trobeu la quantitat d'enters de 20 dígits amb almenys dos dígits consecutius iguals.
   (Sol.: $9(10^{19} - 9^{19})$.)

8. Voleu enviar targetes postals a 12 amics. En el quiosc només hi ha 3 tipus de postals. De quantes maneres diferents podríeu enviar les postals si:

   (a) Hi ha prou quantitat de postals de cada classe i voleu enviar una postal a cada amic?

   (b) Hi ha prou quantitat de postals de cada classe i voleu enviar una o més postals a cada amic (però de manera que cap dels amics reba dos postals repetides)?

   (c) Només hi ha 4 postals de cada classe i voleu enviar una postal a cada amic?

   (Sol.: $3^{12}, 7^{12}, \frac{12!}{(4!)^3}$.)

9. Versió actualitzada del problema anterior. Tens al teu mòbil tres gifs "graciosets" i vols enviar-los per whatsapp a 12 amics. Pots enviar a cada amic un, dos, o els tres gifs. De quantes maneres diferents ho pots fer?
   (Sol.: 15^{12}. Noteu que ara sí que importa l'ordre d'enviament dels gifs i per tant, per a cada amic hi ha ara 15 possibilitats: $\{A, B, C, AB, BA, AC, CA, BC, CB, ABC, BCA, CAB, BAC, ACB, CBA\}$.)

10. En el sorteig de quarts de final d'una competició europea s'han d'emparellar els vuit equips que hi han arribat.

    (a) Quants possibles emparellaments hi ha?
    (Sol.: Possibles parelles hi ha $\binom{8}{2} = 28$. Per a la primera parella hi ha per tant 28 possibilitats. Ara ja només en queden 6 equips. Per a la segona parella hi ha per tant $\binom{6}{2} = 15$ possibilitats. Per a la tercera hi haurà $\binom{4}{2} = 6$ possibilitats i per a la quarta, només una. En principi hi hauria $28 \cdot 15 \cdot 6 \cdot 1 = 2520$ possibilitats. Ara bé, com que no estan ordenats, haurem de dividir per $4! = 24$. Així, els possibles resultats només són: 105.)

(b) Dels vuit equips n'hi ha tres que són del mateix estat, quina és la probabilitat de que en el resultat del sorteig no queden emparellats eixos tres equips entre ells?

(Sol.: Possibles resultats en què eixos tres equips no estiguen emparellats hi ha $5 \cdot 4 \cdot 3 = 60$. Per tant la probabilitat és $\frac{60}{105} = \frac{4}{7} = 0.571429$.)

11. Quina és la quantitat de maneres d'acolorir n objectes amb 3 colors si cada color s'ha de fer servir almenys una vegada?

(Sol.: Si els objectes són distints entre sí: $3^n - 3 \cdot 2^n + 3$. Si els objectes són idèntics: $\binom{n-1}{2}$.)

12. Calculeu la quantitat de nombres naturals majors que zero i menors o iguals que 100 que no són divisibles ni per 2, ni per 3, ni per 5, ni per 7.

(Sol.: $100 - 50 - 33 - 20 - 14 + 16 + 10 + 6 + 7 + 4 + 2 - 3 - 2 - 1 - 0 + 0 = 22$.)

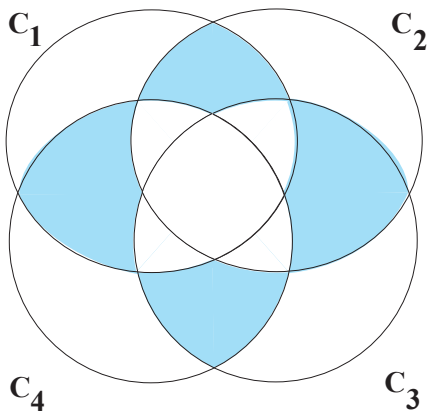
13. Quina és la quantitat de nombres naturals majors que zero i menors o iguals que 100 que són divisibles per dos, i només per dos, dels factors 2, 3 o 5?

(Sol.: 23.)

14. i) Feu la representació gràfica del conjunt format pels elements que pertanyen a tres, i només a tres, dels quatre subconjunts C_1, C_2, C_3 o C_4.

ii) Quin seria el seu cardinal en termes dels cardinals dels subconjunts i de les seues interseccions?

iii) Quina és la quantitat de nombres naturals majors que zero i menors o iguals que 100 que són divisibles per tres, i només per tres, dels factors 2, 3, 5 o 7?



Ens pregunten pel cardinal de la zona de color blau.

15. Quants subconjunts de cardinal divisible per quatre té un conjunt de n elements?

    (*Ajuda: S'ha de substituir x en $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$ per cadascuna de les quatre arrels de la unitat, és a dir les solucions de $x^4 = 1$, $\{1, -1, \mathbf{i}, -\mathbf{i}\}$, i jugar amb els quatre resultats per una banda per tal d'obtenir $\sum_{\ell=0}^{\left[\frac{n}{4}\right]} \binom{n}{4\ell}$, mentre que per una altra banda s'han de calcular potències del tipus $(1+\mathbf{i})^n$ fent servir la fórmula de De Moivre.*)

16. Quants subconjunts de cardinal divisible per tres té un conjunt de n elements?

17. Tenim 7 figuretes d'elfs i 5 de nans que volem col·locar alineats en un prestatge de manera que no hi haja dos nans un al costat de l'altre. De quantes maneres distintes ho podrem fer?

    (Sol.: $\binom{8}{5}$.)

18. (a) Quin és el coeficient de x^2y^3z en el polinomi $(2x - y^2 + 3z)^6$? I el de x^2y^2z? (Sol.: 0 i 0.)
    (b) Quin és el coeficient de x^2y^8z en el polinomi $(2x + y^2 - 5z)^7$? (Sol.: -2100.)
    (c) Quin és el coeficient de $u^2v^3z^3$ en el polinomi $(3uv - 2z + u + v)^7$? (Sol.: -10080.)

19. Quants nombres naturals menors o iguals que 100 no són divisibles pel quadrat de cap enter major que 1?

    (Sol.: $|A_4| = 25, |A_9| = 11, |A_{25}| = 4, |A_{49}| = 2, |A_{4,9}| = 2, |A_{4,25}| = 1$ i la resta d'interseccions són buides. Per tant, $|A_4 \cup A_9 \cup A_{25} \cup A_{49}| = 25 + 11 + 4 + 2 - 2 - 1 = 39$, i així$|X - (A_4 \cup A_9 \cup A_{25} \cup A_{49})| = 61$.)

20. De quantes maneres podem col·locar 4 francesos, 3 russos i 5 italians en una cua de manera que cap de les nacionalitats forme un bloc consecutiu?

    (Sol.: $|A_F| = 9 \cdot \binom{8}{3}$, $|A_R| = 10 \cdot \binom{9}{4}$, $|A_I| = 8 \cdot \binom{7}{3}$, $|A_{FR}| = 42$, $|A_{FI}| = 20$, $|A_{RI}| = 30$, $|A_{FRI}| = 6$. Per tant,

    $$|A_F \cup A_R \cup A_I| = 504 + 1260 + 280 - 42 - 20 - 30 + 6 = 1958.$$

    Com que volem el complementari, el resultat és $\binom{12}{4,3,5} - 1958 = 27720 - 1958 = 25762$.)

21. Una caixa conté 30 boles vermelles, 40 blaves i 50 blanques. Les boles del mateix color són indistingibles. De quantes maneres diferents podem triar un conjunt de 70 boles?

    La resposta la dóna el coeficient de x^{70} en el producte

    $$(1 + x + x^2 + \cdots + x^{30})(1 + x + x^2 + \cdots + x^{40})(1 + x + x^2 + \cdots + x^{50}).$$

    Ara bé, en comptes de multiplicar, el que farem és treballar amb les funcions generatrius de cada factor. Per exemple:

    $$1 + x + x^2 + \cdots + x^{30} = \frac{1 - x^{31}}{1 - x}.$$

Per tant, hem de calcular el coeficient de x^{70} en

$$\frac{1-x^{31}}{1-x}\,\frac{1-x^{41}}{1-x}\,\frac{1-x^{51}}{1-x}=\frac{1}{(1-x)^3}(1-x^{31})(1-x^{41})(1-x^{51})$$

El factor

$$\begin{aligned}(1-x)^{-3} &= \tbinom{-3}{0}-\tbinom{-3}{1}x+\tbinom{-3}{2}x^2-\tbinom{-3}{3}x^3+\dots\\ &= \tbinom{2}{0}+\tbinom{3}{1}x+\tbinom{4}{2}x^2+\tbinom{5}{3}x^3+\dots\\ &= \tbinom{2}{2}+\tbinom{3}{2}x+\tbinom{4}{2}x^2+\tbinom{5}{2}x^3+\dots\end{aligned}$$

Mentre que del producte $(1-x^{31})(1-x^{41})(1-x^{51})$ només interessen els termes de grau menor o igual que 70

$$1-x^{31}-x^{41}-x^{51}+\dots$$

Finalment, el coeficient de x^{70} és

$$\binom{70+2}{2}-\binom{70+2-31}{2}-\binom{70+2-41}{2}-\binom{70+2-51}{2}=1061.$$

22. a) Determineu el coeficient de x^{15} en $(x^2+x^3+x^4+\dots)^4$.

    b) Determineu el coeficient de x^{50} en $(x^7+x^8+x^9+\dots)^6$.

    c) Determineu el coeficient de x^5 en $(1-2x)^{-2}$. (Sol.: $\binom{-2}{5}(-2)^5=192$.)

    d) Determineu el coeficient de x^3 en $(1-x+2x^2)^9$. (Sol.: $9\cdot 8\cdot(-1)\cdot(2)-\binom{9}{3}=-228$.)

23. Trobeu la probabilitat de traure un 12 llançant tres daus.

    (Sol.: Hem de calcular primer els casos favorables i aquestos estan donats pel coeficient de x^{12} en $(x+x^2+x^3+x^4+x^5+x^6)^3=x^3\left(\frac{1-x^6}{1-x}\right)^3$. Equivalentment, el coeficient de x^9 en $(1-3x^6+3x^{12}-x^{18})(1-x)^{-3}$. Aquest coeficient és igual que $\binom{-3}{9}-3\binom{-3}{3}=55-30=25$.

    I ara calcularem els casos possibles i aquests es poden calcular fent servir combinacions amb repetició, $CR_{6,3}=\binom{8}{3}=56$. Per tant, la resposta és $\frac{25}{56}$.)

24. Siga a_n la quantitat de triples ordenats de nombres naturals (i,j,k) tal que $i\geq 0, j\geq 1, k\geq 1$ i $i+3j+3k=n$. Trobeu la funció generatriu de la successió $a_0,a_1,a_2,\dots$ i calculeu una fórmula per a a_n.

(Sol.: La funció generatriu és

$$\begin{aligned}
& (1+x+x^2+\dots)(x^3+x^6+\dots)^2 \\
= \; & x^6(1+x+x^2+\dots)(1+x^3+\dots)^2 \\
= \; & x^6\tfrac{1}{1-x}\left(\tfrac{1}{1-x^3}\right)^2 \\
= \; & x^6\tfrac{1-x^3}{1-x}\left(\tfrac{1}{1-x^3}\right)^3 \\
= \; & x^6(1+x+x^2)\left(1-x^3\right)^{-3} \\
= \; & x^6(1+x+x^2)\left(1-\tbinom{-3}{1}x^3+\tbinom{-3}{2}x^6-\dots+(-1)^k\tbinom{-3}{k}x^{3k}\right) \\
= \; & x^6(1+x+x^2)\left(1+\tbinom{3}{1}x^3+\tbinom{4}{2}x^6-\dots+\tbinom{k+2}{k}x^{3k}\right) \\
= \; & x^6(1+x+x^2)\left(1+\tbinom{3}{1}x^3+\tbinom{4}{2}x^6-\dots+\tbinom{k+2}{2}x^{3k}\right) \\
= \; & x^6+x^7+x^8+3x^9+3x^{10}+3x^{11}+6x^{12}+6x^{13}+6x^{14}+10x^{15}+10x^{16}+10x^{17} \\
& +15x^{18}+15x^{19}+15x^{20}+\dots
\end{aligned}$$

La successió és

$$\{0,0,0,0,0,1,1,1,3,3,3,6,6,6,10,10,10,15,15,15,\dots\}.$$

El terme general, per a $n \geq 6$ és $a_n = \frac{1}{2}\left(\left[\frac{n-6}{3}\right]+2\right)\left(\left[\frac{n-6}{3}\right]+1\right)$.)

25. Siga a_n la quantitat de maneres diferents de pagar n cèntims d'euro fent servir monedes de $1, 2$ i de 5 cèntims. Trobeu la funció generatriu de la successió $a_0, a_1, a_2, \dots$ i calculeu a_{73}.

(Sol.:

$$\begin{aligned}
\tfrac{1}{1-x}\tfrac{1}{1-x^2}\tfrac{1}{1-x^5} &= \frac{\frac{1-x^{10}}{1-x}\frac{1-x^{10}}{1-x^2}\frac{1-x^{10}}{1-x^5}}{(1-x^{10})^3} \\
&= \frac{(1+x+x^2+\dots+x^9)(1+x^2+x^4+x^6+x^8)(1+x^5)}{(1-x^{10})^3}.
\end{aligned}$$

$a_{73} = 8\binom{-3}{6}+2\binom{-3}{7} = 296$.)

26. Per a repassar. Tenim n classes d'objectes i volem determinar la quantitat de maneres diferents de triar k objectes. Considerarem diferents variants: l'elecció és ordenada o desordenada, només es pot triar un objecte de cada classe o no hi ha límit en la tria d'objectes d'una mateixa classe. Ompliu la graella següent amb les respostes per a cada cas.

	Només 1 objecte de cada classe	No hi ha límit d'objectes de cada classe
k-tuples ordenades		
k-tuples desordenades		

27. Quantes solucions estrictament positives té l'equació $a + 2b + c = 9$?

    (Sol.: Hi ha tantes solucions com indica el coeficient de x^9 en el producte

    $$(x+x^2+x^3+\cdots+x^9)^2(x^2+x^4\cdots+x^8) = x^4(1+x+x^2+x^3+\cdots+x^8)^2(1+x^2+x^4\cdots+x^6).$$

    Equivalentment, tantes com el coeficient de x^5 en el producte

    $$\left(1+2x+x^2\right)\frac{1}{(1-x^2)^3}.$$

    Aquest coeficient és $2\cdot\binom{-3}{2} = 12$.

28. I un altre per a repassar. Tenim k boles i les volem distribuir en n urnes. Ompliu la graella següent amb les respostes per a cada cas.

	Com a molt 1 bola en cada urna	No hi ha límit de boles en cada urna
Les boles tenen colors distints		
Les boles són totes iguals		

29. Tenim en una urna boles de dos colors diferents. La probabilitat que, en traure dos boles, totes dues siguen del mateix color, és igual que $\frac{1}{2}$. Demostreu que la quantitat de boles que teníem és un quadrat perfecte.

    (Sol.: Suposem que tenim n boles, de les quals a són d'un color, A, i b de l'altre, B. Tots els possibles subconjunts de dos elements són $\binom{n}{2}$, mentre que tots els possibles subconjunts de dues boles de color A són $\binom{a}{2}$, i tots els possibles subconjunts de dues boles de color B són $\binom{b}{2}$. Per tant, la probabilitat que les dues boles siguen del mateix color és

    $$\frac{\binom{a}{2}+\binom{b}{2}}{\binom{n}{2}} = \frac{1}{2}.$$

Equivalentment,

$$2(a(a-1)+b(b-1)) = n(n-1),$$

o també, tenim en compte que $n = a + b$,

$$2a^2 - 2a + 2b^2 - 2b = (a+b)(a+b-1) = a^2 + ab - a + ba + b^2 - b,$$

$$(a+b)^2 - 2ab - (a+b) = 2ab,$$

$$n^2 - n = 4ab,$$

$$n(n-1) = 4ab.$$

Les solucions del sistema

$$\begin{cases} n(n-1) & = 4ab, \\ n & = a+b, \end{cases}$$

amb incògnites a i b són $\frac{n \pm \sqrt{n}}{2}$. Per tant, perquè a i b siguen nombres naturals cal que $\sqrt{n}$ ho siga també, és a dir, que n siga de la forma $n = k^2$.

Per exemple, si $n = 81$, aleshores a i b són $\frac{81 \pm \sqrt{81}}{2} = \frac{81 \pm 9}{2} = \{45, 36\}$.)

2. Equacions de recurrència

En aquest capítol farem servir habitualment el terme *recurrències*, o en forma estesa, *equacions de recurrència*, perquè es tracta d'equacions que sempre tenen la mateixa forma, que es repeteixen. Ens interessarà calcular, per exemple, el nombre d'estructures combinatòries de grandària o longitud n amb certes característiques. Cada cas, que es correspon amb cada valor de n, dona lloc a un càlcul diferent, i a una resposta diferent, a la que genèricament ens referim amb a_n. Així que l'objecte d'interés és una successió $\{a_n\}_{n=0}^{\infty}$, indexada amb els enters començant en un cert valor n_0.

Començarem aquest capítol amb un exemple que ens condueix a una equació de recurrencia, que hem classificat en funció de quanta informació sobre els casos anteriors cal conéixer i quina complexitat tenen els casos en si. Aquesta introducció pretén il·lustrar la tècnica "artesana" d'aquesta manera d'argumentar. Després explicarem com resoldre equacions de recurrència, o en altres paraules, com obtenir una fórmula general de les successions que les verifiquen, centrant-nos en el cas de les equacions de recurrència lineals i de coeficients constants, que són, potser, les més habituals, i sens dubte les més senzilles. Tal com passava amb les funciones generatrius del tema anterior, les relacions de recurrència són també una tècnica que serveix per a resoldre alguns problemes combinatoris. En general, la dificultat es presenta quan treballem amb grans dimensions.
Ací tenim un problema de combinatòria que les tècniques del tema anterior no resolen directament:

Quantes són les cadenes de n bits sense cap "00"?

És a dir, busquem les cadenes sense cap parell de "0" consecutius. Aquesta situació es pot descriure mitjançant una fórmula que fa referència a etapes de la mateixa en un estat anterior. Si poguerem reduir cada cas a l'anterior (amb un argument general), al final només ens quedarà un primer cas per resoldre, del qual es deduiran tots.
Notem a_n aquest nombre. Per tant
• $a_0 = 1$ (una cadena de longitud zero),
• $a_1 = 2$ (2 cadenes de longitud una: 0 i 1),
• $a_2 = 3$ (3 cadenes de longitud dos: 01, 10 i 11),
• $a_3 = 5$ (5 cadenes de longitud tres: 010, 011, 101, 110 i 111),
• $a_4 = 8$, ...

Podem obtenir els valors de a_n més eficientment? Hi ha alguna fórmula general?

Per a contestar observem que si $n \geq 2$, qualsevol cadena de n bits sense cap "00" compleix una, i solament una de les dues condicions següents:
• o bé acaba per "1". En aquest cas, els bits anteriors poden formar qualsevol cadena de longitud $n - 1$

sense "00".
• o bé acaba per "0". En aquest cas el penúltim bit ha de ser "1", i els bits anteriors poden formar qualsevol cadena de longitud $n-2$ sense "00".
Com que hi ha a_{n-1} cadenes de bits del primer tipus i a_{n-2} cadenes de bits del segon tipus, obtenim la relació:

$$a_n = a_{n-1} + a_{n-2} \quad \text{per a qualsevol } n \geq 2.$$

Aquesta relació és una *relació de recurrència* per a la successió $a_0, a_1, a_2, \ldots$: és una relació que expressa els termes de la successió en funció dels termes amb índexs inferiors. Gràcies a aquesta relació, i als dos valors inicials $a_0 = 1$ i $a_1 = 2$, podem calcular eficientment tants valors a_n com volguem.
En aquest tema, estudiarem com trobar una formula explícita per al terme general de les successions que compleixen certes relacions de recurrència. I l'aplicarem al cas de resoldre els problemes de recompte.

2.1 Successions definides per equacions de recurrència

L'exemple introductori que acabem de veure no és un altre que el famós exemple de la successió de Fibonacci. Aquesta comença amb dos primers termes que són

$$F_0 = 0, \qquad F_1 = 1$$

i que a partir d'ací calcula el terme següent sumant els dos anteriors:

$$F_2 = F_1 + F_0 = 1 + 0 = 1, \quad F_3 = F_2 + F_1 = 1 + 1 = 2, \quad F_4 = F_3 + F_2 = 2 + 1 = 3, \ldots$$

La successió és

$$\{0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots\}$$

Formalment, la llei de recurrència que defineix la successió de Fibonacci és

$$F_{n+2} = F_{n+1} + F_n.$$

La qüestió és saber com calcular directament, per exemple, el terme F_{136}, sense haver de fer 135 iteracions.

Definició 2.1.1 *Una successió $\{a_n\}_{n=0}^{\infty}$ es diu que està definida per una llei de recurrència d'ordre k si existeix una funció $f : \mathbb{R}^k \to \mathbb{R}$ tal que, per a tot $n \in \mathbb{N}$, els termes de la successió verifiquen*

$$a_{n+k} = f(a_n, a_{n+1}, \ldots, a_{n+k-1}). \tag{2.1}$$

Exemple 2.1 *Els primers termes de la successió definida per*

$$a_n = \frac{a_{n-1}}{1 + a_{n-2}}, \qquad a_0 = 1, a_1 = 1$$

són $1, 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{6}, \frac{2}{15}, \frac{4}{35}, \frac{12}{119}, \ldots$. *La funció que defineix la recurrència és* $f(x_0, x_1) = \frac{x_1}{1+x_0}$.

Noteu que si una successió està definida per una llei de recurrència d'ordre k, aleshores els seus primers k termes, $a_0, a_1, \ldots, a_{k-1}$, determinen tota la successió.
Aquest k primers termes, $a_0, a_1, \ldots, a_{k-1}$, s'anomenem de vegades condicions inicials de la successió.

Les relacions de recurrència que ens interessaran, bàsicament perquè són les més senzilles, són les lineals.

Definició 2.1.2 *Una successió $\{a_n\}_{n=0}^{\infty}$ es diu que està definida per una llei de recurrència* **lineal** *i* **homogènia** *d'ordre k si existeixen nombres reals $\lambda_0 \neq 0, \lambda_1, \ldots, \lambda_{k-1}$ tal que, per a tot $n \in \mathbb{N}$, els termes de la successió verifiquen*

$$a_{n+k} = \lambda_{k-1}\, a_{n+k-1} + \cdots + \lambda_1\, a_{n+1} + \lambda_0\, a_n. \tag{2.2}$$

Noteu que la condició $\lambda_0 \neq 0$ no és cap restricció perquè si $\lambda_0 = 0$, aleshores, la llei de recurrència seria almenys d'un ordre menor.
Hi ha infinites successions que verifiquen una llei de recurrència concreta. Per exemple, si en comptes de triar els dos termes inicials com en la successió de Fibonacci, triem $a_0 = -1, \quad a_1 = 3$, el resultat d'aplicar la mateixa llei de recurrència, $a_{n+2} = a_{n+1} + a_n$, hauria donat un altre resultat:

$$-1, 3, 2, 5, 7, 12, 19, \ldots$$

Exemple 2.2 *Els nombres de Lucas, $\{L_n\}_{n=0}^{\infty}$, són els definits per la mateixa llei de recurrència que els de Fibonacci,*

$$L_{n+2} = L_{n+1} + L_n,$$

però amb les condicions inicials

$$L_0 = 2, \quad L_1 = 1.$$

Proposició 2.1.3 *El conjunt $S_{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}}$ de totes les successions definides per una mateixa llei de recurrència lineal amb els coeficients $\lambda_0, \lambda_1, \ldots, \lambda_{k-1}$ té estructura d'espai vectorial real de dimensió k, amb les operacions habituals per a la suma de successions i el producte d'una successió per un escalar.*

Demostració. Com que el conjunt de les successions ja sabem que té estructura d'espai vectorial, només haurem de provar que $S_{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}}$ és un subespai vectorial d'aquest conjunt. Per a això, siga $\alpha, \beta \in \mathbb{R}$ i siguen $a_n, b_n \in S_{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}}$. Tenim que:

$$\begin{aligned} \alpha a_{n+k} + \beta b_{n+k} &= \alpha(\lambda_0 a_n + \cdots + \lambda_{k-1} a_{n+k-1}) + \beta(\lambda_0 b_n + \cdots + \lambda_{k-1} b_{n+k-1}) \\ &= \lambda_0(\alpha a_n + \beta b_n) + \cdots + \lambda_{k-1}(\alpha a_{n+k-1} + \beta b_{n+k-1}) \end{aligned}$$

Per tant $S_{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}}$ és un subespai vectorial de l'espai vectorial de les successions.

Per veure que la seua dimensió és k, considerem l'aplicació

$$\Phi : S_{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}} \to \mathbb{R}^k$$

definida per $\Phi(a_n) = (a_0, a_1, \ldots, a_{k-1})$. Aquesta aplicació és clarament lineal, i a més es tracta d'un isomorfisme. En efecte:

- (Injectiva) En principi,

$$\ker(\Phi) = \{\{a_n\}_{n=0}^{\infty} \in S_{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}} \text{ tal que } \; a_0 = a_1 = \cdots = a_{k-1} = 0\}.$$

Anem a comprovar que si $\{a_n\}_{n=0}^{\infty}$ està en $\ker(\Phi)$, aleshores és la successió nul·la.

Per la llei de recurrència, la successió $\{a_n\}_{n=0}^{\infty}$ complirà

$$a_k = \lambda_0 \cdot 0 + \lambda_1 \cdot 0 + \cdots + \lambda_{k-1} \cdot 0 = 0,$$

$$a_{k+1} = \lambda_0 \cdot 0 + \lambda_1 \cdot 0 + \cdots + \lambda_{k-1} \cdot a_k = 0,$$

ja que $a_k = 0$, i així successivament. És a dir tots els termes de la successió són nuls: això significa que el nucli de l'homomorfisme és la successió nul·la i per tant l'homomorfisme és injectiu.

• (Suprajectiva) Donat $(x_0, x_1, \ldots, x_{k-1}) \in \mathbb{R}^k$, prenem la successió $\{a_n\}_{n=0}^{\infty}$ de $S_{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}}$ de la qual els k primers termes siguen precisament les components d'aquest vector i la resta es calculen mitjançant la llei de recurrència. Clarament $\Phi(a_n) = (x_0, x_1, \ldots, x_{k-1})$, i això prova que Φ és suprajectiva.

Així doncs Φ és un isomorfisme de $S_{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}}$ en $\mathbb{R}^k$, de dimensió k, per tant aquests espais tenen la mateixa dimensió per ser isomorfs. Això conclou la demostració. □

2.2 Solució de les lleis de recurrència lineals i homogènies

Quan es treballa amb espais vectorials, sempre hem d'intentar triar la base de l'espai millor adaptada al problema. I el problema, en el nostre cas, és el de calcular el terme general de la successió.
Comencem amb un exemple de successió definida per una llei de recurrència de primer ordre:

$$a_{n+1} = 2\, a_n, \quad a_0 = 1.$$

La successió no és una altra que la successió geomètrica de raó 2, de terme general

$$a_n = 2^n.$$

Qualsevol altra successió definida per la mateixa llei de recurrència té com a terme general

$$a_n = a_0\, 2^n.$$

Anàlogament, és fàcil comprovar que les successions definides per una llei de recurrència

$$a_{n+1} = \lambda a_n,$$

són totes successions geomètriques de raó λ i de terme general

$$a_n = a_0\, \lambda^n.$$

Tornem ara a la llei de recurrència que defineix la successió de Fibonacci:

$$a_{n+2} = a_{n+1} + a_n.$$

La pregunta ara és si existirà alguna successió geomètrica, $\{a_n = x^n\}_{n=0}^{\infty}$, per a alguna raó x, que verifique aquesta llei de recurrència. Si així fóra, tindríem que, per a tot $n \in \mathbb{N}$,

$$x^{n+2} = x^{n+1} + x^n.$$

Equivalentment,

$$(x^2 - x - 1)x^n = 0.$$

És a dir, x hauria de ser una solució de l'equació quadràtica $x^2 - x - 1 = 0$. Aquesta equació té dues solucions, l'anomenada raó àuria i la seua conjugada,

$$x_1 = \frac{1+\sqrt{5}}{2}, \qquad \text{i} \qquad x_2 = \frac{1-\sqrt{5}}{2}.$$

Així, les dues successions geomètriques següents:

$$\{x_1^n\}_{n=0}^{\infty} = \left\{\left(\frac{1+\sqrt{5}}{2}\right)^n\right\}, \qquad \text{i} \qquad \{x_2^n\}_{n=0}^{\infty} = \left\{\left(\frac{1-\sqrt{5}}{2}\right)^n\right\},$$

formen una base de l'espai vectorial de successions definides per $a_{n+2} = a_{n+1} + a_n$.

És a dir, qualsevol successió $\{a_n\}_{n=0}^{\infty}$, definida per la matixa llei de recurrència, és una combinació lineal de $\{x_1^n\}_{n=0}^{\infty}$ i de $\{x_2^n\}_{n=0}^{\infty}$: existeixen dos escalar $A, B \in \mathbb{R}$ tal que

$$\{a_n\}_{n=0}^{\infty} = A \cdot \{x_1^n\}_{n=0}^{\infty} + B \cdot \{x_1^n\}_{n=0}^{\infty}.$$

Equivalentment,

$$a_n = A \cdot x_1^n + B \cdot x_1^n, \qquad \forall\, n \in \mathbb{N}.$$

Per a calcular ara les coordenades de la successió de Fibonacci en aquesta base, només cal determinar els nombres reals A, B tal que

$$\begin{cases} A\left(\frac{1+\sqrt{5}}{2}\right)^0 + B\left(\frac{1-\sqrt{5}}{2}\right)^0 = 0, \\ A\left(\frac{1+\sqrt{5}}{2}\right)^1 + B\left(\frac{1-\sqrt{5}}{2}\right)^1 = 1. \end{cases}$$

Els membres de la dreta, 0 i 1, en el sistema anterior són els dos primers termes de la successió de Fibonacci. Equivalentment, el sistema es pot escriure com a

$$\begin{cases} A + B = 0, \\ \frac{A+B}{2} + \frac{A-B}{2}\sqrt{5} = 1. \end{cases}$$

I la solució és $A = \frac{1}{\sqrt{5}}, B = -\frac{1}{\sqrt{5}}$. Això vol dir que el terme general de la successió de Fibonacci és

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n. \tag{2.3}$$

Aquesta fórmula s'anomena Fórmula de Binet, i noteu que el número $\sigma = \frac{1+\sqrt{5}}{2}$ no és un altre que la raó àuria. Així, amb la fórmula de Binet, ja podem calcular directament

$$F_{136} = 11825896447871834976429068427.$$

El procediment que hem seguit per a determinar el terme general de la successió de Fibonacci es pot fer per a qualsevol altra successió definida per una llei de recurrència lineal i homogènia.

Definició 2.2.1 *Anomenarem polinomi característic associat a l'espai vectorial $S_{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}}$ al polinomi*

$$P(x) = x^k - \lambda_{k-1}\, x^{k-1} - \cdots - \lambda_1\, x - \lambda_0. \tag{2.4}$$

El Teorema Fonamental de l'Àlgebra afirma que l'equació associada a (2.4) té k solucions en el cos dels nombres complexos, $\mathbb{C}$. La resolució de les recurrències lineals passa per la nostra capacitat de trobar les arrels d'este polinomi. Distingirem els casos en què les arrels siguen simples o quan tinguen una certa multiplicitat. En ambdós casos és senzill trobar una base de $S_{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}}$, resultat donat per la proposició següent.

Proposició 2.2.2 *Si el polinomi característic té k arrels simples (reals o complexes), $x_0, x_1, \ldots, x_{k-1}$, llavors les successions:*

$$x_0^n, x_1^n, \ldots, x_{k-1}^n$$

formen una base de $S_{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}}$.

Demostració. Siga x una arrel del polinomi característic. Primer de tot s'ha de dir que $x_0 \neq 0$. En efecte, si x_0 fóra 0 aleshores

$$0 = P(0) = 0^k - \lambda_{k-1}\, 0^{k-1} - \cdots - \lambda_1\, 0 - \lambda_0 = -\lambda_0.$$

Per tant, $\lambda_0 = 0$ cosa que contradiu la Def. 2.1.2 de successió definida per una llei recurrència lineal, homogènia i d'ordre k, ja que allí exigíem que $\lambda_0 \neq 0$.

Anem a comprovar ara que la successió geomètrica de raó x_0 pertany a $S_{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}}$. En efecte, si $a_n = x^n$ es compleix que:

$$\begin{aligned} a_{n+k} &= x^{n+k} = x^n x^k = x^n(\lambda_{k-1}x^{k-1} + \lambda_{k-2}x^{k-2} + \cdots + \lambda_1 x + \lambda_0) \\ &= \lambda_{k-1}x^{n+k-1} + \lambda_{k-2}x^{n+k-2} + \cdots + \lambda_1 x^{n+1} + \lambda_0 x^n \\ &= \lambda_{k-1}a_{n+k-1} + \lambda_{k-2}a_{n+k-2} + \cdots + \lambda_1 a_{n+1} + \lambda_0 a_n \end{aligned}$$

Això prova que totes les successions $x_0^n, x_1^n, \ldots, x_{k-1}^n$ són elements de $S_{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}}$. Per a provar que formen una base és suficient amb provar que són linealment independents, ja que hi ha en total k successions. Per a això farem servir l'isomorfisme Φ de la proposició anterior (2.1.3), que associava a cada successió els k primers termes:

$$\begin{aligned} \Phi(x_0^n) &= (1, x_0, x_0^2, \ldots, x_0^{k-1}) \\ \Phi(x_1^n) &= (1, x_1, x_1^2, \ldots, x_1^{k-1}) \\ \cdots &\quad \cdots \\ \Phi(x_{k-1}^n) &= (1, x_{k-1}, x_{k-1}^2, \ldots, x_{k-1}^{k-1}) \end{aligned}$$

Si provem que els k vectors de $\mathbb{R}^k$ de la dreta de les igualtats anteriors són linealment independents haurem provat que tenim una base de $\mathbb{R}^k$ i per tant de $S_{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}}$, ja que els isomorfismes transformen bases en bases. El determinant format per les files d'aquests vectors és:

$$\begin{vmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^{k-1} \\ 1 & x_1 & x_1^2 & \ldots & x_1^{k-1} \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 1 & x_{k-1} & x_{k-1}^2 & \ldots & x_{k-1}^{k-1} \end{vmatrix}$$

Aquest determinant és el que s'anomena determinant de Vandermonde, i el seu valor és el producte de totes les possibles diferències:

$$(x_1 - x_0)(x_2 - x_0)\cdots(x_{k-1} - x_0)(x_2 - x_1)(x_3 - x_1)\cdots(x_{k-1} - x_1)\cdots(x_{k-1} - x_{k-2}).$$

Una altra manera d'escriure això és amb el símbol del productori:

$$\prod_{0\le i<j\le n}(x_j - x_i).$$

Com que hem suposat que totes les arrels són simples, aleshores tots els factors són no nuls, i llavors, el determinant és no nul. □

Per al cas en què apareguen arrels múltiples, tenim el següent resultat.

Proposició 2.2.3 *Si x és una arrel de multiplicitat $\ell > 1$, aleshores les successions*

$$x^n, nx^n, n^2x^n, \ldots, n^{\ell-1}x^n$$

verifiquen la llei de recurrència.

Demostració. Per a cada $n > k$ formem el polinomi

$$p_n(x) = x^n(x^k - (\lambda_0 + \lambda_1 x + \lambda_2 x^2 + \cdots + \lambda_{k-1}x^{k-1})).$$

El grau d'aquest polinomi és $n+k$. Si x_0 és una arrel del polinomi característic amb multiplicitat ℓ, ho serà també amb multiplicitat ℓ de $p_n(x)$. Però això significa (per teoria de polinomis) que x_0 serà una arrel de multiplicitat $\ell - i$ de la seua derivada i-èsima $p_n^{(i)}(x)$ per a tot $i = 0, 1, \ldots, \ell - 1$. Modificarem una mica els polinomis $p_n^{(i)}(x)$ per a formar una família de polinomis $q_n^1, q_n^2, \ldots, q_n^{\ell-1}$.

El primer, $p_n'(x)$, el multipliquem per x, i així considerem $q_n^1(x) = xp_n'(x)$. Considerem després $q_n^2(x) = x\left(q_n^1\right)'(x)$. I en general, per a $i = 2, \ldots, \ell - 1$, $q_n^i(x) = x\left(q_n^{i-1}\right)'(x)$.

És fàcil comprovar que x_0 és una arrel de tots els polinomis $q_n^i(x)$, per a $i = 1, 2, \ldots, \ell - 1$. Com que

$$q_n^1(x) = (n+k)x^{n+k} - (\lambda_0 nx^n + \lambda_1(n+1)x^{n+1} + \cdots + \lambda_{k-1}(n+k-1)x^{n+k-1}),$$

$$q_n^2(x) = (n+k)^2x^{n+k} - (\lambda_0 n^2x^n + \lambda_1(n+1)^2x^{n+1} + \cdots + \lambda_{k-1}(n+k-1)^2x^{n+k-1}),$$

i en general,

$$q_n^i(x) = (n+k)^ix^{n+k} - (\lambda_0 n^ix^n + \lambda_1(n+1)^ix^{n+1} + \cdots + \lambda_{k-1}(n+k-1)^ix^{n+k-1}),$$

si substituïm x per x_0, tenim que

$$(n+k)^ix_0^{n+k} = \lambda_0 n^ix_0^n + \lambda_1(n+1)^ix_0^{n+1} + \lambda_2(n+2)^ix_0^{n+2} + \cdots + \lambda_{k-1}(n+k-1)^ix_0^{n+k-1}.$$

I això vol dir que la successió $\{n^i\, x_0^n\}_{n=0}^{\infty}$ verifica la llei de recurrència. □

Vegem-ne uns exemples.

Exemple 2.3 *La successió definida per*

$$y_{n+1} - 2y_n \cos(\alpha) + y_{n-1} = 0,$$

té per equació associada

$$x^2 - 2x\cos(\alpha) + 1 = 0.$$

Les arrels d'aquesta equació quadràtica són

$$x = \cos(\alpha) \pm \sqrt{\cos^2(\alpha) - 1} = \cos(\alpha) \pm \mathbf{i}\sin(\alpha) = e^{\pm \mathbf{i}\alpha}.$$

Per tant, una base de l'espai vectorial de totes les successions que verifiquen aquesta llei de recurrència és

$$\{\{e^{\mathbf{i}n\alpha}\}_{n=0}^{\infty}, \{e^{-\mathbf{i}n\alpha}\}_{n=0}^{\infty}\}.$$

També podem canviar la base ja que, donat que,

$$\begin{aligned} \tfrac{1}{2}\left(e^{\mathbf{i}n\alpha} + e^{-\mathbf{i}n\alpha}\right) &= \cos(n\alpha), \\ \tfrac{1}{2\mathbf{i}}\left(e^{\mathbf{i}n\alpha} - e^{-\mathbf{i}n\alpha}\right) &= \sin(n\alpha), \end{aligned}$$

aleshores

$$\{\{\cos(n\alpha)\}_{n=0}^{\infty}, \{\sin(n\alpha)\}_{n=0}^{\infty}\},$$

és una altra base.

Exemple 2.2.4 *Considerem la llei de recurrència*

$$a_{n+2} = 4\, a_{n+1} - 4a_n.$$

L'equació associada és $x^2 - 4x + 4 = (x-2)^2 = 0$, que té una solució doble, $x_0 = 2$.
Així, les dues successions geomètriques següents:

$$\{2^n\}_{n=0}^{\infty}, \qquad i \qquad \{n2^n\}_{n=0}^{\infty},$$

formen una base de l'espai vectorial de successions definides per $a_{n+2} = 4\, a_{n+1} - 4a_n$.

Exemple 2.2.5 *Considerem la successió definida per*

$$a_{n+2} = -a_n, \quad a_0 = 0, a_1 = 1.$$

L'equació associada és $x^2 + 1 = 0$, i té dues solucions imaginàries, $x = \pm\mathbf{i}$.
Així, les dues successions geomètriques següents:

$$\{\mathbf{i}^n\}_{n=0}^{\infty}, \qquad i \qquad \{(-\mathbf{i})^n\}_{n=0}^{\infty},$$

formen una base de l'espai vectorial de successions definides per $a_{n+2} = -a_n$.
Per a calcular ara les coordenades de la successió en aquesta base, només cal determinar els nombres reals A, B tal que

$$\begin{cases} A + B = 0, \\ A\mathbf{i} - B\mathbf{i} = 1. \end{cases}$$

La solució és $A = -\frac{\mathbf{i}}{2}, B = \frac{\mathbf{i}}{2}$. Noteu que són nombres complexos. Això vol dir que el terme general de la successió és

$$a_n = -\frac{\mathbf{i}}{2}\mathbf{i}^n + \frac{\mathbf{i}}{2}(-\mathbf{i})^n = \frac{\mathbf{i}^{n+1}}{2}\left(-1 + (-1)^n\right) = \begin{cases} 0 & n \text{ parell} \\ -(-1)^{\frac{n+1}{2}} & n \text{ senar.} \end{cases}$$

Noteu, i això és el que és important, en el cas d'arrels imaginàries, encara que les successions que formen la base siguen successions geomètriques amb raó un nombre complex, la combinació d'ambdues dóna lloc a una successió els termes de la qual són tots nombres reals.

Finalment, el resultat general, sense demostració

Teorema 2.2.6 *Siga*

$$a_{n+k} = \lambda_{k-1}\, a_{n+k-1} + \cdots + \lambda_1\, a_{n+1} + \lambda_0\, a_n$$

una llei de recurrència d'ordre k lineal.

1. *Si x és una solució simple (real o complexa) del polinomi característic associat (2.4), aleshores la successió geomètrica de raó x, $\{x^n\}_{n=0}^{\infty}$, verifica la llei de recurrència.*

2. *Si x és una solució de multiplicitat $\ell > 1$ del polinomi característic associat (2.4), aleshores les successions*

   $$\{x^n\}_{n=0}^{\infty},\ \{nx^n\}_{n=0}^{\infty},\ \{n^2x^n\}_{n=0}^{\infty}, \ldots, \{n^{\ell-1}x^n\}_{n=0}^{\infty},$$

   verifiquen la llei de recurrència.

3. *La família formada per totes les successions anteriors per a totes les arrels del polinomi característic associat és una base de l'espai vectorial de totes les successions que verifiquen la mateixa llei de recurrència. Com a conseqüència, el terme general de la successió és una combinació lineal de totes elles.*

Resumint, el mètode de resolució de les recurrències lineals és:

1. Escriure la recurrència en la forma estandard i el seu polinomi característic.

2. Trobar les arrels del polinomi característic.

3. Per a cada arrel del polinomi característic, α_i, de multiplicitat ℓ_i s'afig un sumand a la solució general de la recurrència lineal de la forma "producte d'un polinomi de grau $\ell_i - 1$ per α_i^n ".

4. Se substitueixen els valors inicials en la solució general per a trobar els valors de les constants arbitràries.

2.3 El determinant d'una classe de matrius

Considerem, per a cada $n > 0$, la matriu $n \times n$

$$M_n = \begin{pmatrix} 2 & 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 2 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 2 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1 & 2 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 2 & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 & 2 \end{pmatrix}.$$

Observeu que M_n és una matriu quadrada on les entrades de la diagonal principal i de les diagonals paral·leles adjacents són iguals. Totes les altres entrades són nul·les. Aquest és un cas particular del que s'anomena matriu de Toeplitz. L'objectiu és calcular per a tot $n > 0$ el determinant, D_n, de la matriu M_n. Observeu que $D_1 = 2, D_2 = 3, D_3 = 4$. Amb un poc més d'esforç podem calcular $D_4 = 5$. Sembla que $D_n = n + 1$. Però, podrem demostrar-ho?
Intentem trobar si la successió de determinants $\{D_n\}_{n=1}^{\infty}$ verifica alguna llei de recurrència. Si desenvolupem per la primera columna el determinant D_n, tenim que $D_n = 2D_{n-1} - 1\det(C_{n-1})$, on

$$C_{n-1} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 2 & 1 & \dots & 0 & 0 \\ 0 & 1 & 2 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2 & 1 \\ 0 & 0 & 0 & \dots & 1 & 2 \end{pmatrix}.$$

Si desenvolupem ara el determinant de C_{n-1}, ara per la primera fila, tenim que

$$D_n = 2D_{n-1} - D_{n-2}.$$

Aquesta és la llei de recurrència que buscàvem. L'equació associada és

$$x^2 - 2x + 1 = (x-1)^2 = 0.$$

Té una solució doble $x = 1$, per tant, la base de successions és

$$\{1^n\}_{n=0}^{\infty} = \{1\}_{n=0}^{\infty}, \qquad \text{i} \qquad \{n\,1^n\}_{n=0}^{\infty} = \{n\}_{n=0}^{\infty}.$$

Per a calcular ara les coordenades de la successió en aquesta base, només cal determinar els nombres reals A, B tal que

$$\begin{cases} A \cdot 1 + B \cdot 1 = D_1 = 2, \\ A \cdot 1 + B \cdot 2 = D_2 = 3. \end{cases}.$$

La solució és $A = 1, B = 1$. Això vol dir que el terme general de la successió és

$$a_n = 1 + n,$$

que és el que conjecturàvem.

2.4 Equacions de recurrència lineals i funcions generatrius

Podem resoldre recurrències lineals usant funciones generatrius. Tota successió, $\{a_n\}_{n=0}^{\infty}$, pot tenir una funció generatriu associada, la que li correspon a la sèrie infinita

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots .$$

El problema és saber determinar el que es diu la forma tancada d'aquesta sèrie. És a dir, la funció $F(x)$ tal que el seu desenvolupament en sèrie de Taylor siga precísament $\sum_{n=0}^{\infty} a_n x^n$.
En el cas de successions definides per equacions de recurrència lineals, això és sempre possible. Vejam com exemple quina seria la funció generatriu de la successió de Fibonacci.
Comecem escrivint

$$F(x) = \sum_{n=0}^{\infty} F_n x^n = F_0 + F_1 x + F_2 x^2 + F_3 x^3 + \cdots .$$

L'equació de recurrència permet fer les següents manipulacions:

$$\begin{aligned}
F(x) &= F_0 + F_1 x + \textstyle\sum_{n=2}^{\infty} F_n x^n \\
&= F_0 + F_1 x + \textstyle\sum_{n=2}^{\infty} (F_{n-1} + F_{n-2}) x^n \\
&= F_0 + F_1 x + \textstyle\sum_{n=2}^{\infty} F_{n-1} x^n + \sum_{n=2}^{\infty} F_{n-2} x^n \\
&= F_0 + F_1 x + x \textstyle\sum_{n=2}^{\infty} F_{n-1} x^{n-1} + x^2 \sum_{n=2}^{\infty} F_{n-2} x^{n-2} \\
&= F_0 + F_1 x + x \textstyle\sum_{n=1}^{\infty} F_n x^n + x^2 \sum_{n=0}^{\infty} F_n x^n \\
&= F_0 + F_1 x + x \left(-F_0 + \textstyle\sum_{n=0}^{\infty} F_n x^n\right) + x^2 \sum_{n=0}^{\infty} F_n x^n \\
&= 0 + 1\, x + x \left(-0 + \textstyle\sum_{n=0}^{\infty} F_n x^n\right) + x^2 \sum_{n=0}^{\infty} F_n x^n \\
&= x + xF(x) + x^2 F(x).
\end{aligned}$$

És a dir, la funció generatriu cercada ha de complir l'equació:

$$F(x) = x + xF(x) + x^2 F(x).$$

Per tant, la funció generatriu de la successió de Fibonacci és

$$F(x) = \frac{x}{1 - x - x^2}.$$

Això vol dir que la derivada n-èsima de la funció F en $x = 0$, dividida per $n!$, és terme n-èsim de la successió de Fibonacci:

$$F_n = \frac{F^{(n)}(0)}{n!}.$$

Una vegada ja coneixem la funció generatriu, podem fer més coses. Noteu que la funció que hem trobat és de les que s'anomenen funcions racionals (quocient entre funcions polinòmiques). Aquestes funcions es poden descomposar en fraccions més senzilles. Si ja heu vist alguna cosa d'integració de funcions reals, això és el que es fa per a integrar aquest tipus de funcions.
El procediment és el següent: primer s'obtenen els factors simples del polinomi que apareix en el denominador. En el nostre cas, $1-x-x^2$. Com que les arrels són, tret del signe, la raó àuria $\sigma=\frac{1+\sqrt{5}}{2}$ i la seua conjugada $\overline{\sigma}=\frac{1-\sqrt{5}}{2}$, aleshores

$$1-x-x^2=-(x+\sigma)(x+\overline{\sigma}).$$

Això vol dir que la funció racional es pot escriure com a suma de les funcions elementals $\frac{1}{x+\sigma}$ i $\frac{1}{x+\overline{\sigma}}$:

$$F(x)=\frac{x}{1-x-x^2}=\frac{A}{x+\sigma}+\frac{B}{x+\overline{\sigma}},$$

on A i B són nombres reals. Vejam com es determinen A i B. Si sumem

$$\frac{A}{x+\sigma}+\frac{B}{x+\overline{\sigma}}=\frac{A(x+\overline{\sigma})+B(x+\sigma)}{(x+\sigma)(x+\overline{\sigma})}=\frac{(A+B)x+A\overline{\sigma}+B\sigma}{-1+x+x^2}.$$

Igualant ara numeradors (atenció al signe) $x=-(A+B)x+A\overline{\sigma}+B\sigma$, aleshores

$$\begin{cases}1 &= -A-B\\ 0 &= A\overline{\sigma}+B\sigma.\end{cases}$$

La solució del qual és $A=-\frac{1}{\sqrt{5}}\sigma, B=\frac{1}{\sqrt{5}}\overline{\sigma}$. Això vol dir que

$$F(x)=\frac{x}{1-x-x^2}=\frac{1}{\sqrt{5}}\left(-\frac{\sigma}{x+\sigma}+\frac{\overline{\sigma}}{x+\overline{\sigma}}\right)=\frac{1}{\sqrt{5}}\left(-\frac{1}{1+\frac{x}{\sigma}}+\frac{1}{1+\frac{x}{\overline{\sigma}}}\right).$$

Com que $\frac{1}{\sigma}=-\overline{\sigma}$, llavors

$$F(x)=\frac{1}{\sqrt{5}}\left(-\frac{1}{1-\overline{\sigma}x}+\frac{1}{1-\sigma x}\right).$$

Noteu que d'acíes pot tornar a obtenir la fórmula de Binet (2.3) sense més que aplicar el que ja sabem sobre els coeficients de x^n en cadascun dels termes $\dfrac{1}{1-\overline{\sigma}x}$ i $\dfrac{1}{1-\sigma x}$, és a dir,

$$F(x)=\frac{1}{\sqrt{5}}\sum_{n=0}^{\infty}\binom{1+n-1}{n}(\sigma x)^n-\sum_{n=0}^{\infty}\binom{1+n-1}{n}(\overline{\sigma}x)^n=\frac{1}{\sqrt{5}}\sum_{n=0}^{\infty}(\sigma^n-\overline{\sigma}^n)x^n$$

Com que $F(x)=\displaystyle\sum_{n=0}^{\infty}F_nx^n$, aleshores

$$F_n=\frac{1}{\sqrt{5}}\left(\sigma^n-\overline{\sigma}^n\right)=\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n-\frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Tot això ho hem fet només en l'exemple de la successió de Fibonacci, però és ben fàcil fer-ho també per a qualsevol altra successió definida per una llei de recurrència lineal.

2.5 Equacions en diferències finites

Les equacions en diferències finites poden considerar-se com a equacions de recurrència no homogènies. El seu estudi dependrà en gran part de la resolució de l'equació en recurrència homogènia associada. En aquesta secció mostrarem un mètode per a obtindre les seues solucions, posant l'accent en les de primer i segon ordre. Com en la primera part del tema, ens centrarem en l'estudi de les equacions en diferències finites lineals amb coeficients constants

Definició 2.5.1 *Una successió $\{a_n\}_{n=0}^{\infty}$ es diu que está definida per una equació en diferències finites d'ordre k si existeix una aplicació $f : \mathbb{R}^{k+1} \to \mathbb{R}$ tal que, per a tot $n \in \mathbb{N}$, els termes de la successió verifiquen*

$$a_{n+k} = f(a_n, a_{n+1}, \ldots, a_{n+k-1}, n). \tag{2.5}$$

Noteu que la diferència amb les successions definides per una llei de recurrència és el darrer argument de la funció.

Exemple 2.4 *Els primers termes de la successió definida per*

$$a_n = \frac{a_{n-1}}{1 + a_{n-2}} + (-2)^n, \qquad a_0 = 1, a_1 = 1$$

són $1, 1, \frac{1}{2} + (-2)^2, \frac{1}{4} + (-2)^3 = \frac{9}{2}, \frac{1}{6} + (-2)^4 = -\frac{23}{4}, \frac{2}{15} + (-2)^5 = \frac{329}{44}, \ldots$.
La funció que defineix la recurrència és $f(x_0, x_1, n) = \frac{x_1}{1+x_0} + (-2)^n$.

Com en el cas de les successions definides per una llei de recurrència, ací només estudiarem les que s'anomenen lineals, en les quals la funció f és de la forma

$$f(a_n, a_{n+1}, \ldots, a_{n+k-1}, n) = g_0(n)a_n + g_1(n)a_{n+1} + \cdots + g_{k-1}(n)a_{n+k-1} + \psi(n),$$

on $g_i(n)$, per a $i = 0, \ldots, k-1$, i $\psi(n)$ són funcions només de la darrera variable, n.
A més a més, direm que és de coeficients constants, si les funcions $g_i(n)$, per a $i = 0, \ldots, k-1$, i $\psi(n)$ tampoc no depenen de n, és a dir, són constants:

$$f(a_n, a_{n+1}, \ldots, a_{n+k-1}, n) = c_0a_n + c_1a_{n+1} + \cdots + c_{k-1}a_{n+k-1} + \psi.$$

Exemple 2.5 *L'exemple anterior (2.4) no és lineal. Un que sí que ho és seria el següent: La successió definida per*

$$a_n = na_{n-1} + (n-2)^2a_{n-2} + (-2)^n, \qquad a_0 = 1, a_1 = 1.$$

Aquest exemple no és de coeficients constants. Un altre que sí que ho és seria el següent: La successió definida per

$$a_n = 2a_{n-1} + 3a_{n-2} - 2, \qquad a_0 = 1, a_1 = 1.$$

Aprofitant aquest darrer exemple, si definim a partir de la successió $\{a_n\}_{n\geq 0}$ una altra successió per

$$b_n = a_{n+1} - a_n,$$

aleshores, és fàcil comprovar que la successió $\{b_n\}_{n\geq 0}$ verifica la llei de recurrència lineal i de segon ordre

$$b_n = 2b_{n-1} + 3b_{n-2}.$$

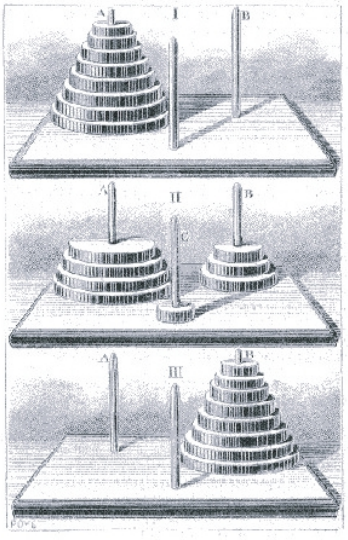
La construcció d'una nova successió a partir de diferències entre termes d'una altra és el que dóna nom a aquest apartat: equacions en diferències finites.
Noteu també que podem definir en el conjunt de les successions un operador, anomenat operador increment, i denotat per Δ, per

$$\Delta a_n = a_{n+1} - a_n, \quad \forall n \geq 0.$$

2.5.1 *Primer ordre*

Abans d'estudiar aquest tipus d'equacions, vegem un exemple clàssic denominat *Les torres d'Hanoi*, que deu el seu origen al matemàtic francés Edward Anatole Lucas (1842-1891).

Exemple 2.6 *Conta la llegenda que els monjos d'un monestir de Hanoi mesuren el temps que manca per a l'arribada de la fi del món amb el següent procediment: disposen de tres agulles de diamant, en una de les quals s'apilen* 64 *discos d'or de diàmetres distints, i ordenats pel seu diàmetre. Cada segon un dels monjos mou un disc d'una agulla a una altra. Aquesta tasca finalitzarà (i amb ella, també s'acabarà el món) quan aconseguisquen transportar tots els discos a una altra agulla. Ara bé, al llarg del procés mai es pot col·locar un disc sobre un altre de diàmetre inferior. Quants moviments són necessaris per a resoldre el problema?*



Les torres de Hanoi.

Podeu mirar la pàgina web següent:
`http://www.psicoactiva.com/juegos/hanoi/jg_hanoi.htm`.

Per a començar tractarem de trobar la solució del problema per a casos xicotets, és a dir, per a pocs discos, i després generalitzarem el resultat. Definim a_n el mínim nombre de moviments necessaris per a passar una torre de n discos d'una agulla a una altra. És obvi que $a_1 = 1$ i $a_2 = 3$. Però, què passa quan hi ha més discos? Si $n = 3$, és fàcil adonar-se que la forma òptima de procedir és passar els dos primers discos a l'agulla intermèdia, després passar el tercer disc a la tercera agulla i finalment els dos discos de l'agulla intermèdia a la tercera. Això ens dona una estratègia recursiva. En el fons, si sabem com procedir amb dos discos, també sabem fer-ho amb tres.
Amb n discos el raonament és similar. Cal transferir $n-1$ discos a l'agulla intermèdia, passar l'últim disc a la tercera agulla i, finalment, els $n-1$ discos de l'agulla intermèdia a la tercera. Per tant, en termes de a_n, el nombre de moviments que es necessiten són:

- *a_{n-1} moviments per a transferir els $n-1$ primers discos a l'agulla intermèdia.*
- *Un moviment per a passar l'últim disc a la tercera agulla.*
- *a_{n-1} moviments per a transferir els $n-1$ primers discos de l'agulla intermèdia a la tercera.*

En resum, el total de moviments per a transferir una torre de n discos és

$$a_n = 2a_{n-1} + 1, \qquad a_1 = 1.$$

Aquesta és una successió recurrent, ja que el terme n-èsim de la successió s'obté a partir del $(n-1)$-èsim. Per al nostre problema cal determinar el valor de a_{64}. Per a donar la resposta hauríem de calcular tots els valors de la successió fins a $n = 63$. El següent resultat ens dona una manera de trobar la solució per a un n qualsevol.

Intentarem trobar el terme general d'una successió definida per una equació en diferències finites de primer ordre, lineal, i de coeficients constants. Concretament, una que siga de la forma

$$a_{n+1} = \lambda\, a_n + c. \tag{2.6}$$

Si posem que $a_0 = \alpha_0$, aleshores

$$\begin{aligned} a_1 &= \lambda\, \alpha_0 + c, \\ a_2 &= \lambda^2\, \alpha_0 + \lambda\, c + c, \\ a_3 &= \lambda^3\, \alpha_0 + \lambda^2\, c + \lambda\, c + c, \\ \dots &\quad \dots \quad \dots \end{aligned}$$

Per tant, el terme general no és un altre que

$$\begin{aligned} a_n &= \lambda^n\, \alpha_0 + (\lambda^{n-1} + \cdots + \lambda^2 + \lambda + 1)c \\ &= \lambda^n\, \alpha_0 + \left(\sum_{i=0}^{n-1} \lambda^i \right) c. \end{aligned}$$

Només queda calcular la suma de la sèrie que multiplica c.

$$a_n = \begin{cases} \lambda^n\ \alpha_0 + \frac{\lambda^n - 1}{\lambda - 1} c, & \text{si } \lambda \neq 1, \\ \alpha_0 + cn, & \text{si } \lambda = 1. \end{cases}$$

Una vegada vist aquest exemple, cal remarcar que el terme $\lambda^n\ \alpha_0$ no és un altre que el terme general de la successió definida per la relació $a_{n+1} = \lambda\ a_n$ amb condició inicial $a_0 = \alpha_0$, mentre que l'altre terme és una solució particular de $a_{n+1} = \lambda\ a_n + c$, però amb $a_0 = 0$.

Passem al cas general.

Teorema 2.7 *La solució de l'equació en diferències finites lineal de primer ordre*

$$a_{n+1} = \lambda a_n + \psi(n),$$

amb condició inicial $a_0 = \alpha_0$, està donada per

$$a_n = \alpha_0 \lambda^n + \sum_{i=0}^{n-1} \psi(i) \lambda^{n-i-1}.$$

Demostració. Siga s_n una successió el primer terme de la qual és α_0 i que per a $n \geq 1$ els termes valen

$$s_n = \alpha_0 \lambda^n + \sum_{i=0}^{n-1} \psi(i) \lambda^{n-i-1}.$$

Aquesta successió compleix la relació de recurrència. En efecte

$$\begin{aligned} \lambda s_n + \psi(n) &= \lambda \left(\alpha_0 \lambda^n + \sum_{i=0}^{n-1} \psi(i) \lambda^{n-1-i} \right) + \psi(n) \\ &= \alpha_0 \lambda^{n+1} + \sum_{i=0}^{n-1} \psi(i) \lambda^{n-i} + \psi(n) \\ &= \alpha_0 \lambda^{n+1} + \sum_{i=0}^{n-1} \psi(i) \lambda^{n-i} + \psi(n) \lambda^{n-n} \\ &= \alpha_0 \lambda^{n+1} + \sum_{i=0}^{n} \psi(i) \lambda^{n-i} = s_{n+1}. \end{aligned}$$

Per a acabar la demostració, siga s_n una successió que complisca la llei de recurrència i que verifique $s_0 = a_0$. Hi hauria prou amb provar que $s_1 = a_1$ per a concloure que $s_n = a_n, \forall n \in \mathbb{N}$, però això és trivial perquè

$$a_1 = a_0 \lambda + \psi(0) = \alpha_0 \lambda + \sum_{i=0}^{0} \psi(i) \lambda^{0-i} = \alpha_0 \lambda + \psi(0) \lambda^{0-0} = \alpha_0 \lambda + \psi(0) = s_1.$$

□

Exemple 2.8 *Trobarem ara el terme general de*

$$a_{n+1} = a_n + 2^{n+2} - 4$$

amb condició inicial $a_0 = \alpha_0$. *En aquest cas, noteu que* $\lambda = 1$. *Per tant, segons el teorema,*

$$\begin{aligned} a_n &= \alpha_0 1^n + \sum_{i=0}^{n-1} (2^{i+2} - 4) 1^{n-i} \\ &= \alpha_0 + \sum_{i=0}^{n-1} (2^{i+2} - 4) \\ &= \alpha_0 + \sum_{i=0}^{n-1} 2^{i+2} - \sum_{i=0}^{n-1} 4 \\ &= \alpha_0 + \tfrac{2^{n+2} - 2^2}{2-1} - 4n \\ &= \alpha_0 + 4(2^n - 1 - n). \end{aligned}$$

2.5.2 *Qualsevol ordre*

Ara volem trobar solucions de l'equació en diferències finites

$$a_{n+k} = c_0 a_n + c_1 a_{n+1} + \cdots + c_{k-1} a_{n+k-1} + \psi(n).$$

Teorema 2.9 *(Solució particular)*
Siga $\{b_n\}_{n=0}^{\infty}$ *la solució de la llei de recurrència d'ordre* k, *lineal,*

$$a_{n+k} = c_0 a_n + c_1 a_{n+1} + \cdots + c_{k-1} a_{n+k-1}, \tag{2.7}$$

amb condicions inicials

$$b_0 = 0, b_1 = 0, \ldots, b_{k-2} = 0, b_{k-1} = 1.$$

Aleshores, per a qualsevol successió $\{\psi(n)\}_{n=0}^{\infty}$, *la successió* $\{a_n\}_{n=0}^{\infty}$ *definida per*

$$a_0 = 0, a_1 = 0, \ldots, a_{k-2} = 0, a_{k-1} = 0$$

$$a_n = (\psi(0), \ldots, \psi(n-k)) \cdot (b_{n-1}, \ldots, b_{k-1}) = \sum_{j=0}^{n-k} b_{n-j-1} \psi(j),$$

on el punt "$\cdot$*" representa el producte escalar de vectors, és una solució particular de l'equació en diferències finites*

$$a_{n+k} = c_0 a_n + c_1 a_{n+1} + \cdots + c_{k-1} a_{n+k-1} + \psi(n). \tag{2.8}$$

Demostració. Per a no complicar la cosa, farem la demostració per a $k = 2$. La demostració general és anàloga però molt més llarga. L'únic que hem de fer és comprovar que la successió així construïda verifica l'equació (2.8). Noteu que, per ser $\{b_n\}_{n=0}^{\infty}$ la solució de la llei de recurrència (2.7), aleshores

$$b_{n+2} = c_0 b_n + c_1 b_{n+1}.$$

Així,

$$\begin{aligned}
a_{n+2}-c_0a_n-c_1a_{n+1} &= \sum_{j=0}^{n} b_{n+2-j-1}\psi(j) - c_0\sum_{j=0}^{n-2} b_{n-j-1}\psi(j) - c_1\sum_{j=0}^{n-1} b_{n+1-j-1}\psi(j)\\
&= \sum_{j=0}^{n} b_{n+1-j}\psi(j) - c_0\sum_{j=0}^{n-2} b_{n-j-1}\psi(j) - c_1\sum_{j=0}^{n-1} b_{n-j}\psi(j)\\
&= \sum_{j=0}^{n-2} b_{n+1-j}\psi(j) - c_0\sum_{j=0}^{n-2} b_{n-j-1}\psi(j) - c_1\sum_{j=0}^{n-2} b_{n-j}\psi(j)\\
&\qquad +b_{n+1-n}\psi(n)+b_{n-(n-1)+1}\psi(n-1)-c_1b_{n-(n-1)}\psi(n-1)\\
&= \sum_{j=0}^{n-2}\left(b_{n-j+1}-c_0b_{n-j-1}-c_1b_{n-j}\right)\psi(j)\\
&\qquad +b_1\psi(n)+b_2\psi(n-1)-c_1b_1\psi(n-1)\\
&= \sum_{j=0}^{n-2}(0)\,\psi(j)+1\psi(n)+(b_2-c_1b_1)\psi(n-1)\\
&= \psi(n)
\end{aligned}$$

on hem aplicat, al final, que $b_1=1$ i que $b_2=c_0b_0+c_1b_1=c_1b_1$. □

Exemple 2.10 *Troba una solució particular de*

$$a_{n+2}=5a_{n+1}-4a_n+2^n.$$

Primer resolem la part lineal

$$b_{n+2}=5b_{n+1}-4b_n$$

amb les condicions inicials $b_0=0, b_1=1$. *L'equació característica és*

$$x^2-5x+4=(x-1)(x-4).$$

Per tant, $b_n=A\cdot 1^n+B\cdot 4^n$. *A partir de les condicions inicials, obtenim el resultat*

$$b_n=\frac{4^n-1}{3}.$$

Ara la solució particular, tal com indica el teorema:

$$\begin{aligned} a_n^{part} &= \sum_{j=0}^{n-2} b_{n-j-1}\psi(j) = \frac{1}{3}\sum_{j=0}^{n-2}(4^{n-j-1}-1)2^j \\ &= \frac{1}{3}\sum_{j=0}^{n-2}(2^{2n-2j-2}-1)2^j = \frac{1}{3}\sum_{j=0}^{n-2}2^{2n-2j-2}2^j - \frac{1}{3}\sum_{j=0}^{n-2}2^j \\ &= \frac{1}{3}2^{2n-2}\sum_{j=0}^{n-2}2^{-j} - \frac{1}{3}\sum_{j=0}^{n-2}2^j \\ &= \frac{1}{3}\left(2^{2n-2}\frac{1-2^{-(n-1)}}{1-2^{-1}} - \frac{1-2^{n-1}}{1-2}\right) \\ &= \frac{2^{n-1}(2^n-3)+1}{3}. \end{aligned}$$

Observem que el sumand $\frac{1}{3}$ de la solució particular també ix en b_n amb el factor -1. Si ho posem en la combinació de la solució de la part lineal llavors també és una solució particular

$$a_n^{part} - \frac{1}{3} = \frac{2^{n-1}(2^n-3)}{3}.$$

Exemple 2.11 *Troba una solució particular de*

$$a_{n+2} = 2a_{n+1} - a_n + 2^{n+2}.$$

El primer que hem de fer és trobar la solució de la part lineal

$$b_{n+2} = 2b_{n+1} - b_n$$

amb les condicions inicials $b_0 = 0, b_1 = 1$. L'equació característica és

$$x^2 - 2x + 1 = (x-1)^2.$$

Per tant, $b_n = (An+B)1^n = An + B$. A partir de les condicions inicials, tenim que $B = 0$ i $A = 1$. Per tant, $b_n = n$.
Fent servir la fórmula del teorema ix el sumatori:

$$a_n^{part} = \sum_{i=0}^{n-2}(n-i-1)2^{i+2} = \sum_{i=2}^{n}(n-i+1)2^i.$$

L'única dificultat és la suma $\sum_{i=2}^{n} i2^i$. Per a avaluar-la, fent servir la fórmula

$$\sum_{i=2}^{n} x^i = \frac{x^2 - x^{n+1}}{1-x}.$$

Si derivem respecte a x i després multipliquem per x queda:

$$\sum_{i=0}^{n} ix^i = x\frac{d}{dx}\left(\frac{x^2 - x^{n+1}}{1-x}\right) = x\frac{nx^{n+1} - (n+1)x^n - x^2 + 2x}{(1-x)^2}.$$

Substituïm la x pel valor 2 i obtenim el resultat. Després de realitzar tots els càlculs queda:

$$a_n^{part} = 4(2^n - 1 - n).$$

Forma general de les solucions

Proposició 2.5.2 *Siguen $\{x_n\}_{n=0}^{\infty}$ i $\{y_n\}_{n=0}^{\infty}$ dues solucions de l'equació en diferències finites*

$$a_{n+k} = c_0 a_n + c_1 a_{n+1} + \cdots + c_{k-1} a_{n+k-1} + \psi(n).$$

Llavors la successió $\{z_n\}_{n=0}^{\infty}$, amb $z_n = x_n - y_n$ és una solució de la recurrència lineal

$$a_{n+k} = c_0 a_n + c_1 a_{n+1} + \cdots + c_{k-1} a_{n+k-1}.$$

Demostració. Siga $z_n = x_n - y_n$, aleshores

$$\begin{aligned} c_0 z_n + c_1 z_{n+1} + \cdots + c_{k-1} z_{n+k-1} &= (c_0 x_n + c_1 x_{n+1} + \cdots + c_{k-1} x_{n+k-1}) - \\ &\quad -(c_0 y_n + c_1 y_{n+1} + \cdots + c_{k-1} y_{n+k-1}) \\ &= (x_{n+k} - \psi(n)) - (y_{n+k} - \psi(n)) \\ &= x_{n+k} - y_{n+k} = z_{n+k}. \end{aligned}$$

□

Corol·lari 2.5.3 (Solució general)
Donada $\{a_n^{(P)}\}_{n=0}^{\infty}$, una solució particular de l'equació lineal en diferències finites

$$a_{n+k} = c_0 a_n + c_1 a_{n+1} + \cdots + c_{k-1} a_{n+k-1} + \psi(n),$$

aleshores qualsevol altra solució $\{x_n\}_{n=0}^{\infty}$ es podrà expressar com la suma $\{a_n^{(H)} + a_n^{(P)}\}_{n=0}^{\infty}$ on $\{a_n^{(H)}\}_{n=0}^{\infty}$ és una solució de la llei de recurrència lineal d'ordre k,

$$a_{n+k} = c_0 a_n + c_1 a_{n+1} + \cdots + c_{k-1} a_{n+k-1}.$$

El superíndex (H) de la successió $\{a_n^{(H)}\}_{n=0}^{\infty}$ vol indicar que la successió és una solució de l'equació homogènia. Per això la "H".

Demostració. Siga x_n una solució qualsevol, aleshores $x_n = z_n + a_n^{(P)}$ on $z_n = x_n - a_n^{(P)}$. Segons la proposició anterior, z_n és solució de la recurrència lineal

$$a_{n+k} = c_0 a_n + c_1 a_{n+1} + \cdots + c_{k-1} a_{n+k-1}.$$

□

Per a resoldre una equació en diferències finites lineal hi ha prou amb trobar una solució particular i sumar-li una expressió de la part lineal amb coeficients arbitraris. Després s'ajusten els coeficients amb les condicions inicials.

Exemple 2.12 *Resoldre l'equació en diferències finites*

$$a_{n+2} = 2a_{n+1} - a_n + 2^{n+2}, \quad a_0 = 3, a_1 = -2.$$

La parte lineal ha estat estudiada anteriorment i la solució és

$$a_n^{(H)} = An + B$$

Una solució particular vista també en l'exemple anterior era

$$a_n^{(P)} = 4(2^n - 1 - n).$$

Per tant la solució general sería de la forma:

$$a_n = An + B + 4(2^n - 1 - n).$$

Fent servir ara les condicions inicials $a_0 = 3, a_1 = -2$, podem trobar A i B. Hem de resoldre

$$\begin{cases} 3 & = a_0 = A.0 + B + 4(2^0 - 1 - 0) = B, \\ -2 & = a_1 = A.1 + B + 4(2^1 - 1 - 1) = A + B. \end{cases}$$

Per tant, $A = -5, B = 3$, i així,

$$a_n = -5n + 3 + 4(2^n - 1 - n) = 2^{n+2} - 9n - 1.$$

2.5.3 *Algunes sumes que poden ser útils*

Tal com hem vist en els exemples anteriors, de vegades arribar al que s'anomena la forma tancada del terme general exigeix calcular una suma. Aixíque donarem acíles més comunes:

$$\begin{aligned}
\sum_{i=1}^{n} i &= \tfrac{n(n+1)}{2}, \\
\sum_{i=1}^{n} i^2 &= \tfrac{n(n+1)(2n+1)}{6}, \\
\sum_{i=0}^{n} x^i &= \tfrac{x^{n+1}-1}{x-1}, \quad \text{si } x \neq 1, \\
\sum_{i=0}^{n} i x^i &= \tfrac{nx^{n+2}-(n+1)x^{n+1}+x}{(x-1)^2}, \quad \text{si } x \neq 1, \\
\sum_{i=0}^{n} i^2 x^i &= \tfrac{n^2x^{n+3}-(2n^2+2n-1)x^{n+2}+(n^2+2n+1)x^{n+1}-x^2-x}{(x-1)^3}, \quad \text{si } x \neq 1.
\end{aligned}$$

2.6 Cercant solucions particulars

Ja sabem que la solució general d'una equació en diferències finites de coeficients constants és la suma de la solució de l'equació homogènia més una solució particular. Trobar la solució de l'equació homogènia és un procés ben clar. També hi ha un procés ben determinat per trobar una solució particular. Aquest segon procés, però, no dóna una expressió tancada. Hi ha casos en què podem trobar directament una solució particular.
Ho veurem amb un exemple. Volem trobar la solució general de

$$a_{n+1} - 2a_n + a_{n-1} = q^n \qquad (q \neq 1).$$

A la vista del membre de la dreta, no és del tot estrany provar amb una solució particular que siga proporcional a q^n. És a dir, provarem si hi ha alguna solució particular de la forma

$$a_n^{(P)} = Aq^n$$

amb A una constant que hem de determinar.
Substituint en l'equació s'obté

$$A\left(q^{n+1} - 2q^k + q^{n-1}\right) = q^n.$$

Simplificant,

$$A\left(q - 2 + \frac{1}{q}\right) = 1.$$

Per tant,

$$A = \frac{q}{q^2 - 2q + 1} = \frac{q}{(q-1)^2}$$

i així, una solució particular és

$$a_n^{(P)} = \frac{q}{(q-1)^2} q^n = \frac{q^{k+1}}{(q-1)^2}.$$

Com que la solució de l'equació homogènia és $a_n^{(H)} = c_1 + c_2 n$, aleshores la solució general de l'equació inicial és

$$a_n = a_n^{(H)} + a_n^{(P)} = c_1 + c_2 n + \frac{q^{n+1}}{(q-1)^2}.$$

Els paràmetres c_1 i c_2 es determinen finalment a partir de les condicions inicials.

Un altre exemple. Volem trobar ara la solució general de

$$a_{n+1} - 2a_n + a_{n-1} = n.$$

A la vista del membre de la dreta, no és del tot estrany novament provar amb una solució particular que siga proporcional a n. Ara bé, com ja ho hem vist, la solució de l'equació homogènia ja conté aquesta possibilitat. Així, provar amb $a_n = An$ no donarà res. Provarem doncs amb la menor potència de la possibilitat anterior que no estiga inclosa en la solució general. Provarem amb

$$a_n^P = An^2.$$

Substituint en l'equació s'obté

$$A\left((n+1)^2 - 2n^2 + (n-1)^2\right) = n.$$

Equivalentment,

$$A\left(n^2 + 2n + 1 - 2n^2 + n^2 - 2n + 1\right) = n,$$

$$A\,(2) = n,$$

i no ens ha quedat una solució constant per a A.
Provarem amb

$$a_n^P = An^3.$$

Substituint en l'equació s'obté

$$A\left((n+1)^3 - 2n^3 + (n-1)^3\right) = n.$$

Equivalentment,

$$A\left(n^3 + 3n^2 + 3k + 1 - 2n^3 + n^3 - 3n^2 + 3n - 1\right) = n,$$

$$A\,(6n) = n,$$

i ara síque tenim $A = \frac{1}{6}$. Aleshores la solució general de l'equació inicial és

$$a_n = a_n^{(H)} + a_n^{(P)} = c_1 + c_2 n + \frac{n^3}{6}.$$

2.7 Comentari final

Que una llei de recurrència no siga lineal no vol dir que no siga interessant, sinó que és molt més complicada. Ja no tenim cap ajuda per la banda de la teoria d'espais vectorials. Per exemple, la llei de recurrència de primer ordre donada per

$$z_{n+1} = z_n^2 + 1,$$

la definició de la qual és ben senzilla, dóna lloc a coses molt complicades. Per exemple, si la llei de recurrència es considera en el pla complex, aleshores apareix el conjunt de Mandelbrot, l'exemple de fractal per excel·lència. Aquest conjunt està definit com el conjunt dels nombres complexos z_0 tal que la successió generada per la llei de recurrència $z_{n+1} = z_n^2 + 1$, amb z_0 com a terme inicial, és convergent.

2.8 Exercicis

1. Calculeu el terme general de la successió definida per

   (a) $a_0 = 2, a_1 = 3, a_{n+2} = 3a_n - 2a_{n+1},\ (n = 0, 1, 2, \ldots)$,
   (Sol.: $a_n = \frac{1}{4}\left(9 - (-3)^n\right)$.)

(b) $a_0 = 0, a_1 = 1, a_{n+2} = 4a_{n+1} - 4a_n,\ (n = 0, 1, 2, \ldots)$.
(Sol.: $a_n = 2^{n-1}n$.)

2. Calculeu el terme general de la successió definida per

(a) $a_0 = -1, a_1 = 8, a_2 = 4, a_3 = 16, a_{n+4} = 8a_{n+2} - 16a_n,\ (n = 0, 1, 2, \ldots)$,
(Sol.: $a_n = (-2)^n n - 3(-2)^n + 2^{n+1}$.)

(b) $a_0 = 9, a_1 = -18, a_2 = 66, a_{n+3} = 2a_{n+2} + 5a_{n+1} - 6a_n,\ (n = 0, 1, 2, \ldots)$.
(Sol.: $a_n = 11(-2)^n + 3^{n+1} - 5$.)

3. En la successió $a_0, a_1, a_2, \ldots$, cada terme tret dels dos primers és la mitjana aritmètica dels dos precedents, així és, $a_{n+2} = \frac{a_{n+1}+a_n}{2}$. Determineu el límit $\lim_{n\to\infty} a_n$ com a funció de les condicions inicials a_0, a_1.
(Sol.: Com que $a_n = \frac{1}{3}a_0(-1)^n 2^{1-n} + \frac{a_0}{3} - \frac{1}{3}a_1(-1)^n 2^{1-n} + \frac{2a_1}{3}$, aleshores $\lim_{n\to\infty} a_n = \frac{a_0+2a_1}{3}$.)

4. Una matriu Q es pot escriure de la forma $Q = \mathrm{Id} + B$ on B és una matriu idempotent, és a dir, de les que verifiquen $B^2 = B$. Calculeu l'expressió general de Q^n.

5. Troba la solució general de

(a) $2y_{n+3} - 7y_{n+2} + 5y_{n+1} + 2y_n = 0$.
(b) $y_{n+3} - 5y_{n+2} + 8y_{n+1} - 4y_n = 0$.
(c) $y_{n+4} + y_n = 0$.
(d) $y_{n+2} + 2y_n + y_{n-2} = 0$.

6. Resoleu la relació de recurrència (no lineal) $a_{n+2} = \sqrt{a_{n+1}a_n}$ amb les condicions inicials $a_0 = 2, a_1 = 8$ i trobeu $\lim_{n\to\infty} a_n$.
(Sol.: Si calculeu els primers termes de la successió, s'observa que són de la forma $4 \cdot 2^p$, amb p un racional. Si posem, per tant, que $a_n = 4 \cdot 2^{b_n}$, aleshores la relació de recurrència no lineal es transforma en una altra sobre la successió dels exponents, b_n, la qual síque és lineal. La resposta final és $\lim_{n\to\infty} a_n = 4 \cdot 2^{\frac{1}{3}}$.
Més elegant encara és considerar la successió $b_n = \log_2 a_n$ i aplicar l'exercici 3.)

7. Ja sabem que la successió de Fibonacci, $\{F_n\}_{n=0}^{\infty}$, està definida per la relació de recurrència

$$F_{n+2} = F_{n+1} + F_n.$$

També verificarà la llei de recurrència següent:

$$F_{n+3} = F_{n+2} + F_{n+1} = F_{n+1} + F_n + F_{n+1} = 2F_{n+1} + F_n.$$

Comproveu que la successió definida per la llei de recurrència

$$a_{n+3} = 2a_{n+1} + a_n,$$

i amb les condicions inicials

$$a_0 = 1, \quad a_1 = 1, \quad a_2 = 2,$$

és la successió de Fibonacci, és a dir, que

$$a_n = F_n.$$

8. Considerem, per a cada $n > 0$, la matriu

$$M_n = \begin{pmatrix} 2 & -1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 2 & -1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 2 & -1 & \dots & 0 & 0 \\ 0 & 0 & 1 & 2 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 2 & -1 \\ 0 & 0 & 0 & 0 & \dots & 1 & 2 \end{pmatrix}$$

Comproveu que

$$|M_n| = \frac{2+\sqrt{2}}{4}(1+\sqrt{2})^n + \frac{2-\sqrt{2}}{4}(1-\sqrt{2})^n.$$

9. Considerem, per a cada $n > 0$, la matriu

$$M_n = \begin{pmatrix} 2 & 3 & 0 & 0 & \dots & 0 & 0 \\ 1 & 2 & 3 & 0 & \dots & 0 & 0 \\ 0 & 1 & 2 & 3 & \dots & 0 & 0 \\ 0 & 0 & 1 & 2 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 2 & 3 \\ 0 & 0 & 0 & 0 & \dots & 1 & 2 \end{pmatrix}$$

Comproveu que

$$|M_n| = \frac{2-\mathbf{i}\sqrt{2}}{4}(1+\mathbf{i}\sqrt{2})^n - \frac{2+\mathbf{i}\sqrt{2}}{4}(1-\mathbf{i}\sqrt{2})^n.$$

10. Considerem, per a cada $n > 0$, la matriu

$$M_n = \begin{pmatrix} 2 & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & \dots & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 & 2 \end{pmatrix}$$

(a) Comproveu que si $D_n = \det(M_n)$, aleshores la successió $\{D_n\}_{n=1}^{\infty}$ verifica, per a tot $n \in \mathbb{N}$,

$$D_{n+4} = 2D_{n+3} - 2D_{n+1} + D_n.$$

(b) Comproveu que les arrels de l'equació associada són 1, arrel triple, i -1.

(c) Demostreu després que

$$D_n = |M_n| = \frac{2n^2 + 8n + 7 + (-1)^n}{8}.$$

(d) Calculeu D_{50} segons la fórmula i, d'una altra banda, intenteu calcular, amb algun programa informàtic de cálcul simbòlic, el valor del determinant de la matriu M_{50}.

11. Trobeu la funció generatriu de la successió definida per la recurrència

$$a_n = 5a_{n-1} - 6a_{n-2},$$

amb les condicions inicials $a_0 = 1, a_1 = 2$.

12. Trobeu la quantitat de successions formades per n lletres del conjunt $\{a, b, c, d\}$ de manera que a mai siga adjacent a b.

(Sol.: Siga a_n la quantitat de successions formades per n lletres del conjunt $\{a, b, c, d\}$ que comencen per a i en les quals a mai siga adjacent a b. Si la llista de n lletres acaba en d o c, la quantitat d'ells és a_{n-1} ja que l'anterior pot ser qualsevol lletra. Llavors d'aqueix tipus hi ha $2a_{n-1}$. Si els a_n buscats acaben en a, l'anterior necessàriament ha d'acabar en a, c o d. Per tant són $3a_{n-2}$. Notar que és el mateix si acaba amb b. Per tant:

$$a_n = 2a_{n-1} + 6a_{n-2}.$$

L'equació associada és $x^2 - 2x - 6 = 0$, les arrels de la qual són $1 \pm \sqrt{7}$. Mentre que les condicions inicials són $a_1 = 4, a_2 = 14$, la solució és

$$a_n = A\left(1 + \sqrt{7}\right)^n + B\left(1 - \sqrt{7}\right)^n.$$

Falta calcular les constants usant les condicions inicials)

13. Demostreu que el nombre real $(6 + \sqrt{37})^{999}$ s'escriu amb 999 zeros a la dreta del punt decimal.

(Sol.: Considereu la successió de terme general $a_n = (6 + \sqrt{37})^n + (6 - \sqrt{37})^n$ la qual verifica la relació de recurrència $a_{n+2} = 12a_{n+1} + a_n$ amb condicions inicials $a_0 = 2, a_1 = 12$. Per tant, a_n sempre és un nombre enter. Finalment, a partir de $\sqrt{37} - 6 < 0.1$, s'obté el resultat.

14. Exercici extret d'un llibre de divulgació matemàtica (*El prodigio de los números*, de Clifford A. Pickover, Ed. RBA, 2007).

Els veïns del senyor Fibonacci

Si calculem l'expressió decimal de $\frac{1}{89}$, obtenim

$$0.011235955056179775\ldots$$

que és el mateix resultat que la suma següent definida a partir dels nombres de Fibonacci

$$\begin{aligned} F_1 = 1 &\mapsto 0.01, \\ F_2 = 1 &\mapsto 0.001, \\ F_3 = 2 &\mapsto 0.0002, \\ F_4 = 3 &\mapsto 0.00003, \\ F_5 = 5 &\mapsto 0.000005, \\ F_6 = 8 &\mapsto 0.0000008, \\ F_7 = 13 &\mapsto 0.00000013, \\ F_8 = 21 &\mapsto 0.000000021, \\ &\ldots \\ &\quad 0.01123595\ldots \end{aligned}$$

El llibre planteja com demostrar això. Doncs bé, si denotem[1]

$$X = \sum_{n=1}^{\infty} \frac{F_n}{10^{n+1}},$$

tenim que

$$\begin{aligned} 89 \cdot X &= (100 - 10 - 1) \cdot X \\ &= 100 \textstyle\sum_{n=1}^{\infty} \frac{F_n}{10^{n+1}} - 10 \sum_{n=1}^{\infty} \frac{F_n}{10^{n+1}} - \sum_{n=1}^{\infty} \frac{F_n}{10^{n+1}} \\ &= \textstyle\sum_{n=1}^{\infty} \frac{F_n}{10^{n-1}} - \sum_{n=1}^{\infty} \frac{F_n}{10^{n}} - \sum_{n=1}^{\infty} \frac{F_n}{10^{n+1}} \\ &= F_1 + \frac{F_2}{10} + \textstyle\sum_{n=3}^{\infty} \frac{F_n}{10^{n-1}} - \frac{F_1}{10} - \sum_{n=2}^{\infty} \frac{F_n}{10^{n}} - \sum_{n=1}^{\infty} \frac{F_n}{10^{n+1}} \\ &= F_1 + \frac{F_2}{10} + \textstyle\sum_{n=1}^{\infty} \frac{F_{n+2}}{10^{n+1}} - \frac{F_1}{10} - \sum_{n=1}^{\infty} \frac{F_{n+1}}{10^{n+1}} - \sum_{n=1}^{\infty} \frac{F_n}{10^{n+1}} \\ &= F_1 + \frac{F_2}{10} - \frac{F_1}{10} + \textstyle\sum_{n=1}^{\infty} \frac{F_{n+2} - F_{n+1} - F_n}{10^{n+1}} \\ &= F_1 = 1. \end{aligned}$$

Per tant, $X = \frac{1}{89}$.

15. Siga $\{a_n\}_{n=0}^{\infty}$ una successió definida per $a_{n+2} = c_1 a_{n+1} + c_2 a_n$ on c_1 i c_2 són dues constants que verifiquen $D = c_1^2 + 4c_2 = 0$. Demostreu que si $a_0 = \alpha_0$ i $a_1 = \alpha_1$, aleshores

$$a_n = \alpha_0 \left(\frac{c_1}{2}\right)^n + n \left(\alpha_1 - \frac{\alpha_0 c_1}{2}\right)^n \left(\frac{c_1}{2}\right)^{n-1}.$$

[1] Tenint en compte la funció generatriu de la successió de Fibonacci, $X = \frac{1}{10} F\left(\frac{1}{10}\right)$.

16. Trobeu el terme general de la successió de nombres de Lucas definits en (2.2).

    (Sol.: $L_n = \sigma^n + \overline{\sigma}^n$, on $\sigma = \frac{1+\sqrt{5}}{2}$ és la raó àuria i $\overline{\sigma} = \frac{1-\sqrt{5}}{2}$ la seua conjugada.)

17. Demostra que els nombres de Fibonacci verifiquen

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \sigma \qquad \text{i} \qquad \lim_{n\to\infty} \frac{F_n}{F_{n+1}} = \overline{\sigma}.$$

18. Una variació de la successió de Fibonacci és l'anomenada successió de Pell. És aquella que verifica la relació de recurrència $P_{n+2} = 2P_{n+1} + P_n$ i té com a condicions inicials $P_0 = 0, P_1 = 1$. Demostra que

$$\lim_{n\to\infty} \frac{P_{n+1}}{P_n} = 1 + \sqrt{2}, \quad \text{la } \textbf{raó de plata}.$$

19. Ja coneixem de sobres que la raó àuria està relacionada amb la successió de Fibonacci. Aquesta està definida per la llei de recurrència que diu que cada terme de la successió és la suma dels dos anteriors: $a_{n+2} = a_{n+1} + a_n$. Si en comptes de definir una successió d'eixa forma, ho haguèrem fet dient que cada terme és la suma següent:

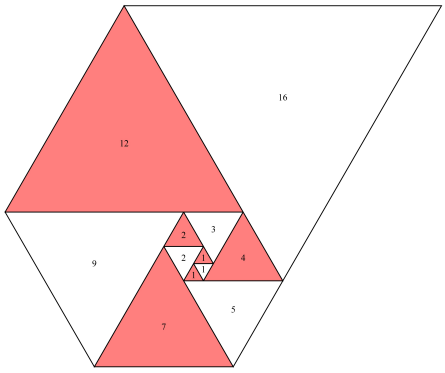
$$a_{n+3} = a_{n+1} + a_n,$$

    aleshores les coses canvien un poc.

    Definim la **constant plàstica**, ρ, com a l'única solució real de l'equació $x^3 = x + 1$. Les altres dues solucions són complexos α i $\overline{\alpha}$ on $|\alpha| < 1$.

    Definim també la successió de Padovan, $\{P_n\}_{n=0}^{\infty}$, com aquella que verifica la relació de recurrència $P_{n+3} = P_{n+1} + P_n$ i té com a condicions inicials $P_0 = P_1 = P_2 = 1$. Demostra que

$$\lim_{n\to\infty} \frac{P_{n+1}}{P_n} = \rho.$$



Espiral del primers triangles equilàters que tenen per costat el corresponent terme de la successió de Padovan.

20. (Matemàtica financera) Calcula el TAE (Taxa anual equivalent) corresponent a un interés compost del 10% anual amb pagaments mensuals.

    (Sol.: Suposem que el capital inicial de la inversió és C i siga a_n el capital després de n mesos. Aleshores la llei de recurrència és

    $$a_{n+1} = a_n + a_n \cdot \frac{10}{100} \cdot \frac{1}{12} = a_n \cdot \left(1 + \frac{1}{120}\right).$$

    El terme general d'aquesta successió és

    $$a_n = a_0 \cdot \left(1 + \frac{1}{120}\right)^n.$$

    Per tant, per a calcular la solució fem

    $$\left(1 + \frac{1}{120}\right)^{12} - 1 \sim 0.10471,$$

    i això vol dir que la TAE és 10.471.)

21. Resoleu

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

    amb les condicions inicials $a_0 = 2, a_1 = -3$.

22. Trobeu la solució general de la recurrència

    $$a_n = 5a_{n-1} - 6a_{n-2}.$$

    (Sol.: $a_n = A \cdot 2^n + B \cdot 3^n$.)

23. Trobeu una solució particular de l'equació en diferències finites

    $$a_{n+2} = 5a_{n+1} - 6a_n + (n+2)3^{n+2}.$$

    (Sol.: $a_n = -9 \cdot 2^n + \frac{1}{2}(6 - 3n + n^2) \cdot 3^{n+1}$.)

24. Resoleu l'equació en diferències finites

    $$a_{n+2} = 5a_{n+1} - 6a_n + (n+2)3^{n+2}$$

    amb les condicions inicials $a_0 = 1, a_1 = 2$.
    (Sol.: $a_n = -2^{n+3} + \frac{1}{2}(6 - 3n + n^2) \cdot 3^{n+1}$.)

25. Equacions en diferències finites de primer ordre, lineals i de coeficients variables.

    Una de les solucions explícites que hem vist d'equacions en diferències finites és el cas d'equacions de primer ordre, lineals i de coeficients constants (vegeu l'eq. (2.6)).

    En aquest exercici veurem les de coeficients variables:

$$x_{n+1} = a_n\, x_n + b_n, \qquad n = 0, 1, \ldots, \tag{2.9}$$

    on $\{a_n\}_{n\geq 0}$ i $\{b_n\}_{n\geq 0}$ són dues successions, conegudes, de nombres reals.

    Demostreu que l'única solució de l'equació (2.9) amb la condició inicial $x_0 = d$ està donada per

$$x_n = \left(\prod_{i=0}^{n-1} a_i\right) d + \sum_{k=0}^{n-1} \left(\prod_{i=k+1}^{n-1} a_i\right) b_k, \qquad n = 0, 1, \ldots$$

    on, per conveni,

$$\prod_{i=0}^{-1} a_i = 1, \prod_{i=n}^{n-1} a_i = 1.$$

    Comproveu, en aplicar el resultat anterior, que la solució de

$$x_{n+1} = \frac{2n+1}{2n+3} x_n + r, \qquad n = 0, 1, \ldots$$

    amb la condició inicial $x_0 = d$, està donada per

$$x_n = \frac{d + (n^2 + 2n)r}{2n+1}.$$

26. Trobeu la solució general de les equacions en diferències finites de primer ordre, lineals i de coeficients variables següents:

    (a) $x_{n+1} = \frac{n+2}{n+1} x_n,\ n = 0, 1, \ldots$

    (b) $x_{n+1} = \frac{n+1}{n+2} x_n,\ n = 0, 1, \ldots$

    (c) $x_{n+1} = -e^{-n} x_n,\ n = 0, 1, \ldots$

    (d) $x_{n+1} = \frac{\ln(n+1)}{\ln(n+2)} x_n,\ n = 0, 1, \ldots$

27. Troba una solució particular de

    (a) $a_{n+1} - 2a_n + a_{n-1} = \sin(cn)$.

    (b) $a_{n+1} - 2a_n + a_{n-1} = e^{bn}, \qquad b \neq 0$.

    (c) $a_{n+1} - 2a_n + a_{n-1} = 1$.

    (d) $a_{n+1} - 2a_n + a_{n-1} = ne^{bn}, \qquad b \neq 0$.

28. Comprova que la funció generatriu de la successió definida per

$$a_{n+2} - 2a_{n+1} + a_n = 1$$

amb condicions inicials $a_0 = 1, a_1 = 0$ és

$$\phi(x) = \frac{1 - 3x + 3x^2}{(1-x)^3}.$$

29. Comprova que la funció generatriu de la successió definida per

$$D_{n+2} = bD_{n+1} - acD_n, \qquad b^2 \neq 4ac,$$

amb condicions inicials $D_0 = 1, D_1 = b$ és

$$f(x) = \frac{1}{1 - bx + acx^2}.$$

30. Si la successió

$$1, 4, 12, 32, 80, 192, \ldots$$

té com a funció generatriu $f(x) = \dfrac{1}{(1-2x)^2}$, quina serà la funció generatriu de la successió

$$0, 1, 4, 12, 32, 80, 192 \ldots ?$$

I la de

$$1, -4, 12, -32, 80, -192, \ldots ?$$

31. Dos jugadors, un amb m monedes, l'altre amb n, fan apostes llançant una moneda a l'aire. Les apostes són d'una moneda cadascun d'ells. El joc s'acaba quan un dels dos jugadors es queda amb tots els diners. Quina és la probabilitat de que guanye el primer jugador?

Si p_k representa la probabilitat de que guanye el primer jugador quan aquest té inicialment k monedes, comprova primer que

$$p_k = \frac{p_{k+1} + p_{k-1}}{2}.$$

Comproveu també que tenim les condicions (no inicials!)

$$p_0 = 0, \qquad p_{m+n} = 1.$$

Determineu el terme general p_k i el terme p_m.

32. Denotem per $r_n = \frac{F_n}{F_{n+1}}$ el quocient entre dos termes consecutius de la successió de Fibonacci. Demostreu primer que la successió $\{r_k\}_{k=0}^{\infty}$, satisfà la llei de recurrència no lineal

$$r_k = \frac{1}{1 + r_{k-1}}$$

amb la condició inicial $r_0 = 0$.

Demostra, per tant, que

$$\frac{\sqrt{5}-1}{2} = \frac{1}{1 + \frac{1}{1+\frac{1}{1+\dots}}}$$

3. Teoria elemental de grafs

La teoria de grafs ha tingut, en els últims anys, un gran desenvolupament probablement a causa de l'enorme quantitat d'aplicacions que aquests tenen. Té el seu inici en 1736 quan Leonhard Euler[1] va publicar *Solutio problematis and geometrian situs pertinentisen* on apareix la solució al famós problema dels Ponts de Königsberg. Durant el segle XIX la teoria de grafs va tornar a l'actualitat gràcies a l'estudi de diversos problemes obtenint així més resultats importants. Per exemple, Arthur Cayley[2] en 1857, mentre estudiava la quantitat possible que podia haver-hi de certes estructures químiques, va descobrir una important família de grafs, a les quals va anomenar arbres. Encara que a poc a poc anava augmentant l'interés en aquesta àrea, va anar fins a 1936 quan l'hongarés Dénes König[3] va publicar el primer llibre sobre aquest tema. Podem dir que la Teoria de grafs és una àrea molt jove dins del món de les matemàtiques, sobretot si la comparem amb l'antiguitat d'altres àrees com la Geometria o l'Àlgebra.

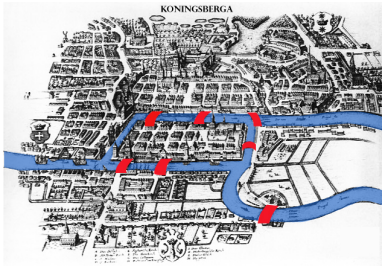
Els grafs són extremadament útils per a representar primer, i després analitzar, problemes molt diversos. Informalment, un graf és una col·lecció de vèrtexs, a la qual acompanya un conjunt d'arestes que relacionen aquests vèrtexs. Quan argumentem amb grafs és habitual dibuixar els vèrtexs com a punts (o xicotets cercles) sobre el pla, i representar les arestes com a línies que uneixen aquests punts. Per a comprovar l'àmplia capacitat de representació del llenguatge dels grafs, exhibim un exemple, el més famós, que analitzarem amb detall més endavant, el dels ponts de Königsberg.

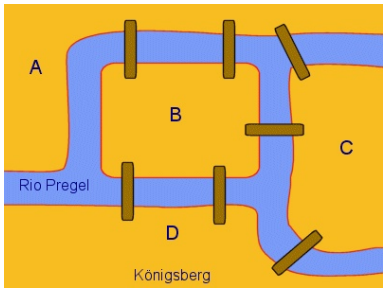
En un dels seus viatges, Euler va visitar una ciutat llavors prussiana anomenada Königbserg (avui anomenada Kaliningrad), es troba situada en els voltants de la mar Bàltica, pertany a Rússia i manté fronteres amb Lituània i amb Polònia, i és travessada pel riu Pregolya, en alemany Pregel. En l'època d'Euler, aquest riu separava tres zones de terra, les marcades en el dibuix com A, C i D, deixant un illot, anomenat Kneiphof marcat com B en el dibuix. A més, entre l'illa Keneiphof i les altres zones de terra hi havia 7 ponts, com els que mostra el dibuix, que les connectaven. El problema consistia a determinar si una persona era capaç de realitzar un passeig de tal manera que creuara tots els ponts una única vegada i a més acabara el seu passeig en la mateixa zona de la qual va partir.

[1] L. Euler, *Solutio problematis and geometrian situs pertinentis, Commentarii Academiae Scientiarum Imperialis Petropolitanae* 8 (1736), 128-140

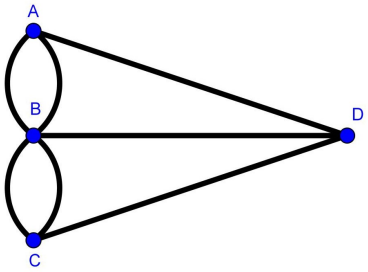
[2] A. Cayley, On the theory of the analytical forms called trees, Philosophical Magazine (4) 13 (1857), 172-176

[3] D. König, Theorie der endlichen und unendlichen Graphen, Akademische Verlagsgesells-chaft, Leipzig, 1936





Euler, en 1736, va publicar la resposta a aquesta pregunta. Per a resoldre el problema va realitzar el que avui dia es coneix com un model matemàtic. En aquest representava a cadascuna de les illes i a les dues riberes per un vèrtex i va posar una aresta per a cada pont. D'aquesta forma va obtindre el diagrama que apareix en la figura següent. No és difícil veure que resoldre el problema dels Ponts de Königsberg és equivalent a realitzar el dibuix, del diagrama associat al problema, sense alçar el llapis del paper ni traçar dues vegades la mateixa línia.



Després d'un estudi minuciós sobre les condicions que ha de complir el diagrama perquè existisca un recorregut amb aquestes característiques, Euler dedueix que perquè aquest recorregut siga possible és necessari que tots els vèrtexs en el diagrama siguen incidents amb un nombre parell de línies. Com que en el diagrama tots els vèrtexs tenen un nombre imparell de línies es conclou que no existeix una solució al problema dels ponts de Königsberg. L'anàlisi i la solució a aquest problema es detallen en la Secció 3.1 del Capítol 3.

Hui dia, una representació com la dels ponts de Königsberg es diu graf. Gustav Kirchhoff, que va nàixer a Königsberg, va utilitzar esquemes tipus graf en la seua teoria de circuits en 1847, Cayley va usar els grafs per a classificar isòmers d'un compost orgànic. Hui dia s'usen en investigació operativa, en dissenys d'algorismes i en multitud de camps de les ciències pures així com de les ciències socials.

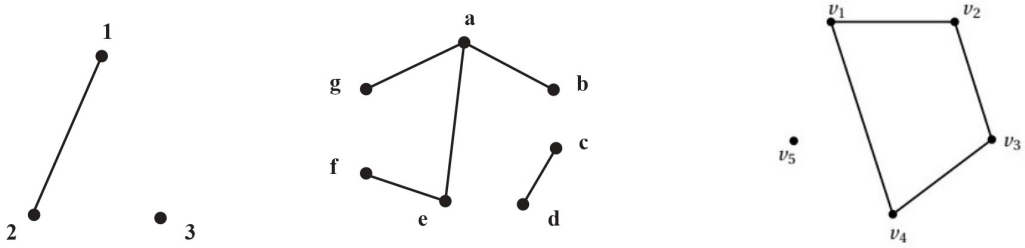
3.1 Noció de graf. Isomorfisme. Grafs complets

Definició 3.1.1 *Un graf G és una estructura formada per un conjunt no buit $V = V(G)$ els elements del qual són anomenats vèrtexs, i un conjunt $A = A(G)$ de parells no ordenats de vèrtexs anomenats arestes. Per comoditat, una aresta $\{u, v\}$ serà denotada per uv, on $u, v \in V$.*

Exemple 3.1 *1. Considerem $V = \{1, 2, 3\}$ i $A = \{\{1, 2\}\}$, aleshores $G = (V, A)$ és un graf.*

2. *Considerem* $V = \{a, b, c, d, e, f, g\}$ *i* $A = \{\{a, b\}, \{c, d\}, \{e, f\}, \{a, g\}, \{a, e\}\}$*, aleshores* $G = (V, A)$ *és un graf.*

Un graf es pot representar geomètricament mitjançant un dibuix, en el qual els vèrtexs són punts i les arestes són línies que connecten als punts. Es pot observar que el dibuix del graf determina completament el graf. Per exemple, els grafs del exemple anterior i el graf G definit per $V = \{v_1, v_2, v_3, v_4, v_5\}$ i $A = \{v_1v_2, v_1v_4, v_2v_3, v_3v_4\}$ es pot representar mitjançant els dibuixos que apareixen en la figura següent:



La definició de graf es pot ampliar si es permeten llaços, és a dir, arestes de la forma uu, i arestes paral·leles entre parells de vèrtexs. A un graf amb llaços i arestes paral·leles se'l coneix com *multigraf*. També, si es consideren direccions en les arestes, llavors estem parlant de **grafs dirigits**. Direm que un graf és **simple** si no conté llaços ni arestes paral·leles, i tampoc arestes dirigides. Llevat que s'esmente el contrari, en aquest tema només treballarem amb grafs simples.

Ni llaços ni arestes múltiples

Donat un graf $G = (V, A)$, si $\{u, v\} \in A$, aleshores direm que u i v són adjacents, o que són veïns, o que són amics.

Definició 3.1.2 *Donat* $u \in V$*, el grau del vèrtex* u *és la quantitat d'amics que té.*

Exemple 3.2 *En l'exemple anterior, el grau de* c *és* 1*, el de* a *és* 3 *i el de* e *és* 2*. El grau del vèrtex* 3 *és* 0*.*

Un dels primers resultats bàsics sobre els grafs simples és el lema conegut com el Lema de l'Encaixada. Es pot formular de la següent forma:

En tota festa el nombre total de mans que s'estrenyen quan les persones se saluden és parell.

És un resultat que relaciona el nombre d'arestes d'un graf i els graus dels seus vèrtexs. Si sumem els graus de tots els vèrtexs d'un graf, es pot veure que cada aresta uv es compta dues vegades (una vegada quan comptem el grau de u i una altra quan comptem el grau de v).
O bé, si tenim el graf sense cap aresta i volem posar-les totes en la seua posició, cada vegada que posem una aresta nova, afegim un grau a cadascun dels seus extrems. Per tant, la suma total de graus es veu incrementada en dos. Quan acabem de posar-les totes, la suma total de graus haurà passat de 0 fins al doble de les arestes que hàgem posat.

Lema 3.1.3 *(Lema de l'Encaixada)*
Donat un graf $G = (V, A(G))$, sense llaços però on poden haver-hi arestes múltiples, amb m arestes, és a dir $|A(G)| = m$, es té

$$\sum_{v \in V} grau(v) = 2m.$$

Demostració. Procedirem per inducció sobre el nombre de vèrtexs, n. Per a $n = 1$, el teorema és trivial ja que, en no haver-hi llaços, el grau de l'únic vèrtex és 0 que coincideix amb el doble del nombre d'arestes, que també és zero.
Suposem que la proposició és certa per a n vèrtexs. Per a això considerem dos grafs G i H els conjunts de vèrtexs de la qual són respectivament $\{v_1, \ldots, v_n\}$ i $\{v_1, \ldots, v_n\} \cup \{a\}$. Així mateix el conjunt d'arestes de H estarà format per les de G juntament amb les arestes incidents amb el vèrtex a.
Descomponguem el conjunt V en dos subconjunts A i B, sent A el conjunt de vèrtexs que tinguen una aresta que siga incident amb a i B la resta dels vèrtexs de V. És evident que A i B són disjunts i que la seua unió és V.

$$\sum_{x \in V(G)} grau_H(x) = \sum_{x \in A} grau_H(x) + \sum_{x \in B} grau_H(x).$$

Si $x \in A$ llavors $grau_H(x) = grau_G(x) + x(a)$, sent $grau_G(x)$ el grau de x en el graf G i $x(a)$ el nombre d'arestes incidents amb x i a en el graf H. Si $x \in B$ llavors $grau_H(x) = grau_G(x)$. Es té per tant:

$$\sum_{x \in V(G)} grau_H(x) = \sum_{x \in A} (grau_G(x) + x(a)) + \sum_{x \in B} grau_G(x) = \sum_{x \in A \cup B} grau_G(x) + \sum_{x \in A} x(a).$$

Si fem valdre la hipòtesi d'inducció i $A(G)$ és el conjunt d'arestes del graf G, $A(H)$ el conjunt d'arestes del graf H, el primer sumand és justament $2|A(G)|$, el segon sumand és simplement el grau de a, $grau_H(a)$. Per tant

$$\sum_{x \in V(G)} grau_H(x) = 2|A(G)| + grau_H(a).$$

Tenim finalment:

$$\begin{aligned} \sum_{x \in V(H)} grau(x) &= \sum_{x \in V(G)} grau_H(x) + grau_H(a) \\ &= 2|A(G)| + grau_H(a) + grau_H(a) \\ &= 2(|A(G)| + grau_H(a)) = 2|A(H)|. \end{aligned}$$

□

Com a conseqüència directa, tenim

Corol·lari 3.1.4 *En tot graf simple el nombre de vèrtexs de grau imparell és parell.*

Demostració. Suposem que l'afirmació és falsa: la suma dels graus per als vèrtexs de grau imparell donaria un nombre imparell, ja que la suma d'una quantitat imparella de nombres imparells és imparella. En el còmput total dels graus, els vèrtexs de grau parell contribueixen en una quantitat parella, per la qual cosa la suma total dels graus donaria un nombre imparell, en contradicció amb la proposició anterior. □

Podem assegurar, per exemple, que la quantitat de persones que, des que el món és món, han xocat la mà amb una altra diferent un nombre imparell de vegades és parell.

Exemple 3.3 *Pot haver-hi un graf simple en què els graus de tots els vèrtexs siguen*

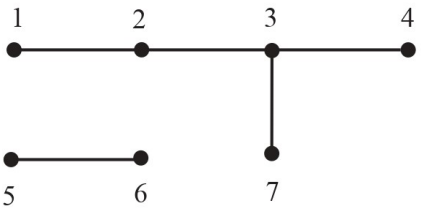
$$\{1, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5, 5, 5\}?$$

Resposta: Clarament no, ja que hi ha 9 vèrtexs de grau imparell.

Exemple 3.4 *Pot haver-hi un graf simple els graus del qual de tots els vèrtexs siguen* $\{1, 2, 3, 5, 7\}$*?*
No, ja que per a 5 vèrtexs el grau màxim possible en un graf simple és 4 i hi ha almenys dos vèrtexs amb graus majors que 4.

Definició 3.1.5 (Isomorfisme de grafs)
Donats els grafs $G = (V(G), A(G))$ *i* $H = (V(H), A(H))$*, es diu que són isomorfs si existeix una aplicació bijectiva* $f : V(G) \to V(H)$ *que respecte les arestes, això és: si* u *i* v *són dos vèrtexs qualssevol de* $V(G)$ *que siguen extrems de* p *arestes diferents de* $A(G)$*, llavors existeixen exactament* p *i solament* p *arestes diferents en* $A(H)$ *de les quals* $f(u)$ *i* $f(v)$ *són extrems. Si no hi ha cap aresta de la qual* u *i* v *són extrems, llavors tampoc existeix cap aresta en* $A(H)$ *de la qual* $f(u)$ *i* $f(v)$ *són extrems.*
Equivalentment, es pot dir que: $\{u, v\} \in A(G) \iff \{f(u), f(v)\} \in A(H)$*. (És a dir, si* f *conserva les relacions de veïnatge entre vèrtexs)*

Exemple 3.5 *El graf següent*



és isomorf al de la figura anterior centre. L'isomorfisme està donat per:

$$a \to 3, b \to 4, c \to 5, d \to 6, e \to 2, f \to 1, g \to 7.$$

En general, no és fàcil comprovar si dos grafs són isomorfs o no. En els casos senzills, si els dos grafs són isomorfs, es pot trobar la bijecció a "ull". Quan el conjunt de vèrtexs del graf és gran, és més complicat trobar una bijecció. No obstant això, comptem amb unes certes propietats d'un graf per a saber si dos grafs no són isomorfs:

- Ambdós grafs han de tindre el mateix nombre de vèrtexs (si no el tenen, no podrem construir una bijecció entre els conjunts de vèrtexs).
- Conservació de la relació de veïnatge: si $G = (V(G), A(G))$ i $H = (V(H), A(H))$ són isomorfs mitjançant f, llavors, per a cada $o \in V(G)$:

  $$\text{grau}(u) = \text{grau}(f(u)).$$

  f és una bijecció que conserva l'adjacència: el nombre de vèrtexs adjacents a u en G ha de ser el mateix que el de vèrtexs adjacents a $f(u)$ en H; per tant, el nombre d'arestes amb extrem en u ha de coincidir amb el nombre d'arestes amb extrem en $f(u)$ i, conseqüentment, els seus graus seran iguals.
  Si, per exemple, en un graf tenim un vèrtex de grau 5 i en l'altre no, no podran ser isomorfs.

- Com que sabem que en tot graf la suma dels graus és igual a dues vegades el nombre d'arestes, deduïm que dos grafs isomorfs han de tindre el mateix nombre d'arestes.

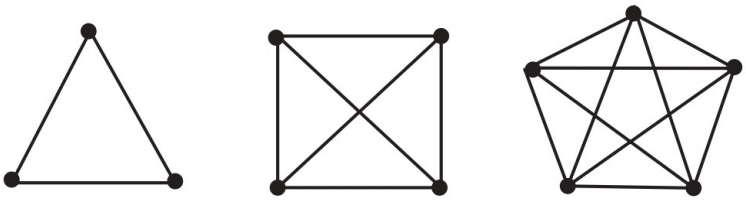
Exemple 3.6 *Considerem els dos grafs següents:*

Tots dos grafs tenen sis vèrtexs, cinc arestes i la seua successió de graus és $(1, 1, 1, 2, 2, 3)$. *No obstant això, no són isomorfs perquè, per exemple, el vèrtex de grau 3 és, en un cas, veí de dos de grau 1 i d'un de grau 2; i en l'altre, d'un de grau 1 i de dos de grau 2.*

Definim ara els *grafs complets*.

Definició 3.1.6 *Denotarem per* K_n *el graf complet amb* n *vèrtexs. És a dir:*

$$K_n = (\{1, 2, \ldots, n\}, \{\{i, j\}, \quad 1 \leq i < j \leq n\}).$$



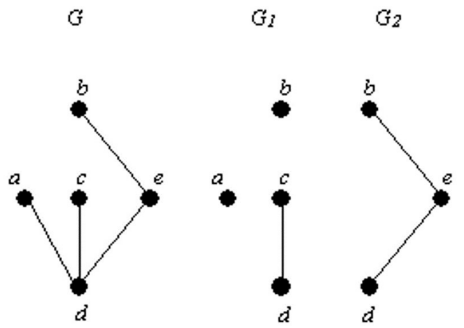
Els grafs complets K_3, K_4 i K_5

Noteu que en un graf complet regna l'harmonia perfecta. Tots són amics de tots.

3.2 Subgrafs, matriu d'adjacència i grafs connexos

Definició 3.2.1 (Subgraf - Subgraf induït)
Siguen $G = (V, A)$ *i* $G' = (V', A')$ *dos grafs. Direm que* G *és un subgraf de* G' *si* $V \subset V'$ *i* $A \subset A'$.
Direm que G *és un subgraf induït de* G' *si* $V \subset V'$ *i si les arestes de* G *són només les arestes de* G' *que connecten vèrtexs de* V*, és a dir,* $A = \{\{a, b\} \in A' : a, b \in V\}$.

Exemple 3.7 *Pels subgrafs de la figura següent, veiem que* G_2 *és un subgraf induït de* G *però el subgraf* G_1 *no és un subgraf induït ja que no apareix l'aresta* ad.



Ara veurem com podem representar els grafs simples mitjançant matrius. A partir d'aquestes matrius podrem obtindre propietats sobre els grafs.

Donat un graf $G = (V, A)$, podem crear una matriu quadrada $n \times n$, que anomenarem **matriu d'adjacència**. Si denotem per A_G aquesta matriu, llavors l'element de la fila i i la columna j vindrà donat pel nombre d'arestes que siguen adjacents a tots dos vèrtexs. Per a un graf simple, aquest valor serà sempre 0 o 1.

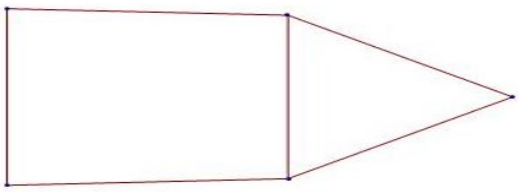
Definició 3.2.2 *Siga $G = (V, A)$ un graf amb n vèrtexs. Denotem els vèrtexs per $v_1, v_2, \ldots, v_n$. La matriu d'adjacència de G, respecte de l'ordenació triada per als vèrtexs, és la matriu quadrada $n \times n$, $A_G = (a_{ij})$ definida per*

$$a_{ij} = \begin{cases} 1 & \textit{si} \quad v_i v_j \in A, \\ 0 & \textit{en un altre cas.} \end{cases}$$

Exemple 3.8 *Per exemple, pensem com seria el graf corresponent a aquesta matriu:*

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

La solució és el següent graf



Moltes propietats es poden obtenir a partir de la matriu d'adjacència d'un graf. La matriu d'adjacència d'un graf simple sempre serà simètrica, amb zeros en la diagonal. Notar també que si sumem els elements d'una determinada fila obtenim el grau del vèrtex corresponent a aqueixa fila. A més, les potències de la matriu d'adjacència compleixen una interessant propietat. Per a enunciar-la, necessitem definir la noció de camí i la seua longitud.

Definició 3.2.3 *Siga $G = (V, A)$ un graf. Un camí en el graf G és una successió de vèrtexs*

$$v_0, v_1, \ldots, v_n$$

tal que per a tot $i = 1, 2, \ldots, n$, $v_{i-1}v_i \in A$. El nombre natural n s'anomena **longitud** *del camí, ja que és la quantitat d'arestes d'aquest.*

El següent resultat ens mostra la importància de les matrius d'adjacència.

Proposició 3.2.4 *Siga $G = (V, A)$ un graf amb conjunt de vèrtexs $\{v_1, v_2, \ldots, v_n\}$ i siga A_G la seua matriu d'adjacència. Siga $(A_G)^k$ la potència k-èsima de la matriu d'adjacència. Siga $a_{ij}^{(k)}$ l'entrada i, j de la matriu $(A_G)^k$. Aleshores, el nombre de camins (es poden repetir vèrtexs i arestes) de longitud k entre els vèrtexs v_i i v_j és l'entrada a_{ij} de la matriu A_G^k.*

Demostració. Procedirem per inducció sobre l'exponent k en A_G^k.
Per a $k = 1$ la proposició es redueix a la pròpia definició de la matriu d'adjacència i per tant aquest cas és trivial. Suposem que la proposició és certa per a $k-1$. Prenguem dos vèrtexs qualssevol v_i i v_j (que poden coincidir) de V. Un camí de longitud k que unix v_i amb v_j serà de la forma:

$$v_i x_1 x_2 x_3 \ldots x_{k-1} v_j.$$

Això es pot descompondre en $v_i x_1$ i $x_1 x_2 x_3 \ldots x_{k-1} v_j$. El primer camí de longitud 1 es correspon amb una aresta adjacent amb v_i i el segon de longitud $k-1$ és un camí que uneix un vèrtex connectat amb v_i amb el vèrtex v_j. Tenint en compte això, si anomenem $H_{i,j}(k)$ al nombre de camins de longitud k que connecten v_i amb v_j, es tindrà:

$$\begin{aligned} H_{i,j}(k) \quad = \quad & \sum_{v \in V} (\text{nombre d'arestes adjacents a } v_i \text{ i } v) \times (\text{nombre de camins de longitud} \\ & \qquad k-1 \text{ que connecten } v \text{ i } v_j) \end{aligned}$$

Donat un vèrtex qualsevol, v_k, el nombre d'arestes adjacents a v_i i v_k és precisament l'element de matriu $(A_G)_{i,k}$, per la qual cosa la suma anterior es pot expressar així:

$$H_{i,j}(k) = \sum_{l=1}^{n} (A_G)_{i,l} \times (\text{nombre de camins de longitud } k-1 \text{ que connecten } v_l \text{ i } v_j)$$

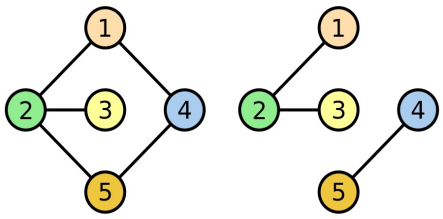
Però per la hipòtesi d'inducció el segon factor és $(A_G^{k-1})_{i,k}$. Pel que

$$H_{i,j}(k) = \sum_{l=1}^{n} (A_G)_{i,l} \cdot (A_G^{k-1})_{i,k} = (A_G^k)_{i,k}$$

Això conclou la demostració. □

Definició 3.2.5 *Un graf $G = (V, A)$ es diu que és connex si tot parell de vèrtexs té un camí que els unisca. En cas contrari, es diu que el graf és disconnex.*

Exemple 3.9 *La següent figura mostra exemples de grafs connex i disconnex:*

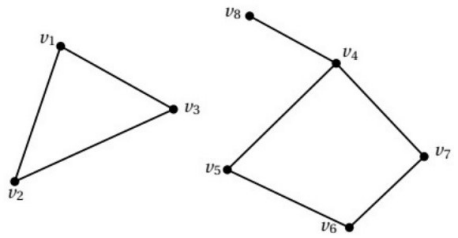


Graf connex (esquerra). Graf disconnex (dreta)

En un graf no connex hi ha vèrtexs que no poden ser connectats per cap camí. Per tant, el graf estarà format per diversos "blocs" de vèrtexs, cadascun dels quals és un graf connex.

Definició 3.2.6 *Si H és un subgraf de G, direm que H és una component connexa de G si H no està continguda en cap subgraf connex de G. És a dir, una component connexa de G és un subgraf que és maximal respecte a la propietat d'estar connectat.*

A continuació tenim un exemple de graf amb dues components connexes.



Per definició, les components connexes d'un graf són grafs connexos i és fàcil veure que tot graf es pot representar com a unió de grafs connexos (les seues components connexes).

Teorema 3.2.7 *Si $G = (V, A)$ és un graf connex, aleshores, $|A| \geq |V| - 1$.*

Demostració. Per inducció sobre $n = |V|$. Si $n = 1$, només hi ha un vèrtex i cap aresta, per tant, l'únic graf amb un vèrtex ja és connex i verifica que $|A| = 0 = |V| - 1$.
Suposem que la hipòtesi es verifica per a n. Ho demostrem per a $n + 1$. Triem un vèrtex v_0 i siga k el seu grau. Si llevem de G el vèrtex v_0 i les arestes associades, aleshores com a molt poden quedar k components connexes, $G_i = (V_i, A_i)$, per a $i = 1, \ldots, \ell \leq k$. Aplicant la hipòtesi d'inducció a cada component connexa, tenim que $|A_i| \geq |V_i| - 1$. Si ara sumem, s'obté

$$\sum_{i=1}^{\ell} |A_i| \geq \sum_{i=1}^{\ell} (|V_i| - 1) = \left(\sum_{i=1}^{\ell} |V_i| \right) - \ell.$$

Si ara tenim en compte el vèrtex que havíem llevat i les seues k arestes, aleshores

$$|A| = k + \sum_{i=1}^{\ell} |A_i| \geq \left(\sum_{i=1}^{\ell} |V_i| \right) + (k - \ell) = |V| - 1 + (k - \ell) \geq |V| - 1.$$

□

Nota 3.2.8 *El recíproc d'aquest resultat no és cert.*

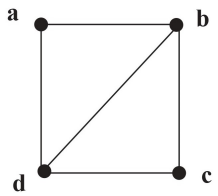
Definició 3.2.9 *Una successió de vèrtexs $v_0, v_1, \ldots, v_n$, amb $n > 1$ és un* **cicle** *si*

1. *són tots distints,*
2. *per a tot $i = 0, 1, \ldots, n-1$, v_i és amic de v_{i+1},*
3. *v_0 és amic de v_n.*

Equivalentment, direm que un cicle és una successió d'arestes adjacents, on no es recorre dues vegades la mateixa aresta, i on es torna al vèrtex inicial.

En aquest cas direm que el cicle té longitud $n+1$, que són la quantitat d'arestes que formen el cicle tancat.

Exemple 3.10 *En el graf*



a, b, d *és un cicle de longitud* 3.

3.3 Estructures de tipus arbre

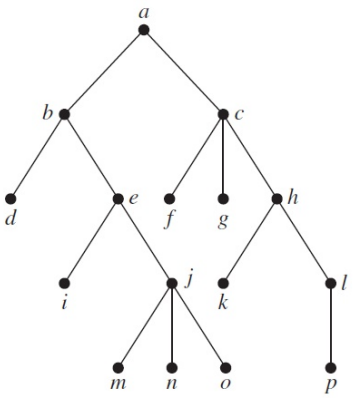
Entre els grafs hi ha una classe especial: els arbres. És una família de grafs molt important que des del seu origen ha demostrat tindre un gran nombre d'aplicacions en àrees com la química molecular i les ciències de la computació, on s'utilitzen per al disseny d'algorismes i estructures de dades, respectivament.

Definició 3.3.1 *Un arbre és un graf connex sense cicles.*

D'esta definició podem deduir que:

• Entre dos vèrtexs diferents, hi ha un únic camí. En cas contrari, obtindríem un cicle. I tot arbre és un graf simple.

Exemple 3.11 *Exemple d'un arbre:*



Definició 3.3.2 *Si G és un arbre, una fulla de l'arbre és un vèrtex amb grau* 1.

Proposició 3.3.3 *Tot arbre que complisca $|V| > 1$ té almenys dues fulles.*

Demostració. Per a demostrar el resultat anterior, com que el nombre de vèrtexs és finit, existirà un camí de longitud màxima i sense vèrtexs repetits. Siga aquest camí $v_0v_1v_2 \dots v_n$, llavors afirmem que si v_0 i v_n no tingueren grau 1 arribaríem a una contradicció. En efecte, si el grau de v_0 fora major d'1 llavors existiria una altra aresta diferent de v_0v_1, adjacent amb v_0. Si el vèrtex diferent de v_0 adjacent amb aquesta nova aresta estiguera en la seqüència, llavors hi hauria un cicle, sinó podríem ampliar la seqüència amb aquest vèrtex per l'esquerra. En tots dos casos arribem a una contradicció. El mateix raonament val per a v_n. □

Observar que ser connex exigeix tindre "prou" arestes quan el graf té molts vèrtexs, per a així poder connectar-los, mentre que no tindre cicles suposa que hi haja "poques" arestes relativament, perquè no es formen cicles. Els arbres estan just en el punt d'equilibri. El següent resultat representa aquesta idea. Té quatre apartats. El tercer d'ells ens diu que els arbres són els connexos "més pobres", en el sentit que tenen el nombre mínim d'arestes que permeten la connexió; en altres termes, un arbre és un graf mínimalment connectat. El quart ens diu que els arbres per no tindre cicles són grafs màximalment sense cicles.

Teorema 3.3.4 (Propietats equivalents dels arbres)
Per a tot graf $G = (V(G), A)$ són equivalents:

1. *G és un arbre.*
2. *(Unicitat del camí) Donats dos vèrtexs $u, v \in V(G)$, existeix exactament només un camí, sense vèrtexs repetits, que connecta u amb v.*
3. *(Graf connex minimal) G és connex i si suprimim una aresta qualsevol, deixa de ser-ho.*
4. *(Graf maximal sense cicles) G no té cicles i si afegim una aresta, el nou graf obtingut té un cicle.*
5. *$G = (V(G), A)$ és connex i $|A| = |V(G)| - 1$.*
6. *$G = (V(G), A)$ no té cicles i $|A| = |V(G)| - 1$.*

Demostració. $(1 \Rightarrow 2)$ G és un arbre per tant és connex i donats $u, v \in V(G)$ existeix almenys un camí que els uneix. Suposem que entre els vèrtexs u i v existeixen dos camins. Denotem per x el vèrtex on aquests camins divergeixen per primera vegada i per w el vèrtex on aquests camins convergeixen novament. Per tant els dos camins diferents entre els vèrtexs x i w formen un cicle, la qual cosa contradiu la definició d'arbre.

$(2 \Rightarrow 1)$ Suposem que per a tot $u, v \in V(G)$ existeix un únic camí que els uneix. Llavors G és connex i sense cicles, perquè d'existir un cicle existirien dos vèrtexs connectats per dos camins.

$(1 \Rightarrow 3)$ Suposem primer que tenim un graf G connex i sense cicles. Volem provar que es desconnecta en llevar una aresta qualsevol. Donada una aresta e de G, formem el graf $G\backslash\{e\}$ eliminant-la. Si $G\backslash\{e\}$ fora connex, podríem connectar en $G\backslash\{e\}$ els vèrtexs de l'aresta e, i afegint l'aresta e tindríem un cicle en G: contradicció. Així $G\backslash\{e\}$ no és connex (siga com siga l'aresta e triada).

$(3 \Rightarrow 1)$ Per hipòtesi, G és connex i es desconnecta si llevem qualsevol aresta. Si tinguera un cicle, llavors en suprimir una aresta d'aquest cicle obtindríem un graf que seria connex el que suposa una contradicció amb la hipòtesi.

$(1 \Rightarrow 4)$ Com que G és connex, dos vèrtexs qualssevol es poden connectar per un camí en G. En afegir una aresta entre aquests dos vèrtexs, aquesta aresta juntament amb el camí esmentat forma un cicle.

$(4 \Rightarrow 1)$ Siga G un graf sense cicles per al qual afegir una aresta qualsevol suposa la formació d'un cicle. Suposem que G no és connex. Llavors existeixen almenys dos vèrtexs u i v que no són connectats. En agregar l'aresta $\{uv\}$ apareix un cicle, la qual cosa implica l'existència d'un camí entre u i v. Contradicció. G és connex per tant és un arbre.

$(1 \Rightarrow 5)$ Farem la demostració per inducció sobre $|V|$. El pas inicial de la inducció és quan $|V| = 1$. Si un graf només té un vèrtex, no pot tindre aresta i, per tant $|A| = 0$.
Vam demostrar ara que l'enunciat és cert per a $n > 1$ suposant que és cert per a $n - 1$. Sabem que tot arbre té almenys una fulla. Si eliminem aquesta fulla del graf, la qual cosa queda, el graf $G' = (V', A')$, continua sent un graf connex sense cicles. Per tant, un arbre, amb un vèrtex i una aresta menys. Aplicant la hipòtesi d'inducció, tenim que $|A'| = |V'|-1 = (n-1)-1 = n-2$. Llavors, $|A| = |A'|+1 = (n-2)+1 = n-1$.

$(5 \Rightarrow 1)$ Si un graf connex amb $|A| = |V(G)| - 1$ tinguera un cicle, llavors podríem llevar-li una aresta (del cicle mateix) i el subgraf continuarà sent connex. Però, tindríem un graf connex amb dues arestes menys que la quantitat de vèrtexs, i això contradiu la hipòtesi. Així acaba la demostració del teorema.

$(1 \Rightarrow 6)$ Gràcies a l'equivalència anterior.

$(6 \Rightarrow 1)$ Per reducció a l'absurd. Suposem que G no té cicles i que $|A| = n - 1$, però que no és connex. Dividim el graf en les seues components connexes, $G_i = (V_i, A_i)$, per a $i = 1, \dots k$, amb $k > 1$.

Cada component connexa no té cicles, perquè si existira un cicle en alguna d'elles, aleshores el mateix cicle ho seria de G. Òbviament, cada component connexa és connexa. Per tant, cada component connexa és un arbre, i això implica que $|A_i| = |V_i| - 1$ per a tot $i = 1, \ldots, k$. Per tant,

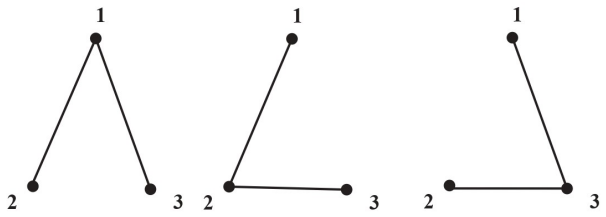
$$|A| = \sum_{i=1}^{k} |A_i| = \sum_{i=1}^{k} (|V - i| - 1) = \left(\sum_{i=1}^{k} |V_i| \right) - k = n - k < n - 1,$$

la qual cosa contradiu la hipòtesi $|A| = n - 1$. □

3.3.1 *Recompte d'arbres etiquetats. Teorema de Cayley*

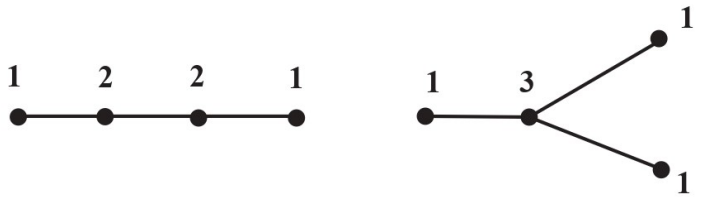
Definició 3.3.5 *Un arbre* **etiquetat** *és un arbre en el que cada vèrtex té una única etiqueta (nom).*

Arbres amb 1 únic vèrtex, n'hi ha un. Arbres amb 2 vèrtexs, només n'hi ha un, també. Amb tres vèrtexs ja tenim més possibilitats:



Representació dels tres arbres etiquetats que hi ha. De no etiquetats, només n'hi ha un

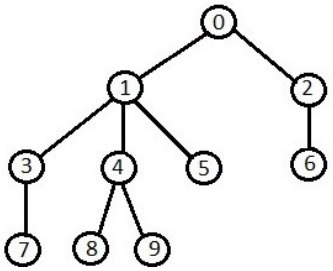
Amb 4 vèrtexs la cosa ja augmenta: n'hi ha 16 arbres etiquetats.



Representació dels dos arbres no etiquetats que hi ha. Els nombres que apareixen ara denoten els graus dels vèrtexs

Definició 3.3.6 *Un arbre arrelat és un arbre amb un vèrtex especial,* 0.

Exemple 3.12 *Exemple d'un arbre arrelat:*



Definició 3.3.7 *Siga $G = (V, A)$ un arbre arrelat. Donat $v \in V$ siga*

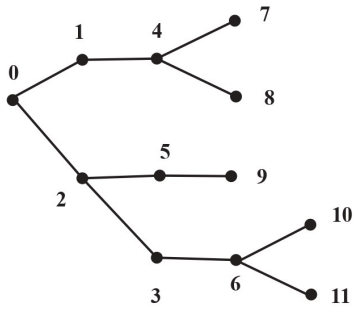
$$v_0 = 0, v_1, v_2, \ldots, v_{n-1}, v_n = v$$

l'únic camí entre 0 i v. Aleshores direm que v_{n-1} és pare de v i que v és fill de v_{n-1}.

3.3.2 *Construcció del codi de Prüfer*

Per tal de poder enumerar tots els arbres amb una quantitat de vèrtexs determinada, el que va fer Cayley va ser assignar a cada arbre arrelat un codi de nombres naturals de manera biunívoca.
Siga G un arbre amb n vèrtexs etiquetats amb els nombres $\{0, 1, 2, \ldots, n-1\}$, i les corresponents $n-1$ arestes. L'algorisme que descrivim a continuació associa a cada arbre etiquetat una llista ordenada de $n-2$ nombres (entre 0 i $n-1$) que anomenarem com $(a_1, \ldots, a_{n-2})$.
1-. Localitzem el vèrtex de grau 1 amb menor etiqueta, que anomenem b_1, i apuntem qui és el seu únic veí, a_1.
2-. Esborrem llavors b_1 i la seua aresta.
3-. Localitzem el vèrtex de grau 1 amb menor etiqueta, b_2, apuntem qui és el seu veí a_2, i esborrem b_2 i la seua aresta.
4-. I així, successivament, fins a quedar-nos amb només un vèrtex.
El que hem anat anotant forma una llista $(a_1, \ldots, a_{n-2})$, anomenada **codi de Prüfer** de l'arbre G. Aquesta llista pot tindre símbols repetits.

Per exemple, per l'arbre



Cayley construïa inicialment una matriu de dues files. En la primera fila anava escrivint, d'esquerra a dreta, el menor índex entre les fulles que no fóra l'arrel, i davall, el seu pare. A cada pas, llevava la fulla, i així successivament. En l'exemple seria: Llevem la fulla de menor valor diferent de l'arrel, si és que 0 fora fulla, i escrivim davall d'ella el seu pare.

$$\begin{matrix} 7 \\ 4 \end{matrix}$$

Repetim l'operació amb el graf que resulta d'eliminar la fulla.

$$\begin{matrix} 7 & 8 \\ 4 & 4 \end{matrix}$$

Continuem el procés fins que només ens quede el 0:

$$\begin{array}{cccccccccccc} & & & & & & & 7 & 8 & 4 & & \\ & & & & & & & 4 & 4 & 1 & & \end{array}$$

Al final del tot s'obté:

$$\begin{array}{cccccccccccc} 7 & 8 & 4 & 1 & 9 & 5 & 10 & 11 & 6 & 3 & 2 \\ 4 & 4 & 1 & 0 & 5 & 2 & 6 & 6 & 3 & 2 & 0 \end{array}$$

Com es pot observar, l'última xifra de la fila de baix sempre serà el 0, perquè sempre s'eliminen arestes de major valor. Notar també que cada columna representa una aresta. Per al codi de Prüfer, només necessitem la fila de baix a la qual li suprimirem el zero, ja que sempre s'acabarà en ell.

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

Mireu que el codi de l'exemple està format per 10 nombres naturals. Si hi afegim l'arrel de l'arbre, això fa un total d'11 columnes. És a dir, l'arbre té 11 arestes i 12 vèrtexs.
Com es faria el procés invers? És a dir, com es faria la reconstrucció de l'arbre a partir del seu codi de Prüfer?
Procedim com segueix: tenim la llista $a = (a_1, \ldots, a_{n-2})$ i el conjunt d'etiquetes $V = \{0, 1, 2, \ldots, n-1\}$.
1-. Declarem que b_1 és el menor element de V que no estiga en la llista a, i formem l'aresta $\{a_1, b_1\}$.
2-. Eliminem ara el símbol b_1 de V i retallem la llista a llevant-li el seu primer element.
3-. Repetim el procés per a obtindre b_2 (el menor element de $V \backslash \{b_1\}$ que no estiga en la llista retallada en el pas anterior), i formar l'aresta $\{a_2, b_2\}$.
4-. I així successivament.

Per exemple, considerem el següent codi de Prüfer:

$$1 \quad 1 \quad 1 \quad 0 \quad 12 \quad 12 \quad 9 \quad 9 \quad 5 \quad 0 \quad 6$$

Procedim així:

$$1 \quad 1 \quad 1 \quad 0 \quad 12 \quad 12 \quad 9 \quad 9 \quad 5 \quad 0 \quad 6 \quad 0$$

Hem afegit l'arrel al final. El primer vèrtex que va desaparèixer va ser el 2, el menor que falta en la seqüència:

$$\begin{array}{cccccccccccc} 2 & & & & & & & & & & & \\ 1 & 1 & 1 & 0 & 12 & 12 & 9 & 9 & 5 & 0 & 6 & 0 \end{array}$$

El següent serà el 3,

$$\begin{array}{cccccccccccc} 2 & 3 & & & & & & & & & & \\ 1 & 1 & 1 & 0 & 12 & 12 & 9 & 9 & 5 & 0 & 6 & 0 \end{array}$$

Després el 4,

$$\begin{array}{cccccccccccc} 2 & 3 & 4 & & & & & & & & & \\ 1 & 1 & 1 & 0 & 12 & 12 & 9 & 9 & 5 & 0 & 6 & 0 \end{array}$$

Ara ve el 1,

$$\begin{array}{cccccccccccc} 2 & 3 & 4 & 1 & & & & & & & & \\ 1 & 1 & 1 & 0 & 12 & 12 & 9 & 9 & 5 & 0 & 6 & 0 \end{array}$$

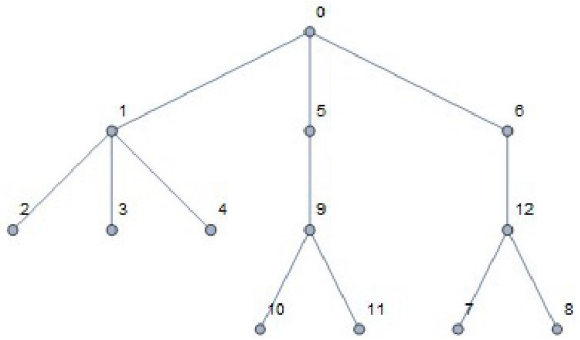
Li segueix el 7,

$$\begin{array}{cccccccccccc} 2 & 3 & 4 & 1 & 7 & & & & & & & \\ 1 & 1 & 1 & 0 & 12 & 12 & 9 & 9 & 5 & 0 & 6 & 0 \end{array}$$

Al final del tot queda

$$\begin{array}{cccccccccccc} 2 & 3 & 4 & 1 & 7 & 8 & 10 & 11 & 9 & 5 & 12 & 6 \\ 1 & 1 & 1 & 0 & 12 & 12 & 9 & 9 & 5 & 0 & 6 & 0 \end{array}$$

que dóna com a resultat aquest bonic arbre etiquetat:



Com que cada codi de Prüfer genera un arbre etiquetat diferent i al revés, és a dir, tot arbre etiquetat té un únic codi de Prüfer, hi haurà tants arbres etiquetats com codis de Prüfer diferents per a cada nombre de vèrtexs n. Cada codi està format per $n-2$ nombres triats entre les xifres $\{0,1,2,\ldots,n-1\}$. El còmput és fàcil: $VR(n,n-2)=n^{n-2}$. Per tant

Teorema 3.3.8 (Cayley) *La quantitat d'arbres etiquetats amb n vèrtexs és n^{n-2}.*

Un darrer comentari. Noteu que el nombre de vegades que apareix un vèrtex en el codi de Prüfer, més 1, és el seu grau.
Per exemple, per a $n=4$ tots els codis possibles són

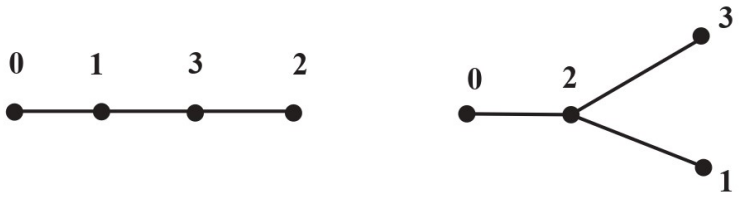
$$\begin{array}{cccc} 00 & 01 & 02 & 03 \\ 10 & 11 & 12 & 13 \\ 20 & 21 & 22 & 23 \\ 30 & 31 & 32 & 33 \end{array}$$

Per a reconstruir l'arbre corresponent al codi 31, primer hem de reconstruir la llista d'arestes:

$$\begin{array}{ccc} 2 & 3 & 1 \\ 3 & 1 & 0 \end{array}$$

I si el codi fóra el 22, la llista d'arestes seria :

$$\begin{array}{ccc} 1 & 3 & 2 \\ 2 & 2 & 0 \end{array}$$



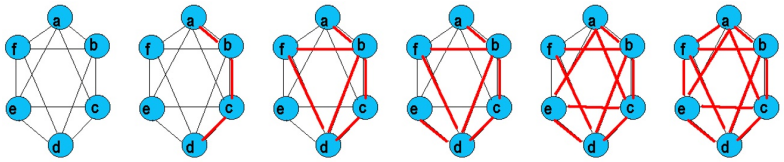
Els arbres associats als codis 31, esquerra, i 22, dreta

3.4 Camins i cicles eulerians

Com esmentem en la introducció d'aquest tema, Euler va resoldre el problema dels ponts de Königsberg. La solució d'aquest problema ha donat lloc a la definició d'una classe de grafs, els grafs eulerians.

Definició 3.4.1 (Cicle (camí) eulerià, graf eulerià)
Donat un graf $G = (V, A)$, un cicle (camí) eulerià és un cicle (camí) en el graf G que passa per tots els vèrtexs i per totes les arestes, però aquestes, exactament una sola vegada. Cal destacar que els vèrtexs del cicle poden repetir-se, les arestes no. Un graf es diu eulerià si té un cicle eulerià.

Exemple 3.13 *Exemple de cicle Eulerià:*



Nota: Un graf serà eulerià quan siguem capaços de traçar-lo de manera contínua, sense alçar el llapis del paper, sense dibuixar dos vegades la mateixa aresta, i coincidint l'origen i l'extrem.
Existeix una condició necessària i suficient per a saber si un graf és eulerià.

Teorema 3.4.2 (Euler)
La condició necessària i suficient perquè un graf siga eulerià és que siga connex i que tots els vèrtexs tinguen grau parell.

Demostració. ($\Rightarrow$) Si G té un cicle eulerià, aleshores és clar que G és un graf connex, ja que l'existència d'un cicle eulerià fa que es puguen connectar qualsevol parell de vèrtexs per un camí.

A més, com que el cicle eulerià entra en cada vèrtex tantes vegades com n'ix, aleshores el grau del vèrtex ha de ser parell.

($\Leftarrow$) Siga G un graf connex tal que tots els seus vèrtexs tenen grau parell. Hem de construir un cicle eulerià. Notem primer que G no pot ser un arbre, perquè en un arbre ja sabem que almenys un dels vèrtexs té grau 1. Per tant, si G no és un arbre, però sí que és connex, aleshores hi ha d'haver un cicle, Γ.

Procedirem ara per inducció sobre el nombre d'arestes de $G = (V, A)$. El cas $|A| = 1$ no es pot donar perquè aleshores només hi hauria dos vèrtexs i necessàriament tindrien grau 1. Una cosa similar passa si

$|A| = 2$. El primer cas possible per a grafs simples és quan $|A| = 3$, aleshores tenim 3 vèrtexs i el cicle eulerià és $\Gamma = A$.

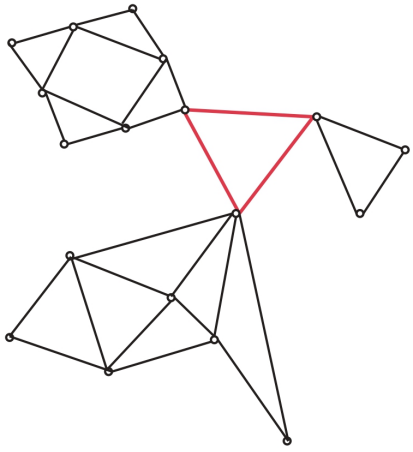
Suposem ara que la condició es verifica quan $|A| \leq n$. La demostrarem també quan $|A| = n + 1$ per reducció a l'absurd. Suposem que $\Gamma \neq A$. Considerem el graf $G' = (V, A - \Gamma)$, és a dir, llevem del graf G totes les arestes del cicle eulerià Γ. Notem que, en fer això, el grau en G' de qualsevol vèrtex, és el mateix que tenia en G, si no li afecta el cicle Γ, o dues unitats menys, si el cicle passava per ell. En qualsevol cas, el grau continua sent parell.

Siguen $G_1, G_2, \ldots, G_p$ les components connexes de G'. Agafem una d'aquestes components connexes, $G_i = (V_i, A_i)$.

Si $|V_i| = 1$, és perquè la component connexa només té un vèrtex i cap aresta. Això vol dir que aquest punt formava part del cicle Γ i al final de la demostració veurem que acabarà també connectat gràcies al cicle eulerià que construirem.

Notem també que no pot quedar una component connexa amb només dos vèrtexs, perquè, en aquest cas, el grau que tindrien seria igual a 1, i ja hem vist que el grau ha de ser parell encara que llevem el cicle Γ.
Suposem ara que $|V_i| > 1$. Ara bé, tots els vèrtexs de G_i tenen grau parell, G_i és connex, i $|A_i| \leq n$. Per la hipòtesi d'inducció, G_i té un cicle eulerià, Γ_i (és a dir, tal que passa per tots els vèrtexs de G_i i per totes les arestes A_i. Aleshores, Γ i Γ_i han de tenir intersecció comuna (perquè G és connex i perquè els G_i eren subgrafs connexos maximals).

Finalment, podem combinar el cicle Γ amb tots els cicles Γ_i i obtenir un cicle eulerià, un camí que passa per tots els vèrtexs de G i per totes les seues arestes, i només una vegada, i que torna al vèrtex d'on havia eixit. □

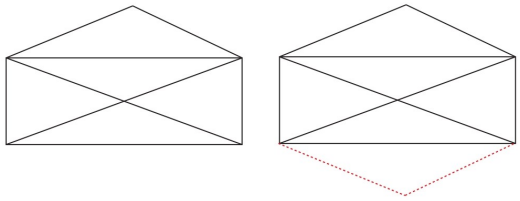


Un graf que verifica les hipòtesis del teorema. El triangle central de color vermell és un cicle. Si el llevem, aleshores queden tres components connexes

El següent corol·lari dóna una condició necessària i suficient d'existència de camí eulerià en un graf.

Corol·lari 3.4.3 *Un graf $G = (V, A)$ té un camí eulerià si i només si és connex i tots els vèrtexs, tret de dos d'ells, tenen grau parell.*

Demostració. Només cal considerar el graf G amb una aresta més que uneix els dos vèrtexs de grau senar si és que no estan connectats prèviament. Si ja estigueren connectats, aleshores afegiríem dues arestes noves i un vèrtex nou, per tal de connectar-los a través d'aquest nou vèrtex. Finalment, només cal aplicar el teorema anterior. □



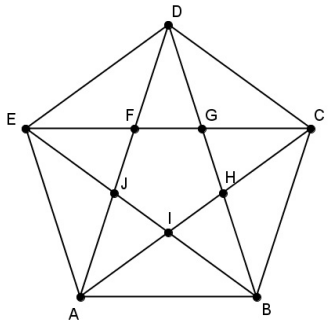
Esquerra: el clàssic graf que representa un sobre. No té cicles eulerians, però sí que té un camí eulerià. Dreta: il·lustració de l'argument en la demostració del corol·lari anterior

Algorisme per trobar el cicle o el camí eulerià

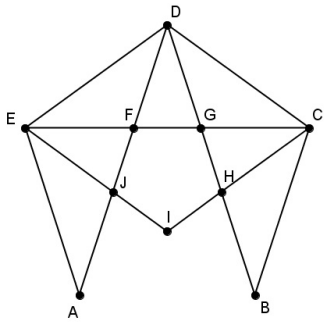
Per a construir els cicles o camins eulerians, podem seguir els passos del **algorisme de Fleury** següent:

1. Verificar que el graf és connex amb tots els vèrtexs de grau parell o bé, excepte dos d'ells, tots tenen grau parell.
2. Comencem triant un vèrtex del graf (de grau imparell si n'hi ha).
3. Anem recorrent el graf, triant arestes que no s'hagen recorregut.
   Sempre hem de triar, si és possible, una aresta tal que la supressió d'aquesta no desconnecte el graf. Si no és possible és perquè només queda una aresta, amb la qual cosa, afegirem aquesta última aresta al camí.
4. A continuació, passem a l'altre vèrtex i eliminem l'aresta triada.
5. I així successivament, fins a l'última aresta.

Vegem un exemple amb el següent graf (que correspon a K_5):



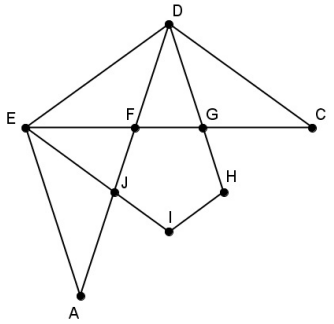
Partim d'un vèrtex, per exemple A, i triem les arestes $\{A, I\}$, després $\{I, B\}$. Eliminem aqueixes arestes (i l'aresta $\{A, B\}$ perquè forma un cicle) i els vèrtexs que queden aïllats. Ens queda aquest graf:



Seguim, per exemple, per l'aresta $\{B, C\}$, després $\{C, H\}$. Llavors tenim ara com ara el camí

$$\{A, I, B, C, H\}.$$

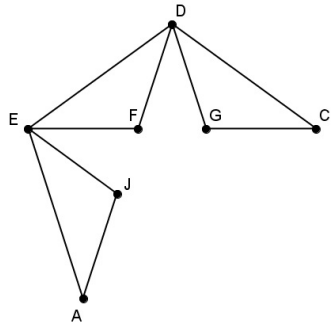
Eliminem les arestes que conté el camí i els vèrtexs aïllats que queden. Arribem a aquest graf:



I continuem de la mateixa forma. Per exemple, ara triem les arestes $\{H, G\}$, $\{G, F\}$, $\{F, J\}$, $\{J, I\}$ i ho inserim en el camí anterior, quedant

$$\{A, I, B, C, H, G, F, J, I\}.$$

Eliminant arestes i vèrtexs aïllats queda



Ara cal inserir els 3 cicles en el camí anterior i tancar-lo. Prenem $\{G, C, D, G\}$ i en inserir queda

$$\{A, I, B, C, H, G, C, D, G, F, J, I\}.$$

Després, per exemple, $\{D, E, F, D\}$, que en inserir ens dona

$$\{A, I, B, C, H, G, C, D, E, F, D, G, F, J, I\}.$$

I, finalment, $\{E, J, A, E\}$, que després d'inserir-ho ens dóna un dels possibles recorreguts que podem fer en el graf inicial per a passar per totes les arestes exactament una vegada començant i acabant pel vèrtex A:

$$\{A, I, B, C, H, G, C, D, E, J, A, E, F, D, G, F, J, I, H, B, A\}.$$

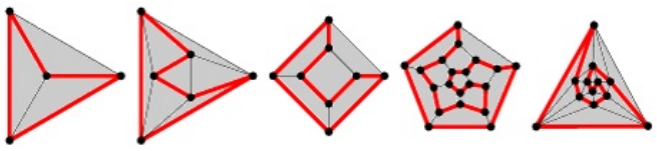
3.5 Camins i cicles hamiltonians

Ara introduïm un altre tipus de grafs, els anomenats hamiltonians. Sir William Hamilton (1805 - 1865) va crear un joc anomenat *Icosian Game*. El joc tenia com a tauler un dodecaedre regular de fusta en el qual cada vèrtex tenia un pivot etiquetat amb el nom d'una ciutat europea. L'objectiu del joc era trobar un itinerari (utilitzant les arestes del dodecaedre) que comença i acaba en la mateixa ciutat i que passe per totes les ciutats una sola vegada.

Llavors el que busca el joc és un cicle que utilitze tots els vèrtexs del dodecaedre. A partir d'allí sorgeix la idea de definir els grafs que tenen un cicle que passe una sola vegada per cada vèrtex del graf.

Definició 3.5.1 *Un cicle en un graf s'anomena cicle hamiltonià si conté tots els vèrtexs una sola vegada, a excepció del primer i de l'últim. Un graf es diu hamiltonià si conté un cicle hamiltonià.*

Exemple 3.14 *Exemples de cicles hamiltonians:*



Malauradament, a diferència dels grafs eulerians, no es coneix una condició necessària i suficient per a determinar si un graf és hamiltonià o no. Podem trobar condicions necessàries i condicions suficients, però fins avui ningú ha donat amb una caracterització que represente una equivalència a la definició.

Teorema 3.5.2 (Condició necessària perquè un graf siga hamiltonià)
Siga $G = (V, A)$ un graf hamiltonià i siga S un conjunt no buit de vèrtexs de G. Siga $G(V - S)$ el subgraf induït de G generat per $V - S$ i si $c(G(V - S))$ és el nombre de components connexes de $G(V - S)$, aleshores

$$c(G(V - S)) \leq |S|.$$

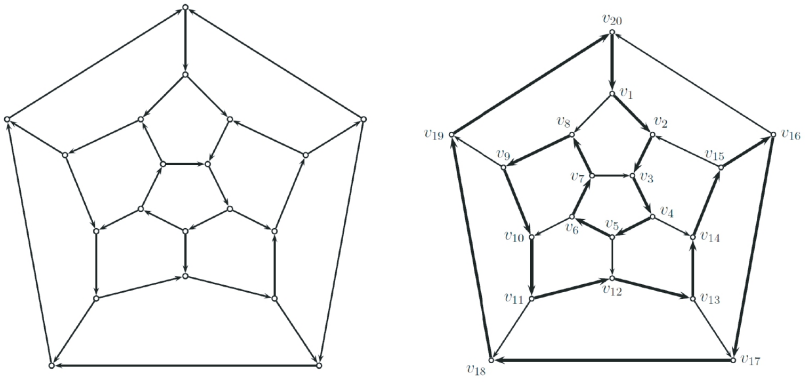
Demostració. Siga Γ un cicle hamiltonià en G i siga $\widetilde{G}$ el graf $\widetilde{G} = (V, \Gamma)$. Si eliminem $|S|$ vèrtexs de G, allò que no passarà mai és que tallarem el cicle en més de $|S|$ trossos i, per tant,

$$c(\widetilde{G}(V - S)) \leq |S|.$$

Ara bé, també tenim

$$c(G(V - S)) \leq c(\widetilde{G}(V - S)),$$

ja que en $G(V - S)$ com a mínim hi ha tantes arestes com en $\Gamma - S$ i els mateixos vèrtexs. Per tant el nombre de les seues components connexes no pot superar al de $\Gamma - S$. I el resultat està demostrat. □



Representació del graf hamiltonià del dodecaedre

Sí que hi ha algun resultat parcial en el sentit del recíproc. Per exemple aquest que no demostrarem:

Proposició 3.5.3 *Si en un graf amb n vèrtexs, $n \geq 3$, tots el vèrtexs tenen grau major o igual a $\frac{n}{2}$, aleshores el graf és hamiltonià.*

El que ve a dir aquest enunciat és que si un graf té "moltes" arestes, aleshores sempre es podrà construir en ell un cicle hamiltonià.

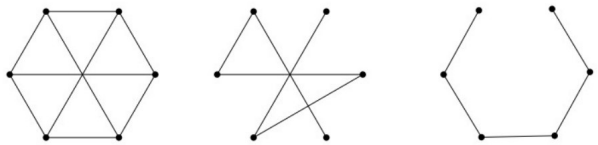
3.6 Arbres generadors

La noció d'arbre generador pot tenir com a punt de partida la següent pregunta: construir una xarxa que connecte una sèrie de punts (per exemple, un sistema d'oleoductes, una xarxa d'ordinadors) de la forma

més barata (quant a nombre de connexions) a partir d'un disseny previ. Per tant, l'objectiu és eliminar el major nombre possible d'arestes de manera que el graf continue sent connex. Estem buscant, en definitiva, un subgraf que siga arbre i que incloga a tots els vèrtexs.

Definició 3.6.1 (Árbol generador)
Donat un graf, un arbre generador és un arbre que ocupa arestes de G i tots els vèrtexs de G.

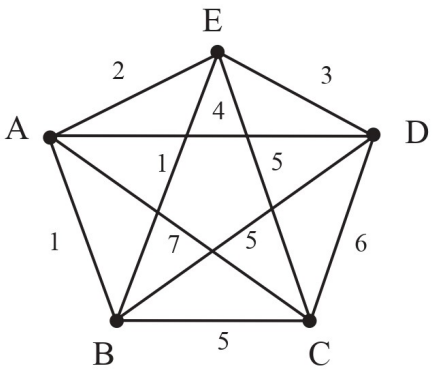
En general, un graf connex pot tindre diversos arbres generadors. En la figura següent es mostra un graf i dos dels seus arbres generadors.



Ara, tornant a l'exemple anterior de la xarxa, si volem renovar la xarxa amb un cost mínim, això es pot traduir amb un graf on les arestes tenen un cert valor o pes, que indique el cost de renovació entre els punts de la xarxa. Si volem minimitzar el cost de renovació de la xarxa, hem de trobar un arbre generador de manera que la suma dels pesos de les arestes siga mínima. Això motiva la definició de graf amb pesos.

Definició 3.6.2 *Un graf amb pesos és un graf $G = (V, A)$ i una funció $f : A \to \mathbb{R}$ que assigna a cada aresta del graf un pes.*

Un exemple podria ser la funció que a cada aresta li assigna la seua longitud.



Un exemple de graf complet amb pesos

Un arbre generador la suma de pesos del qual és la menor possible l'anomenarem **arbre generador de pes mínim**. Hi ha un algorisme que resol el problema de trobar tal arbre. Aquest algorisme és un exemple del tipus d'algorismes anomenats **algorismes golafres**, o **glotons**[4], ja que consisteix a prendre en cada pas l'aresta de menor pes sempre que forme un arbre amb les anteriors.

[4]En anglès: *greedy algorithms*.

Si l'apliquem en l'exemple de la figura, començaríem triant l'aresta AB, que té un pes 1. A continuació triaríem l'aresta BE, que té pes 1. Després, no podem agafar l'aresta EA perquè, encara que té el menor cost, formaríem un cicle. L'aresta que s'agafaria seria la ED, que té pes 3. Per últim, afegiríem l'aresta BC o EC, que tenen pes 5. Per tant, el cost total és $1 + 1 + 3 + 5 = 10$.
Encara que la solució no és única, el que sí que podem assegurar és que el cost total és el menor possible.
Encara que aquest algorisme resol el problema pot ser en alguns casos complicat de dur a terme. El teorema que ve a continuació exposa un altre algorisme més operatiu.

Teorema 3.6.3 (Algorisme de formació de l'arbre de pes mínim)
Siga un graf G amb n vèrtexs i siga $a_1, a_2, \ldots, a_{n-1}$ una successió de $n-1$ arestes de manera que per a cada $i = 1, \ldots, n-1$, l'aresta a_i és l'aresta de menor pes que es puga prendre sense formar cicles. Llavors el graf T format per $V(T) = V(G)$ i $A(T) = \{a_1, a_2, \ldots, a_{n-1}\}$ és un arbre generador de pes mínim.

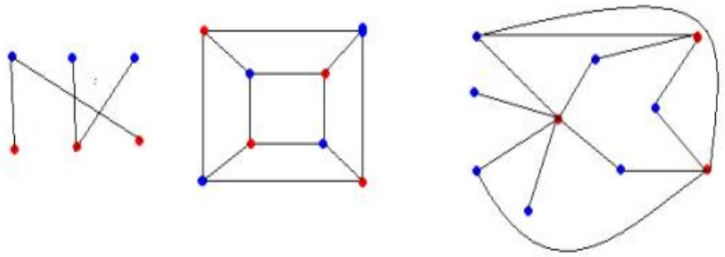
Demostració. Hem de provar primer que T és un arbre. Per hipòtesi sabem que no té cicles i també que el nombre d'arestes és una menys que el nombre de vèrtexs. Pel Teorema 3.3.4, T és un arbre.
A més, és un arbre generador perquè, com que té $n-1$ arestes, aleshores tindrà n vèrtexs.
Ara hem de demostrar que el seu cost és el menor possible. Siga T' un altre arbre generador de G. Hem de demostrar que el cost de T és menor o igual que el cost de T'.
En la successió d'arestes de T' (en principi les podem ordenar com vulguem ja que és un conjunt finit), siga e la primera aresta de T que no està en T'. Si afegim aquesta aresta a T' es formarà un cicle perquè això era una de les caracteritzacions d'un arbre. Siga C aquest cicle. En ell ha d'existir una aresta que no està en T, en cas contrari en T apareixeria un cicle. Siga f aquesta aresta del cicle C, que tindrà un pes major o igual que el de e, ja que no pot ser cap de les anteriors a e, en aquest cas s'hauria format un cicle en el graf T. Formem ara el graf $T + e - f$, és a dir, el graf format canviant en T l'aresta f per la e. El graf $T' + e - f$ és un arbre perquè no té cicles i té $n-1$ arestes. Per la hipòtesi de l'enunciat, el pes de l'aresta e és menor o igual que el pes de l'aresta f. Per tant, el pes de $T' + e - f$ és menor o igual que el pes de T'.
Repetint el procés un nombre finit de vegades arribem al graf T, ja que en cada pas el graf que queda és de menor pes que l'anterior. I la demostració queda finalitzada. □

3.7 Graf bipartit. El Teorema del matrimoni

Un altre problema clàssic és el següent: 50 xiques i 50 xics han d'acudir a un ball per parelles. Cadascun d'ells té les seues preferències respecte als assistents de l'altre sexe. El problema és si existeix un emparellament en què cada xica quede emparellada amb un xic del seu gust.

Definició 3.7.1 *Un graf $G = (V, A)$ és bipartit si existeixen dos conjunts disjunts no buits D i E (són les inicials de dreta i esquerra, respectivament) de forma que:*

1. *$V = D \cup E$.*
2. *Cada aresta de A uneix un vèrtex de D amb un de E.*
3. *No existeixen arestes unint dos elements de D; anàlogament per a E.*



Exemples de grafs bipartits

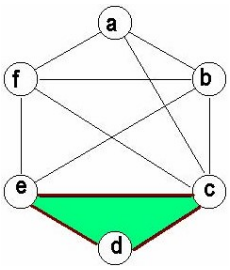
Vegem primer una caracterització dels grafs bipartits:

Teorema 3.7.2 *Un graf $G = (V, A)$ és un graf bipartit si i només si no té cicles de longitud senar.*

Demostració. ($\Rightarrow$) Suposem que $G = (D \cup E, A)$ és un graf bipartit. Siga $v_0, v_1, \ldots, v_{k-1}, v_k (= v_0)$ un cicle en G. Podem suposar que $v_0 \in D$, aleshores necessàriament $v_1 \in E$, $v_2 \in D$,.... Com que $v_k = v_0 \in D$, $v_{k-1} \in E$ i per tant $k-1$ ha de ser senar, aleshores k es parell.
($\Leftarrow$) Podem suposar que G és connex (en un altre cas, treballaríem amb cadascuna de les seues components connexes).
Triem un vertex $v_0 \in V$ qualsevol. Per a cada vèrtex $v \in V$, siga p_v qualsevol camí **minimal** que unisca v_0 amb v. I denotem per d_v la seua longitud. Noteu que tots els camins minimals que uneixen dos vèrtexs tenen la mateixa longitud.
Definim ara

$$D = \{v \in V |\ d_v \text{ és parell }\} \qquad \text{i} \qquad E = \{v \in V |\ d_v \text{ és senar }\}.$$

Òbviament, $V = D \cup E$ és una partició de V. Anem a comprovar, per reducció a l'absurd, que el graf $G = (D \cup E, A)$ és bipartit.
Si el graf $G = (D \cup E, A)$ no fóra bipartit és perquè existirien dos vèrtexs u, v que, o bé estan totsdós en D, o bé estan totsdós en E, i que estan units per una única aresta $\{u, v\}$.
Considerem el camí tancat definit per la unió de $p_u, \{u, v\}$ i p_v (de v_0 a u, de u a v, i de v a v_0.) La longitud total d'aquest camí tancat és $d_u + 1 + d_v$, que és un nombre senar, tant si $u, v \in D$, com si $u, v \in E$. D'aquest camí tancat sempre es pot treure un cicle (sense repeticions de vèrtexs, tret de l'inicial i final) de longitud senar (en efecte, si el camí es descomposara en cicles de longitud parella, aleshores la longitud del camí, que és la suma de les longituds dels cicles en què es descomposa, seria parella), la qual cosa contradiu la hipòtesi. Per tant, el graf $G = (D \cup E, A)$ és bipartit. □



Exemple d'un graf no bipartit
Conté cicles de longitud imparella (en la figura apareix marcat un de longitud 3)

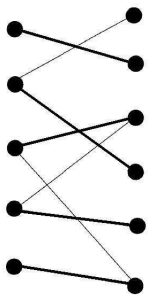
Aquests resultats bàsics sobre grafs bipartits són l'entrada a uns altres més interessants referents als denominats problemes d'aparellament. Suposem que tenim un conjunt de persones X i un conjunt de treballs Y. Cada persona està qualificada per a realitzar alguns dels treballs. Una qüestió important és com assignar persones als treballs de manera que el màxim nombre d'elles aconseguisca un treball per al qual està qualificada.

Definició 3.7.3 *Un emparellament en un graf bipartit $G = (D \cup E, A)$ és un subconjunt M de A amb la propietat que dues arestes de M mai tenen un vèrtex en comú.*
Direm emparellament perfecte en G a un emparellament que cobreix tots els vèrtexs de G. En aquest cas $|D| = |E|$.

Nota 3.7.4

- *Un emparellament es pot definir en qualsevol tipus de grafs.*
- *Un emparellament en un graf G és un conjunt d'arestes M de G sense vèrtexs comuns. És a dir, un subgraf on tots els vèrtexs tenen grau menor o igual que 1.*

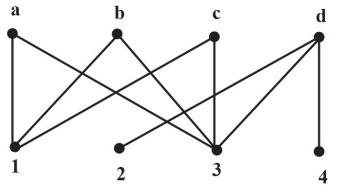
En el graf següent es mostra un emparellament en el graf bipartit on les arestes més gruixudes són precisament l'emparellament.



Emparellament en un graf bipartit

El primer pas en l'estudi dels emparellaments és decidir quan és possible que existisca un emparellament perfecte. El problema del ball es pot formular, segons les definicions anteriors, com el problema de trobar un emparellament perfecte en un graf bipartit.

De vegades no hi ha solució. Per exemple:



Un exemple de graf bipartit per al qual no existeix un emparellament perfecte. Noteu que a, b i c estan competint per 1 i 3

Exemples 3.7.5

- *Problema del matrimoni. D i E representen un conjunt de xics i xiques respectivament. Les arestes venen donades per la relació "voler casar-se amb".*
- *Problema de l'allotjament. D i E representen el mateix conjunt de persones. Es disposa d'un nombre determinat d'habitacions dobles. No obstant això algunes parelles són compatibles per a dormir en la mateixa habitació i altres no. Les arestes representen les compatibilitats.*
- *Problema d'assignació de tasques. D representa un conjunt de persones i E un conjunt de tasques a realitzar. Les arestes venen donades per la capacitat de les persones per a fer aquesta tasca.*

En els exemples anteriors es veu clarament quin és el propòsit que es desitja. Es tracta d'aconseguir que es case el major nombre possible de parelles, allotjar a la major quantitat de persones possible o realitzar la major part de les tasques.

El següent resultat dóna una condició necessària i suficient perquè existisca un emparellament perfecte.

Teorema 3.7.6 *Siga $G = (D \cup E, A)$ un graf bipartit amb $|D| = |E|$. El graf G té un emparellament perfecte si i només si per a cada $S \subset D$ el conjunt*

$$N(S) = \{b \in E : b \text{ és amic de } s \text{ per a algun } s \in S\}$$

té almenys tants elements com S, és a dir,

$$|N(S)| \geq |S|.$$

Demostració. ($\Rightarrow$) Siga $S = \{d_1, d_2, \ldots, d_k\} \subset D$. Si hi ha un emparellament perfecte, aleshores cada element d_i tindrà la seua parella $e_i \in E$. Això implica que $e_i \in N(S)$ per a tot $i \in \{1, 2, \ldots, k\}$. Per tant

$$|N(S)| \geq k = |S|.$$

($\Leftarrow$) Farem la demostració per inducció sobre el nombre d'arestes de G, $|A| = m$.
Si $m = 1$, és a dir, si només tenim una aresta, és fàcil comprovar que aleshores D i E són conjunts monoelementals i que el graf G és el graf complet K_2 que té un emparellament perfecte obvi.
Suposem que tot graf bipartit amb un nombre d'arestes menor igual a m té un emparellament perfecte. Demostrarem el mateix per a un graf amb $|A| = m + 1$. Dividirem la demostració en dos casos:

1. Suposem que per a tot $S \subset D$, amb $0 < |S| < |D|$, tenim que $|N(S)| \geq |S| + 1$ o, en cas contrari,
2. suposem que existeix un $S \subset D$, amb $0 < |S| < |D|$, tal que $|N(S)| = |S|$.

En el primer cas, agafem una aresta qualsevol de G, $\{d, e\}$. Considerem ara el subgraf induït en el subconjunt $(D - \{d\}) \cup (E - \{e\})$ el qual denotarem per G'. És també un graf bipartit i almenys té una aresta menys de les que tenia G. Comprovem que verifica la condició de l'enunciat: siga $S \subset D - \{d\}$, aleshores

$$N^{G'}(S) = \begin{cases} N^G(S) & \text{si } e \notin N^G(S), \\ N^G(S) - \{e\} & \text{si } e \in N^G(S). \end{cases}$$

En ambdós casos, com que estem suposant que $|N^G(S)| \geq |S| + 1$, tenim que $|N^{G'}(S)| \geq |S|$. Podem, per tant, aplicar la hipótesi d'inducció al subgraf G' i deduir que té un emparellament perfecte. Si a aquest emparellament perfecte li afegim l'aresta que havíem llevat, $\{d, e\}$, tindrem l'emparellament perfecte del graf inicial G.
Suposem ara que estem en el segon cas, és a dir, que existeix un $S \subset D$, amb $0 < |S| < |D|$, tal que $|N(S)| = |S|$. En aquest cas, primer apliquem la hipótesi d'inducció al graf bipartit induït en S i $N(S)$. Això en donarà un primer emparellament perfecte que només emparella vèrtexs de S amb vèrtexs de $N(S)$. Siguen ara, $D' = D - S$ i $E' = E - N(S)$, i considerem el subgraf induït en $D' \cup E'$ el qual denotarem per G'. És també un graf bipartit i té menys arestes de les que tenia G. Comprovem que verifica la condició de l'enunciat: per reducció a l'absurd, si existeix $S' \subset D'$ tal que $|N^{G'}(S')| < |S'|$, aleshores

$$N^G(S \cup S') = |N^G(S)| + |N^G(S') \cap E'| = |N^G(S)| + |N^{G'}(S')| < |S| + |S'| = |S \cup S'|,$$

la qual cosa és una contradicció.
Si apliquem en G' la hipótesi d'inducció, tindrem un altre emparellament perfecte que només emparella vèrtexs de $D - S$ amb vèrtexs de $E - N(S)$. Unint ara els dos emparellaments, obtenim el resultat desitjat.
□
Noteu que en l'exemple anterior, si $S = \{a, b, c\}$, aleshores $N(S) = \{1, 3\}$, per tant, no es verifica $|N(S)| \geq |S|$.

L'algorisme que funciona en aquest problema no és ni un algorisme bèstia, ni un algorisme golafre, sinó un algorisme de tipus "prova-error" i torna arrere. S'ha d'anar construint l'emparellament i si en algun moment falla, s'ha de tornar enrere i fer una altra elecció.

3.8 Exercicis

1. Demostreu que en qualsevol reunió de persones, després d'haver-se saludat els coneguts entre si xocant-se la mà, la quantitat de persones que han xocat la mà un nombre senar de vegades sempre és un nombre parell.

2. Demostreu que en una festa en què participen un nombre senar de persones, sempre n'hi ha una que té un nombre parell de coneguts entre els participants. Assumim que la relació "ser conegut" és simètrica. També pot passar que hi haja gent que no hi tinga cap conegut.

3. Un grup d'onze estudiants van de vacances. Com que, cadascú va per la seua banda, decideixen que cada estudiant enviarà una postal a cinc dels altres. És possible que cada estudiant reba postals exactament dels estudiants a qui ha escrit?

4. Quin és el màxim nombre d'arestes que pot tenir un graf amb 10 vèrtexs?

5. Demostreu que si un graf amb n vèrtexs té més d'un vèrtex i més de $\frac{(n-1)(n-2)}{2}$ arestes, aleshores és connex.

6. Demostreu que si en un graf amb n vèrtexs, $n \geq 3$, tots el vèrtexs tenen grau major o igual a $\frac{n}{2}$, aleshores el graf és connex.

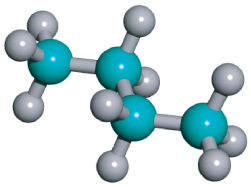
7. Demostreu que si un graf té almenys dos vèrtexs, aleshores hi ha dos vèrtexs que tenen el mateix grau.

8. Siga $G = (V, A)$ un graf. Siga A' el conjunt d'arestes d'un cicle en G. Demostreu que tots els vèrtexs del graf parcial (V, A') tenen grau parell.

9. El graf complet K_n amb n vèrtexs ($n \geq 2$) és el graf que té per arestes tots els subconjunts de dos elements que es puguen formar amb els vèrtexs. Enumereu tots els possibles arbres generadors dels grafs complets K_2 (n'hi ha només un), K_3 (n'hi ha tres) i K_4 (n'hi ha 16).

10. Demostreu que en un arbre sempre hi ha almenys dues fulles. I trobeu un arbre que només en tinga dues.

11. Hidrocarburs saturats i arbres. Els grafs es poden fer servir per a representar molècules. Els vèrtexs representen els àtoms i les arestes representen els enllaços.



Molècula de butà.

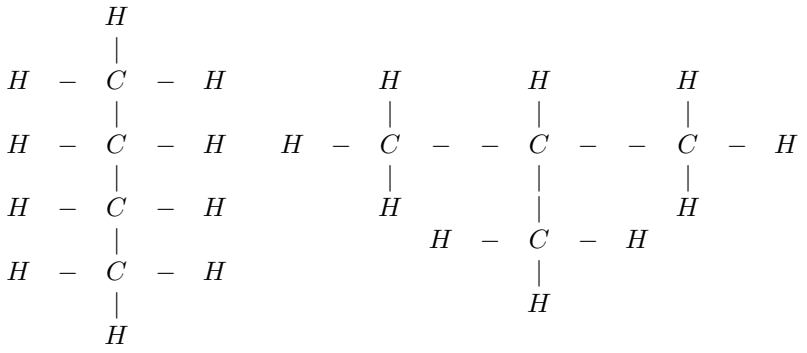
En el models amb grafs dels hidrocarburs saturats, cada àtom de carboni és un vèrtex de grau 4, mentre que cada àtom d'hidrogen és un vèrtex de grau 1. Recordeu allò de les valències dels àtoms.

Quants vèrtexs tindrà qualsevol graf associat a la molècula C_nH_{2n+2}?

Recordant la relació entre els graus dels vèrtexs i el nombre total d'arestes, quantes arestes tindrà qualsevol graf associat a la molècula C_nH_{2n+2}?

Deduïu de les respostes anteriors que qualsevol graf que represente la molècula C_nH_{2n+2} és un arbre.

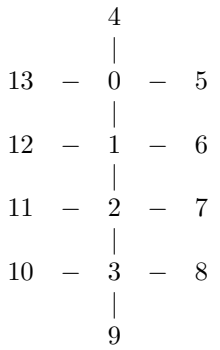
Per a $n = 4$ només hi ha dos arbres no isomorfs que corresponen a dos isòmers diferents de la molècula C_4H_{10}:



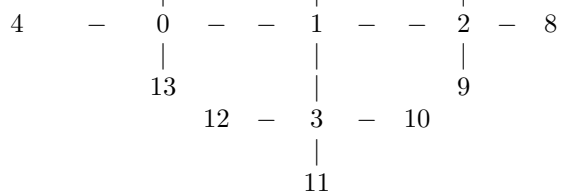
Butà

Isobutà

12. Calculeu els codis de Cayley dels grafs associats a les dues molècules anteriors una vegada etiquetats:



Butà



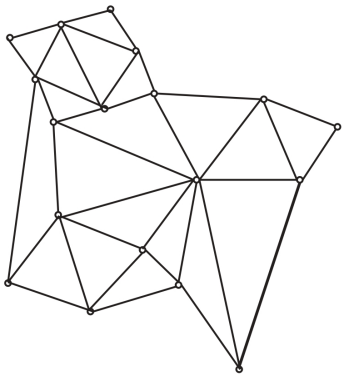
Isobutà

(Sol.: Butà: $0, 0, 1, 2, 3, 3, 3, 2, 2, 1, 1, 0$. Isobutà: $0, 0, 1, 2, 2, 2, 1, 3, 3, 3, 1, 0$.)

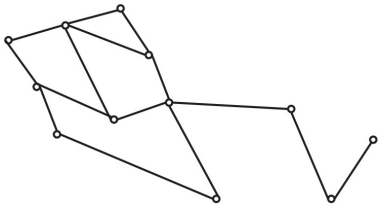
13. Construïu l'arbre que té com a codi de Cayley associat

$$0 \quad 0 \quad 4 \quad 4 \quad 3 \quad 3 \quad 8 \quad 3$$

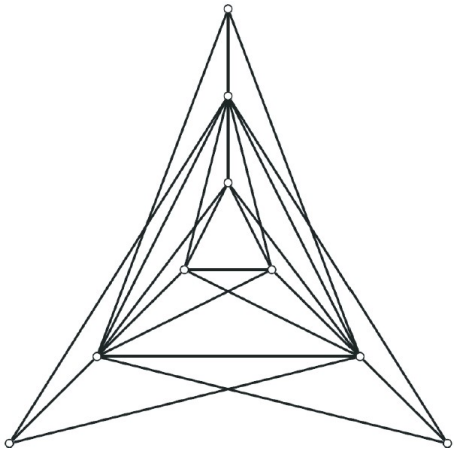
14. Comproveu si en el graf següent hi ha algun camí eulerià:



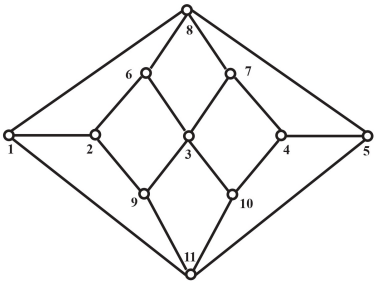
15. Comprova si en el graf següent hi ha algun camí eulerià i en cas contrari, afegiu els vèrtexs i les arestes que considereu necessaris perquè sí que n'existisca un, i calcula'l.



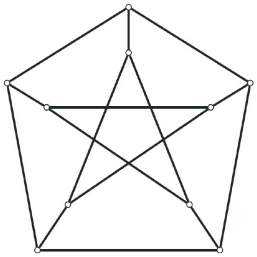
16. Demostreu, fent servir la proposició 3.5.2, que el graf següent no admet un camí hamiltonià:



17. Comproveu que el graf següent no admet un camí hamiltonià:



18. Comproveu que el diabòlic graf següent, anomenat graf de Petersen, verifica la condició de la proposició 3.5.2, però que, malgrat això, no admet un camí hamiltonià. Això demostra que la condició expressada en l'enunciat de la proposició és una condició necessària, però no suficient.



19. Comproveu que si llevem un dels vèrtexs qualsevol i, per tant, també llevem les arestes associades, del graf de Petersen, aleshores sí que hi ha un camí hamiltonià.

20. Comproveu que el graf de l'exercici 17 és un graf bipartit.

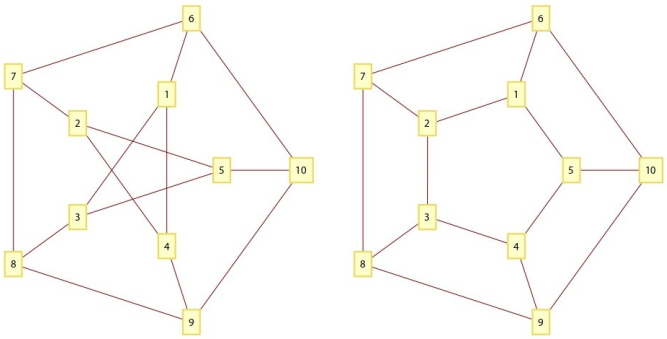
21. Trobeu un emparellament perfecte en el graf de l'exercici 17 després d'haver-li llevat el vèrtex 10.

22. Comproveu que el graf de Petersen (Exer. 18) no és un graf bipartit.

23. Dibuixeu el graf associat al mapa següent. Aprofiteu les capitals com a vèrtex.

    És un graf connex? Quin és el vèrtex amb major grau? Si considerem la major component connexa, hi ha algun cicle eulerià? Hi ha algun camí eulerià?

24. Comprova que en els següents dos grafs tots els vèrtexs tenen el mateix grau. Això no vol dir que siguen isomorfs, i de fet, aquests dos no ho són. Per què? (Ajuda: un dels dos grafs té un cicle hamiltonià. L'altre no.)



4. Aritmètica modular

Algunes de les nocions d'aritmètica modular ja s'han explicat en l'assignatura Matemàtica bàsica de primer quadrimestre. Concretament en el Tema 6, "Nombres enters i divisibilitat", s'han introduït els conceptes de nombre primer i de màxim comú divisor, així com l'algorisme d'Euclides i el teorema de Bèzout.

L'objectiu d'aquest tema és continuar un poc més aquesta part de les matemàtiques que ha tingut una revitalització gràcies a algunes aplicacions recents, per exemple les relacionades amb la criptografia. Tanmateix, començarem recordant aquests conceptes essencials.

4.1 Algorisme d'Euclides

Recordem que el màxim comú divisor de dos nombres naturals, a, b, es denota per m.c.d.(a, b). I aprofitem per recordar també que si m.c.d.$(a, b) = 1$, aleshores dels nombres a i b es diu que són relativament primers entre si, o simplement, que són coprimers.

Donats els nombres enters a i b, el que es fa per tal de calcular el seu màxim comú divisor és descompondre cadascun d'ells com a producte de factors primers i després triar els factors que apareixen en totes dues descomposicions. Per exemple, si volem calcular m.c.d.$(120, 72)$ farem

$$\begin{aligned} 120 &= 2^3 \cdot 3 \cdot 5, \\ 72 &= 2^3 \cdot 3^2. \end{aligned}$$

Per tant, m.c.d.$(120, 72) = 2^3 \cdot 3 = 24$.

Si els nombres amb què treballes són grans no és gens fàcil trobar-ne la descomposició com a producte de nombres primers. Aleshores el càlcul del màxim comú divisor de dos enters s'ha de fer d'una altra manera:
Per a calcular el m.c.d.(a, b), amb $a > b$, l'algorisme d'Euclides diu que s'ha de fer el següent: Primer dividir a entre b i calcular el quocient q_1 i el residu r_1:

$$a = q_1 \cdot b + r_1.$$

Després, tornem a fer el mateix substituint a per b i b per r_1:

$$b = q_2 \cdot r_1 + r_2.$$

Després, r_1 entre r_2:

$$r_1 = q_3 \cdot r_2 + r_3.$$

I continuem aixífins que un r_i divideix r_{i-1}. En aquest cas, m.c.d.$(a, b) = r_i$. El procés de càlcul segons l'algorisme s'acaba després d'una quantitat finita de passos ja que en casdascun dels passos tenim que $r_i < r_{i-1}$.

Exemple 4.1.1 *Calculeu m.c.d.*$(1547, 560)$.

$$\begin{aligned} 1547 &= 2 \cdot 560 + 427, \\ 560 &= 1 \cdot 427 + 133, \\ 427 &= 3 \cdot 133 + 28, \\ 133 &= 4 \cdot 28 + 21, \\ 28 &= 1 \cdot 21 + 7. \end{aligned}$$

Com que 7 *dividix* 21*, ja hem acabat: m.c.d.*$(1547, 560) = 7$.

Proposició 4.1.2 *L'algorisme d'Euclides sempre calcula el màxim comú divisor en una quantitat finita de passos.*

En tot el tema, farem servir la notació $a \mid b$ per a dir que a divideix b.

Teorema 4.1.3 *Siga* $d = m.c.d.(a, b)$*, amb* $a > b$*. Aleshores, existeixen enters* u, v *tal que*

$$d = ua + vb.$$

Aquesta equació s'anomena **Identitat de Bèzout**.

Demostració. Suposem que $a \geq 0$ i $b \geq 0$, i procedirem per inducció sobre $n = a + b$. Si $n = 0$, llavors és suficient prendre $u = v = d = 0$, ja que en aquest cas necessàriament $a = b = 0$. Suposem que el teorema està provat per a $0, 1, 2, \ldots, n-1$. No es perd generalitat si se suposa que $a \geq b$. Si $b = 0$, és suficient prendre $d = a$, $u = 1$ e $v = 0$. Si $b \geq 1$, llavors podem aplicar la hipòtesi d'inducció a $a - b$ i b, ja que $(a - b) + b = a = n - b \leq n - 1$. Així doncs

$$\exists u, v, d \in \mathbb{Z} \text{ de manera que } \; d = (a - b)u + bv$$

i a més $d \mid b$ i $d \mid (a - b)$. Després, per linealitat $d \mid ((a - b) + b)$, això és, $d \mid a$. El teorema queda provat, doncs, en aquest cas, sense més que posar l'expressió anterior de la forma:

$$d = au + b(v - u).$$

Si tots dos a i b són negatius, llavors podem aplicar el cas anterior als nombres $|a|$ i $|b|$, és a dir

$$\exists \; u, v, d \in \mathbb{Z} \text{ de manera que } \; d = |a|u + |b|v$$

sent d un divisor de $|a|$ i de $|b|$. Es té doncs que $-d = u(-|a|) + v(-|b|) = au + bv$ i naturalment $-d \mid a$ i $-d \mid b$.
El cas en què un nombre és positiu i un altre negatiu es raonaria de manera anàloga. □

Exemple 4.1.4 *Ja hem vist adés que* $\text{m.c.d.}(1547, 560) = 7$. *Anem a trobar* u *i* v *tal que*

$$7 = u \cdot 1547 + v \cdot 560.$$

Procedirem a partir dels càlculs de l'algorisme d'Euclides, però del final cap al principi.

$$\begin{aligned} 7 &= 28 - 1 \cdot 21 \\ &= 28 - (133 - 4 \cdot 28) = -133 + 5 \cdot 28 \\ &= -133 + 5 \cdot (427 - 3 \cdot 133) = 5 \cdot 427 - 16 \cdot 133 \\ &= 5 \cdot 427 - 16 \cdot (560 - 427) = -16 \cdot 560 + 21 \cdot 427 \\ &= -16 \cdot 560 + 21 \cdot (1547 - 2 \cdot 560) = 21 \cdot 1547 - 58 \cdot 560. \end{aligned}$$

Per tant,

$$7 = \mathbf{21} \cdot 1547 - \mathbf{58} \cdot 560.$$

Lema 4.1.5 *(***Lema d'Euclides***)*
Si $a \mid bc$ *i* $\text{m.c.d.}(a, b) = 1$*, aleshores* $a \mid c$.

Demostració. Podem escriure que per a alguna parella de enters u, v, $1 = au + bv$. Per tant de $c = acu + bcv$, però com que $a \mid acu$ i $a \mid bcv$, per linealitat $a \mid (acu + bcv)$, això és $a \mid c$. □

4.2 Congruències en els enters

Definició 4.2.1 *Donats tres nombres enters* a, b *i* m*, direm que "*a *és congruent amb* b *mòdul* m*", i escriurem*

$$a \equiv b \pmod{m},$$

si la diferència $a - b$ *és divisible per* m*. El nombre enter* m *s'anomena el "mòdul" de la congruència.*

Les propietats següents es deriven immediatament de la definició.

1. $a \equiv a \pmod{m}$.
2. $a \equiv b \pmod{m}$ si i només si $b \equiv a \pmod{m}$.
3. Si $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$, aleshores $a \equiv c \pmod{m}$.

   Per tant, la relació de congruència és una relació binària d'equivalència.

   Cada classe d'equivalència s'anomena **classe de residus** i té un únic representant entre 0 i $m - 1$. El conjunt quocient, o conjunt de classes d'equivalència, es denota per $\frac{\mathbb{Z}}{m\mathbb{Z}}$ o $\mathbb{Z}_m$.
4. Si $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, aleshores $a + c \equiv b + d \pmod{m}$ i $ac \equiv bd \pmod{m}$.

   És a dir, $\mathbb{Z}_m$ és un anell commutatiu.
5. Si $a \equiv b \pmod{m}$, aleshores $a \equiv b \pmod{d}$ per a qualsevol divisor de m, d.

6. Si $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$, i m i n són primers entre si, aleshores $a \equiv b \pmod{mn}$.

Demostració. Demostrem aquesta darrera. Si $a \equiv b \pmod{m}$, aleshores $a - b = k_1 m$. Si $a \equiv b \pmod{n}$, aleshores $a - b = k_2 n$. Com que $k_1 m = k_2 n$ i com que m i n no tenen factors comuns, aleshores $m \mid k_2$, és a dir, $k_2 = rm$. Per tant,

$$a - b = k_2 n = rmn,$$

és a dir, $a \equiv b \pmod{mn}$. □

Proposició 4.2.2 *Els elements invertibles per al producte de $\mathbb{Z}_m$ són aquells que són relativament primers amb m.*

És a dir, els enters a per als quals existeix un b tal que

$$ab \equiv 1 \pmod{m}$$

són precisament aquells a tal que m.c.d.$(a, m) = 1$.

Exemple 4.1 *Mòdul* 841*, l'enter* 160 *és invertible. En efecte,* $841 = 29^2$ *mentre que* $160 = 2^5 \cdot 5$*. Per tant m.c.d.*$(841, 160) = 1$*. El seu invers és* 205*, ja que*

$$160 \cdot 205 - 1 = 32800 - 1 = 32799 = 39 \cdot 841.$$

Proposició 4.2.3 *Si $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ i $m.c.d.(c, m) = 1$ (i, per tant, també m.c.d.$(d, m) = 1$), aleshores $ac^{-1} \equiv bd^{-1} \pmod{m}$.*

4.3 Teorema xinès del residu

La forma original del teorema xinés de la resta, continguda en un llibre del matemàtic xinés Qin Jiushao publicat en 1247, és un resultat en relació amb els sistemes de congruències. És anomenat així pel fet que les versions més antigues sobre aquests problemes de congruències es troben en treballs matemàtics xinesos. Però el problema més antic es troba en el llibre de Sun Zi, el Sunzi suanjing, datat en el segle III. L'enunciat del problema de Sun Zi és el següent:

Quants soldats té l'exèrcit de Han Xing si, formats en 3 columnes, queden dos soldats, formats en 5 columnes, queden tres soldats i, formats en 7 columnes, queden dos soldats?

Es pot pensar que els xinesos, a base de fer càlculs astronòmics pogueren estar interessats en concordances de calendari i que hagen arribat a interessar-se per preguntes del tipus:

A quants dies del solstici d'hivern caurà la lluna plena?

Si la qüestió es fa mentre queden 6 dies abans del solstici d'hivern i 3 dies abans de la lluna plena, la pregunta es tradueix en:

Existeix un enter x tal que el residu de la divisió de x entre 365 done 6 i el residu de la divisió de x entre 28 done 3?

La resolució proposada per Sun Zi per al problema dels soldats és la següent:

Multipliqueu el residu de la divisió entre 3, és a dir 2, per 70, afegiu-li el producte del residu de la divisió entre 5, és a dir 3, per 21, després afegiu el producte del residu de la división entre 7, és a dir 2, per 15. Mentre el nombre siga més gran que 105, resteu-li 105.
És a dir, calculeu primer

$$2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233.$$

Després, aneu restant-li 105 fins que quede menor que 105:

$$233 - 2 \cdot 105 = 23.$$

La solució és, per tant, 23.

La solució, però, explica més que imperfectament el mètode emprat. Això és el que farem en l'anomenat Teorema xinès del residu. Abans, però, mirem una altra manera d'arribar al resultat:

Noteu que cerquem un nombre x, que si el dividim per 3, el residu dóna 2; si el dividim per 5, el residu dóna 3; i si el dividim per 7, el residu dóna 2.
Per tant, $x - 2$ és múltiple tant de 3 com de 7. La menor de les possibilitats és

$$x - 2 = 3 \cdot 7 = 21.$$

és a dir, $x = 21 + 2 = 23$. Només queda comprovar que el residu de 23, mòdul 5, és 3.

Finalment, seria una llàstima no presentar aquest problema en relació amb pirates i un tresor, exemple citat molt freqüentment per il·lustrar el teorema dels residus xinesos:

Exemple 4.2 *Una banda de 17 pirates posseeix un tresor constituït per peces d'or d'igual valor. Projecten partir-se-les a parts iguals, i donar-ne la resta al cuiner xinès. Aquest rebria llavors 3 peces. Els pirates, però, es barallen i sis d'ells moren. Un nou repartiment donaria al cuiner 4 peces. En un naufragi ulterior, només se salven el tresor, sis pirates i el cuiner, i el repartiment donaria llavors 5 peces d'or a aquest últim. Quina és la fortuna mínima que pot esperar el cuiner si decideix enverinar la resta dels pirates i quedar-se amb tot el tresor?*

Si intentàrem ara trobar la solució del problema dels pirates per un procediment similar al que hem fet servir en l'anterior exemple, veuríem que la cosa ja no és tan senzilla. Els nombres implicats ja no són el 3, el 5 i el 7, sinó el 17, l'11 i el 6, i a més a més, no hi ha coincidència entre residus. Cal un mètode general.

Teorema 4.3.1 *(Teorema xinès del residu)*
Siguen $p_1, p_2, \ldots, p_n$ nombres enters positius de manera que $\text{m.c.d.}(p_i, p_j) = 1$, per a tot $i, j = 1, 2, \ldots, n$, $i \neq j$. Llavors si anomenem $M_i = \dfrac{\prod_{j=1}^{n} p_j}{p_i}$, amb $i = 1, 2, \ldots, n$, existeixen n enters N_i que compleixen

$M_iN_i \equiv 1 \pmod{p_i}$.
Suposem que tenim el sistema de congruències:

$$\begin{cases} x & \equiv a_1 \pmod{p_1}, \\ x & \equiv a_2 \pmod{p_2}, \\ & \dots \quad \dots \\ x & \equiv a_n \pmod{p_n}. \end{cases}$$

Aleshores el nombre $s = \sum_{i=1}^{n} a_iM_iN_i$ *és una solució i qualsevol altra solució és congruent amb* s *mòdul* M, *on* $M = \prod_{i=1}^{n} p_i$.

Demostració. Com que es compleix que m.c.d$(M_i, p_i) = 1$ ja que justament $M_i = \frac{M}{p_i}$, i cap nombre p_j té factors comuns amb un altre p_ℓ diferent d'ell, llavors per la proposició dels elements invertibles en $\mathbb{Z}_{p_i}$ tenim que M_i és invertible en $\mathbb{Z}_{p_i}$, per tant l'existència de N_i complint que $M_iN_i \equiv 1 \pmod{p_i}$ està garantida. En la pràctica, es fa servir l'algorisme d'Euclides per a trobar-lo.
D'altra banda comprovarem que s compleix les equacions anteriors. Provem per exemple que $s \equiv a_1 \pmod{p_1}$.

$$s - a_1 = \sum_{i=1}^{n} a_iM_iN_i - a_1 = a_1(M_1N_1 - 1) + \sum_{i=2}^{n} a_iM_iN_i.$$

El primer sumand és $a_1(M_1N_1 - 1) \equiv 0 \pmod{p_1}$ i com que el segon sumand és múltiple de p_1, perquè el factor p_1 està en tots els M_i amb $i \neq 1$, tenim que $s - a_1 \equiv 0 \pmod{p_1}$. Raonant anàlogament es proven la resta de congruències.
Suposem ara que u és una altra solució. Es compleix que $u \equiv x \pmod{p_i}$, per a tot $i = 1, 2, \dots, n$. És a dir, tots els p_i divideixen $x - u$. Com que entre els p_i no hi ha factors comuns, llavors M divideix $x - u$.
□

Exemple 4.3 *El problema dels soldats es redueix a*

$$\begin{cases} x & \equiv 2 \pmod{3}, \\ x & \equiv 3 \pmod{5}, \\ x & \equiv 2 \pmod{7}. \end{cases}$$

Llavors s'obté

$$M = 105.$$

$$M_1 = 35,\ M_2 = 21,\ M_3 = 15.$$

$$N_1 = 2,\ N_2 = 1,\ N_3 = 1.$$

Una solució per a x *és llavors* $x = 2 \times 70 + 3 \times 21 + 2 \times 15 = 233$ *i les solucions són tots els enters congruents amb 233 mòdul 105, és a dir a 23 mòdul 105.*

$$x = 233 \equiv \mathbf{23} \pmod{M}.$$

Exemple 4.4 *Trobem el nombre de tres dígits en base* 10 *que dividit per* 7 *per* 9 *o per* 11 *sempre deixa de residu* 4*. Per tant, ens estan demanant de trobar una solució entre* 100 *i* 999 *del sistema*

$$\begin{cases} x & \equiv 4 \pmod 7, \\ x & \equiv 4 \pmod 9, \\ x & \equiv 4 \pmod{11}. \end{cases}$$

Encara que en aquesta situació podríem posar directament (aplicant la propietat 6), que el nombre que busquem no és altre que

$$4 + 7 \cdot 9 \cdot 11 = 697,$$

el trobarem aplicant el teorema.
En aquest cas, $M = 7 \cdot 9 \cdot 11 = 693$ *mentre que*

$$M_1 = 9 \cdot 11 = 99, \quad M_2 = 7 \cdot 11 = 77, \quad M_3 = 7 \cdot 9 = 63.$$

Hem de trobar ara els N_i*:*
Com que $M_1 = 99 = 14 \cdot 7 + 1 \equiv 1 \pmod 7$*, aleshores* $N_1 = 1$*.*
Com que $M_2 \cdot 2 = 77 \cdot 2 = 154 = 17 \cdot 9 + 1 \equiv 1 \pmod 9$*, aleshores* $N_2 = 2$*.*
Com que $M_3 \cdot 7 = 63 \cdot 7 = 441 = 40 \cdot 11 + 1 \equiv 1 \pmod{11}$*, aleshores* $N_3 = 7$*.*
Per tant, una solució és

$$x = 4(M_1N_1 + M_2N_2 + M_3N_3) = 4(99 \cdot 1 + 77 \cdot 2 + 63 \cdot 7) = 4 \cdot (99 + 154 + 441) = 2776.$$

Com que busquem una entre 100 *i* 999*:*

$$2776 = 4 + 4 \cdot 693 \equiv 4 + 693 = 697 \pmod{693}.$$

La solució és 697*.*

Exemple 4.5 *Trobeu la menor solució no negativa de*

$$\begin{cases} x & \equiv 12 \pmod{31}, \\ x & \equiv 87 \pmod{127}, \\ x & \equiv 91 \pmod{255}. \end{cases}$$

$$M = 1003935.$$

$$M_1 = 32385,\ M_2 = 7905,\ M_3 = 3937.$$

$$N_1 = 3,\ N_2 = 41,\ N_3 = 148.$$

$$x = 82386511 \equiv \mathbf{63841} \pmod M.$$

Exemple 4.6 *Vegem que el resultat anterior es pot usar fins i tot si els* m_i *no són tots primers entre si (amb la diferència que llavors pot ocórrer que el sistema de congruències no tinga solució). Suposem per exemple que volem resoldre el sistema de congruències*

$$\begin{cases} x & \equiv 5 \pmod{24} \\ x & \equiv 1 \pmod{28} \\ x & \equiv -4 \pmod{15} \end{cases}$$

Evidentment, no estem en les condicions del Teorema xinès del residu, ja que, per exemple, $\text{m.c.d.}(24, 28) = 4$. *No obstant això, podem usar la Propietat 5 per a substituir el nostre sistema pel sistema equivalent:*

$$\begin{cases} x & \equiv & 5 & (\text{mod } 8) \\ x & \equiv & 5 & (\text{mod } 3) \\ x & \equiv & 1 & (\text{mod } 4) \\ x & \equiv & 1 & (\text{mod } 7) \\ x & \equiv & -4 & (\text{mod } 3) \\ x & \equiv & -4 & (\text{mod } 5) \end{cases}$$

Per descomptat, seguim sense estar en les hipòtesis del Teorema xinès del residu, però ara podrem llevar les congruències que ens sobren. En primer lloc, tenim les congruències $x \equiv 5 \pmod 3$ *i* $x \equiv -4 \pmod 3$, *que són equivalents, ja que* $5 \equiv -4 \pmod 3$, *així que podem eliminar una d'elles. Encara tenim el parell de congruències* $x \equiv 5 \pmod 8$ *i* $x \equiv 1 \pmod 4$ *que no ens permeten aplicar el Teorema xinès del residu. En aquest cas, observem que* $x \equiv 5 \pmod 8$ *implica òbviament* $x \equiv 5 \pmod 4$, *que és equivalent a* $x \equiv 1 \pmod 4$, *perquè* $5 \equiv 1 \pmod 4$. *Així doncs, podem eliminar la congruència* $x \equiv 1 \pmod 4$ *i tenim ja el sistema equivalent de congruències:*

$$\begin{cases} x & \equiv & 5 & (\text{mod } 8) \\ x & \equiv & 5 & (\text{mod } 3) \\ x & \equiv & 1 & (\text{mod } 7) \\ x & \equiv & -4 & (\text{mod } 5) \end{cases}$$

que ja està en les hipòtesis del Teorema xinès del Residu, i sabem que té solució. (Val la pena fer ací una pausa per a observar que podria haver ocorregut que, en lloc de trobar congruències equivalents mòdul 4, haguérem trobat congruències incompatibles; això haguera volgut dir que el sistema de partida és incompatible i no té solució).
Apliquem ara el mètode de resolució que ens dóna el Teorema xinès del residu, és a dir, resolem primer les congruències:

$$M = 840.$$

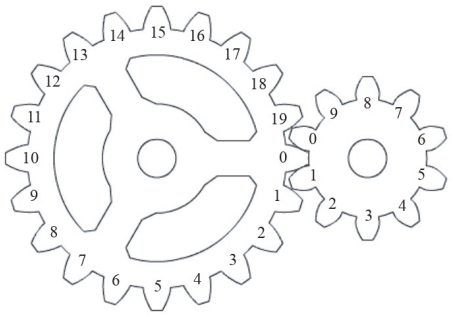
$$M_1 = 105,\ M_2 = 280,\ M_3 = 120,\ M_4 = 168.$$

$$N_1 = 1,\ N_2 = 1,\ N_3 = 1,\ N_4 = 2.$$

La solució final, per tant és

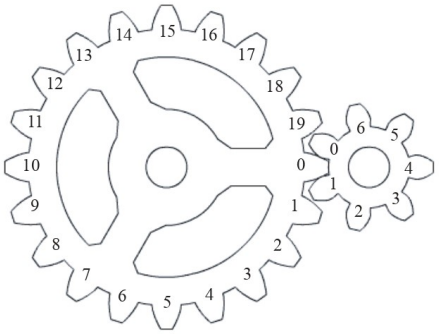
$$x \equiv 105 \cdot 1 \cdot 5 + 280 \cdot 1 \cdot 2 + 120 \cdot 1 \cdot 1 + 168 \cdot 1 \cdot 2 = 1541 \equiv \mathbf{701} \pmod{840}.$$

Exemple 4.3.2 *El teorema xinès del residu admet una interpretació mecànica en termes de rodes dentades. Considerem la representació següent*



Representació de dues rodes dentades, una de 20 dents i l'altra de 10

En aquesta situació és fàcil cerciorar-se que la dent número 17 *de la roda major i la* 4 *de la roda menor mai estaran en contacte com ho estan en el dibuix les dents numerades ambdues amb el* 0*. Sí que ho estaran la dent número* 17 *de la roda major i la* 7 *de la roda menor. No és necessari ni que la roda major faça una volta sencera. Això és així perquè la quantitat de dents de la roda major és un múltiple del nombre de dents de la roda menor.*
La situació és molt diferent si ambdós nombres de dents són coprimers.



Ara la menor té només 7 dents

Ens preguntem ara si en aquest cas hi haurà algun moment en què la dent 17 *de la roda major i la* 4 *de la menor estiguen en contacte.*
En realitat estem preguntant per la resolució del sistema:

$$\begin{cases} x \equiv 17 \pmod{20} \\ x \equiv 4 \pmod{7} \end{cases}$$

La solució més menuda d'aquest sistema de congruències és $x = 137$*. Això vol dir que han de passar* 137 *dents perquè aquestes dues dents estiguen en contacte. A la major de les dues rodes li mancaran* 3 *dents perquè haja fet exactament* 7 *voltes senceres.*

4.4 Equacions diofàntiques lineals

Les equacions diofàntiques, que com indica el seu nom, es deuen a Diofant d'Alexandria, un antic matemàtic grec l'obra del qual va tindre una gran importància i influència en generacions posteriors. Els problemes tractats per Diofant s'ocupaven d'aspectes merament numèrics en els quals intervenen les propietats dels nombres enters.

Una equació diofàntica és qualsevol equació en diverses variables els coeficients de les quals són nombres enters i de la qual únicament ens interessen les solucions que, al seu torn, també són nombres enters. Encara que també hi ha equacions diofàntiques amb diverses incògnites, nosaltres només estudiarem en aquest tema les equacions diofàntiques amb dues incògnites, i, a més, lineals.

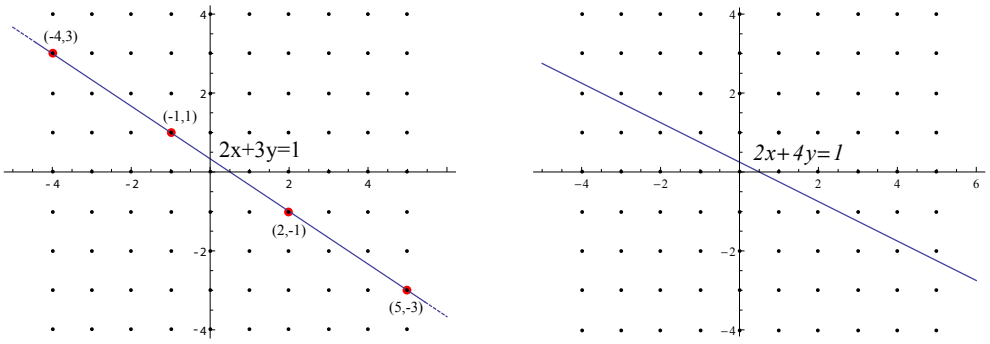
Definició 4.4.1 *Una equació diofàntica lineal és una equació del tipus*

$$ax + by = c,$$

amb $a, b, c \in \mathbb{Z}$ *i on es vol trobar solucions* x, y *que siguen també nombres enters.*

Exemple 4.7 *L'equació* $2x + 3y = 1$ *és una equació diofàntica lineal. Una solució és* $x = 2, y = -1$*, però no és l'única solució. Per exemple,* $x = -1, y = 1$ *és una altra solució.*

Una altra equació diofàntica és $2x + 4y = 1$*. Aquesta, però, no té cap solució entera. Per a qualsevol parell de nombres enters* x *i* y*, la combinació* $2x + 4y$ *sempre serà un nombre parell i, per tant, mai pot ser igual que* 1*.*



Esquerra: representació de la recta $2x + 3y = 1$ *i d'algunes de les seues solucions diofàntiques. Dreta: representació de la recta* $2x + 4y = 1$ *i visualització de la no existència de solucions diofàntiques.*

Una altra equació diofàntica que tampoc no té solucions enteres és $12x + 15y = 100$*. Noteu que si en tinguera, com que el* 3 *divideix tant a* 12 *com a* 15*, aleshores hauria de dividir a* 100*.*

Vegem la condició necessària i suficient perquè existisquen solucions.

Teorema 4.4.2 • *Una equació diofàntica lineal*

$$ax + by = c,$$

té solucions en els enters si i només si m.c.d.(a, b) *divideix c.*

- *Si es complix la condició anterior i si x_0, y_0 és una solució, aleshores totes les solucions són de la forma*

$$x = x_0 + \lambda\, b, \qquad y = y_0 - \lambda\, a, \tag{4.1}$$

per algun $\lambda \in \mathbb{Q}$.

Demostració. Comprovem primer que si existeix alguna solució $x_0, y_0 \in \mathbb{Z}$ i si $d = \text{m.c.d.}(a, b)$, aleshores d divideix c. En efecte, és una conseqüència del fet que d divideix $x_0a + y_0b = c$.
Recíprocament, comprovem ara que si $d \mid c$, aleshores existeix alguna solució de l'equació. D'acord amb la identitat de Bèzout, sabem que existeixen $u, v \in \mathbb{Z}$ tal que

$$ua + vb = d.$$

Si $c = dr$, aleshores $x_0 = ur, y_0 = vr$ és una solució de l'equació.
És ben fàcil comprovar que si x_0, y_0 és una solució de $ax + by = c$, aleshores, per a qualsevol $\lambda \in \mathbb{Q}$, $x = x_0 + \lambda\, b, y = y_0 - \lambda\, a$ també és una solució de $ax + by = c$.
Suposem que la parella (x, y) és una solució, provem que ha de ser de la forma que diu el teorema. Tenim d'una banda $ax_0 + by_0 = c$ i d'altra banda $ax + by = c$. Restant les equacions obtenim

$$a(x - x_0) + b(y - y_0) = 0 \Longleftrightarrow a(x - x_0) = b(y_0 - y).$$

Anomenem $a_1 = \frac{a}{d}$ i $b_1 = \frac{b}{d}$ llavors m.c.d.$(a_1, b_1) = 1$ ja que hem dividit a i b pel seu màxim comú divisor. Així doncs, $a_1(x - x_0) = b_1(y_0 - y)$, és a dir $a_1(x - x_0) \mid b_1(y_0 - y)$; però com que a_1 i b_1 són primers relatius, pel lema d'Euclides sabem que $a_1 \mid (y_0 - y)$, aleshores existeix un λ_1 enter complint $y_0 - y = a_1\lambda_1$. Raonant anàlogament existeix un λ_2 complint $x - x_0 = b_1\lambda_2$. Si $ab \neq 0$ llavors $\lambda_1 = \lambda_2$. En efecte
$c = ax + by = a(x_0 + \lambda_2 b_1) + b(y_0 - \lambda_1 a_1) = ax_0 + by_0 + a\lambda_2 b_1 - b\lambda_1 a_1 = c + a\lambda_2 b_1 - b\lambda_1 a_1$.
Per tant, $a\lambda_2 b_1 = b\lambda_1 a_1$ i multiplicant per d es té que

$$ab\lambda_2 = ab\lambda_1.$$

Si $ab \neq 0$ llavors $\lambda_1 = \lambda_2$ i el teorema està provat. Si $ab = 0$, posem que $b = 0$, l'equació és $ax = c$. Per hipòtesi $a \mid c$ perquè m.c.d.$(a, 0) = a$, la solució és $x = \frac{c}{a} = \frac{c}{a} + 0\lambda$. El valor de y és arbitrari i podem suposar que té la forma indicada. □

Nota 4.8 *Com que volem que x i y en l'eq. (4.1) siguen nombres enters, aleshores podem afinar un poc més de quina forma ha de ser el nombre racional λ. Si posem $\lambda = \frac{p}{q}$, aleshores el denominador q ha de dividir alhora els coeficients a i b. Si anomenem $d = \text{m.c.d.}(a, b)$, i per tant $a = a'd$ i $b = b'd$, llavors el denominador q ha de ser un divisor de d i podem escriure la solució general de l'equació diofàntica com a*

$$x = x_0 + n\, b', \qquad y = y_0 - n\, a',$$

amb $n \in \mathbb{Z}$.

Per a trobar la solució particular que cal, el millor és fer servir la Identitat de Bèzout. Vegem-ne un exemple:

Exemple 4.9 *El famós problema dels ocells.*
Amb 100 *euros volem comprar* 100 *ocells. Sé que una cadernera val* 5 *euros, un canari,* 3*, i* 3 *lloros,* 2*. Quants en puc comprar de cada tipus?*

Doncs bé, si posem que x *és la quantitat de caderneres,* y *de canaris i* z *de lloros, aleshores hi tenim dues equacions:*

$$\begin{cases} 5x + 3y + \frac{2}{3}z & = 100, \\ x + y + z & = 100. \end{cases}$$

Si multipliquem la primera equació per 3 *i la segona per* 2*, obtenim:*

$$\begin{cases} 15x + 9y + 2z & = 300, \\ 2x + 2y + 2z & = 200. \end{cases}$$

Si ara a la primera li restem la segona, tenim una única equació diofàntica lineal:

$$13x + 7y = 100.$$

Cal primer trobar una solució particular. Com que $\text{m.c.d.}(13, 7) = 1$*, si hi apliquem la Identitat de Bèzout tenim que*

$$(-1) \cdot 13 + 2 \cdot 7 = 1.$$

Si multipliquem ara per 100*, obtenim*

$$(-100) \cdot 13 + 200 \cdot 7 = 100.$$

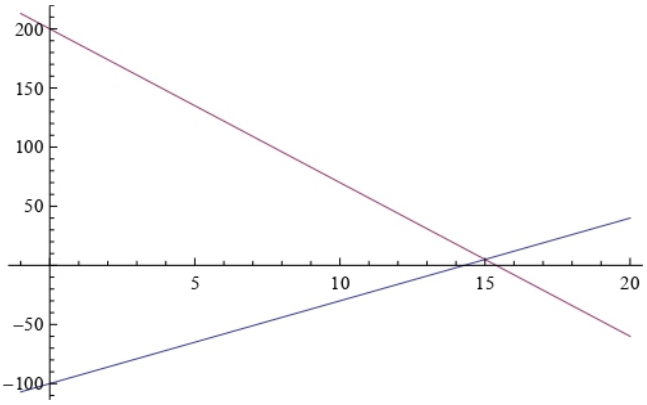
Per tant, una solució particular és

$$x_0 = -100, \qquad y_0 = 200.$$

La solució general serà, per tant,

$$\begin{cases} x & = -100 + 7\lambda, \\ y & = 200 - 13\lambda, \end{cases}$$

amb $\lambda \in \mathbb{Q}$*. Ara hem de trobar un valor del paràmetre* λ *que done valors positius a* x *i a* y*.*
Les expressions $-100+7\lambda$ *i* $200-13\lambda$ *són les equacions paramètriques de dues rectes. Hem de determinar per a quins valors de* λ *ambdues rectes estan en el semipla positiu.*



Representació de les dues rectes

Un càlcul senzill mostra que

$$-100 + 7\lambda \geq 0 \Leftrightarrow \lambda \geq \frac{100}{7} \approx 14.28.$$

D'una altra banda,

$$200 - 13\lambda \geq 0 \Leftrightarrow \lambda \leq \frac{200}{13} \approx 15.38.$$

Així doncs, si volem que tant x com y siguen positives, haurem de triar

$$14.28 \leq \lambda \leq 15.38.$$

Si agafem $\lambda = 15$, aleshores

$$\begin{cases} x &= -100 + 7 \cdot 15 = -100 + 105 = 5, \\ y &= 200 - 13 \cdot 15 = 200 - 195 = 5. \end{cases}$$

Amb la qual cosa

$$z = 100 - x - y = 90.$$

Per tant, haurem de comprar 5 caderneres, 5 canaris i 90 lloros!

En la darrera part del primer capítol, secció 1.7, vam estudiar com calcular quantes solucions naturals tenien equacions com per exemple $ax+by = c$, amb $a, b, c \in \mathbb{N}$. Aquesta equació no és més que un exemple d'equació diofàntica lineal, i ara ja sabem com calcular totes les solucions enteres. Només queda determinar quines d'aquestes solucions enteres estan formades per nombres naturals. Si en el primer capítol sabíem dir quantes solucions hi ha, en aquest darrer capítol també podem determinar-les explícitament. Vegem-ne un exemple.

Exemple 4.10 *Volem calcular totes les solucions naturals de l'equació*

$$3x + 5y = 44.$$

Recordeu que ja sabem calcular quantes solucions hi ha. La resposta la dóna el coeficient de x^{44} de la funció generatriu

$$\begin{aligned} f(x) &= (1 + x^3 + x^6 + x^9 + \dots)(1 + x^5 + x^{10} + x^{15} + \dots) \\ &= \tfrac{1}{1-x^3}\tfrac{1}{1-x^5} \\ &= \tfrac{1-x^{15}}{1-x^3}\tfrac{1-x^{15}}{1-x^5}\tfrac{1}{(1-x^{15})^2} \\ &= (1 + x^3 + x^6 + x^9 + x^{12})(1 + x^5 + x^{10})(1 - x^{15})^{-2} \\ &= (1 + x^3 + x^6 + x^9 + x^{12})(1 + x^5 + x^{10}) \\ &\qquad \left(\tbinom{-2}{0} - \tbinom{-2}{1}x^{15} + \tbinom{-2}{2}x^{30} + \dots\right) \end{aligned}$$

L'únic producte que contribueix al coeficient de x^{44} és x^9 per x^5 per $\binom{-2}{2}x^{30}$. Per tant, el coeficient és $\binom{-2}{2} = (-1)^2\binom{2+2-1}{2} = \binom{3}{2} = 3$.

És a dir, sabem que hi ha tres solucions enteres. Determinem-les explícitament.
La identitat de Bèzout diu que

$$-3 \cdot 3 + 2 \cdot 5 = 1.$$

(Encara que també podríem posar $2 \cdot 3 + -1 \cdot 5 = 1$.)
Si multipliquem per 44, tenim que

$$3 \cdot (-132) + 5 \cdot 88 = 44.$$

Així, una solució particular és $x_0 = -132, y_0 = 88$.
La solució general serà

$$\begin{cases} x &= -132 + 5 \cdot n, \\ y &= 88 - 3 \cdot n, \end{cases}$$

amb $n \in \mathbb{Z}$.

Per a que x siga positiu cal que

$$-132 + 5 \cdot n > 0 \Longleftrightarrow n > \frac{132}{5} > 26.$$

Per a que y siga positiu cal que

$$88 - 3 \cdot n > 0 \Longleftrightarrow n < \frac{88}{3} < 30.$$

Per tant, només tenim 3 possibles valors per a la n: 27, 28 i 29.

$$\begin{aligned} \text{Si } n &= 27 \quad \Rightarrow x = 3, y = 7, \\ \text{Si } n &= 28 \quad \Rightarrow x = 8, y = 4, \\ \text{Si } n &= 29 \quad \Rightarrow x = 13, y = 1. \end{aligned}$$

4.4.1 *Altres equacions diofàntiques*

L'equació diofàntica més famosa en matemàtiques és la que apareix en l'enunciat del darrer teorema de Fermat, conegut actualment també com a teorema de Wiles-Fermat. Aquest teorema afirma que l'equació diofàntica

$$x^n + y^n = z^n$$

no té cap solució entera per a $n > 2$ i sent x, y i z diferents de zero. Va ser precisament en el marge d'una pàgina d'una edició del llibre *Aritmètica* de Diofant d'Alexandria on al voltant de l'any 1680, Fermat va escriure que sabia demostrar que eixa equació no tenia solucions enteres, però que l'estretor del marge no li permetia escriure res més. Van passar més de tres segles fins que una de les conjectures més famoses de la matemàtica va quedar finalment resolta per Andrew Wiles l'any 1997.

Per a $n = 2$ sí que hi ha solucions, ja que l'equació no és més que el teorema de Pitàgores

$$x^2 + y^2 = z^2.$$

Segurament recordareu el clàssic exemple del triangle rectangle amb catets de longituds 3 i 4 i d'hipotenusa 5. No és l'única solució. N'hi ha infinites. Per exemple: si $p, q, r \in \mathbb{Z}$, aleshores

$$\begin{cases} x &= r(p^2 - q^2), \\ y &= 2rpq, \\ z &= r(p^2 + q^2) \end{cases}$$

no només són nombres enters, sinó que verifiquen també $x^2 + y^2 = z^2$.

4.5 Primer teorema de Fermat - Teorema d'Euler

Hi ha dos resultats de la Teoria de nombres que són, juntament amb el Teorema xinès del residu, la base de l'aplicació d'aquesta en la construcció d'un sistema criptogràfic.
Tal com hem dit abans (v. 4.4.1), Fermat estava interessat en l'equació $x^n + y^n = z^n$. És de suposar que primer pensaria en el cas concret en què l'exponent és un nombre primer p, $x^p + y^p = z^p$, i que calcularia residus mòdul p en ambdós membre de l'equació. En calcular uns pocs casos arribaria a una conjetura que de seguida va poder provar (aquesta sí).

4.5.1 *Primer Teorema de Fermat*

El primer teorema de Fermat és un dels teoremes clàssics de teoria de nombres relacionat amb la divisibilitat.

Teorema 4.5.1 *(Primer teorema de Fermat)*
Siga p un nombre primer. Per a qualsevol enter a

$$a^p \equiv a \pmod{p}$$

i per a qualsevol enter a no divisible per p ($p \nmid a$), tenim que

$$a^{p-1} \equiv 1 \pmod{p}. \tag{4.2}$$

Demostració. Suposem primer que p no divideix a. En $\mathbb{Z}_p$ considerem les classes

$$\overline{0a}, \overline{1a}, \overline{2a}, \ldots, \overline{(p-1)a}$$

i demostrem que totes elles són diferents. Com que a i p són coprimers, aleshores existeixen u, v, enters, tal que $au + pv = 1$. Això implica que $au \equiv 1 \pmod{p}$, per tant a és invertible en $\mathbb{Z}_p$, és a dir, $a^{-1} \in \mathbb{Z}_p$. Ara si $\overline{ia} = \overline{ja}$ amb $i \neq j$, llavors $ia = ja$ en $\mathbb{Z}_p$, per tant $iaa^{-1} = jaa^{-1}$, implica que $i = j$, la qual cosa és una contradicció.
D'altra banda, cap element de $\{\overline{0a}, \overline{1a}, \overline{12}, \ldots, \overline{(p-1)a}\}$ pot ser 0 mòdul p, ja que si k és un dels números $\{1, 2, 3, \ldots, p-1\}$, k no és divisible per p i tampoc a. Llavors ka no és divisible per p. Així doncs es té que el conjunt de classes $\{\overline{0a}, \overline{1a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$ està format per p classes diferents, i coincideix amb $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{(p-1)}\}$. Evidentment $\overline{0a} = \overline{0}$, aleshores tenim la següent igualtat entre conjunts:

$$\{1, 2, 3, \ldots, p-1\} = \{a, 2a, 3a, \ldots, (p-1)a\}$$

Multiplicant els elements de l'esquerra i de la dreta obtenim

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

És a dir

$$p \mid [(p-1)!(a^{p-1}-1)].$$

Com que tots els factors de $(p-1)!$ són menors de p, cap té a p com a factor, i d'altra banda, si el producte d'elements de $(p-1)!$ donara com a resultat un múltiple de p, (o el mateix p), llavors p no seria primer. Tot això ens porta al fet que el m.c.d.$((p-1)!, p) = 1$, i pel lema d'Euclides (Si $a|bc$ i m.c.d.$(a,b) = 1$ llavors $a|c$) $p|a^{p-1}-1$ i en conseqüència $a^{p-1} \equiv 1 \pmod{p}$. I el segon resultat queda demostrat.
Ara, si $p \nmid a$, pel resultat anterior, $a^{p-1} \equiv 1 \pmod{p}$. Multiplicant per a s'obte $a^p \equiv a \pmod{p}$.
Si $p|a$ aleshores $a \equiv 0 \pmod{p}$, aleshores $a^p \equiv 0^p \pmod{p}$, i per tant $a^p \equiv 0 \pmod{p}$ i $a^p \equiv a \pmod{p}$. □

Sense que servisca de precedent, oferim ara una altra via de demostració del mateix resultat.
Demostració. (Prova alternativa)
Comprovem primer que si p és un nombre primer, i si $i \in \{2, 3, \ldots, p-1\}$, aleshores el nombre combinatori $\binom{p}{i}$ sempre és divisible per p. En efecte, el nombre combinatori

$$\binom{p}{i} = \frac{p(p-1)(p-2)\ldots(p-i+1)}{i(i-1)\ldots 2.1} \in \mathbb{N}.$$

Com que el resultat és un nombre natural, no un racional, aleshores, tots els factors en el denominador s'han de poder simplificar amb factors del numerador. Com que p és primer, i els factors del denominador són menors que p, aleshores, podem assegurar que en la simplificació sempre sobreviurà el primer factor, el "p". Per tant, $\binom{p}{i} = p \cdot m$.

Passem ara a demostrar que $a^p \equiv a \pmod{p}$. Ho farem per inducció sobre a.
Si $a = 1$, tenim directament que $a^p = 1$.
Suposem ara que $a^p \equiv a \pmod{p}$ i anem a demostrar que $(a+1)^p \equiv a+1 \pmod{p}$.
Si apliquem la fórmula del binomi de Newton, tenim que

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a^1 + 1.$$

Tots els termes d'aquesta suma, tret del primer i del darrer, són divisibles per p. És a dir, que podem escriure que

$$(a+1)^p = a^p + p \cdot m + 1.$$

Aplicant ara la hipòtesi d'inducció,

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

Una vegada ja hem demostrat que $a^p \equiv a \pmod{p}$, provarem ara que per a qualsevol enter a no divisible per p,

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

Si a no és divisible per p, aleshores a és un element invertible en $\mathbb{Z}_p$. Multiplicant l'expressió $a^p \equiv a \pmod{p}$ per l'invers de a tenim que $a^{p-1} \equiv 1 \pmod{p}$. □

Una aplicació del primer teorema de Fermat és per exemple:

Exemple 4.5.2 *Calcular el residu de la divisió de* 2^{98} *per* 101.
Com que 101 *és primer, utilitzant el primer teorema de Fermat tenim que*

$$2^{100} \equiv 1 \pmod{101} \Longleftrightarrow 2^{98} \cdot 2^2 \equiv 1 \pmod{101} \Longleftrightarrow 2^{98} \cdot 4 \equiv -100 \pmod{101}$$

Com que 4 i 101 són primers entre sí, podem dividir l'última congruència per 4 i obtenim

$$2^{98} \equiv -25 \pmod{101} \Longleftrightarrow 2^{98} \equiv 76 \pmod{101}.$$

Per tant el residu de la divisió de 2^{98} *per* 101 *és 76.*

Corol·lari 4.5.3 *Si* p *és un nombre primer positiu,* $p \nmid a$ *i si* $n \equiv m \pmod{(p-1)}$*, aleshores*

$$a^n \equiv a^m \pmod{p}.$$

Demostració. Suposem que $n > m$. Com que $p-1$ divideix $n-m$, tenim que

$$n = m + c(p-1)$$

per a algun enter positiu c. Si multipliquem ara la congruència obtinguda en l'Eq. (4.2) $a^{p-1} \equiv 1 \pmod{p}$ per ella mateixa c vegades i aleshores per $a^n \equiv a^m \pmod{p}$, obtindrem el resultat desitjat. □

Exemple 4.5.4 *Quin és el darrer dígit de* $2^{1000000}$ *quan s'escriu en base* 7*?*
Doncs bé, noteu que ens estan preguntant pel residu de $2^{1000000}$ *mòdul* 7*. Per tal d'aplicar el corol·lari anterior, hem de reduir l'exponent a un nombre menor. Si agafem* $p = 7$*, i* $n = 1000000$*, hem de trobar un* m *convenient tal que* $1000000 \equiv m \pmod{6}$*. Com que*

$$1000000 = 166666 \cdot 6 + 4.$$

Això vol dir que podem agafar $m = 4$*. Si apliquem ara el corol·lari, tenim que*

$$2^{1000000} \equiv 2^4 = 16 \equiv 2 \pmod{7}.$$

Per tant, el darrer dígit de $2^{1000000}$ *quan s'escriu en base* 7 *és el* 2*.*

4.5.2 *Teorema d'Euler*

I si en l'exemple anterior, aquell en què ens demanaven pel darrer dígit de $2^{1000000}$ en base 7, ens hagueren preguntat pel darrer dígit ara però quan s'escriu en base 77.

No podríem aplicar el Teorema de Fermat perquè 77 és un nombre compost. Afortunadament, hi ha un resultat més general, conegut com a Teorema d'Euler-Fermat, perquè és una generalització del primer teorema de Fermat. Necessitem primer definir l'anomenada funció Φ d'Euler.

Definició 4.5.5 *Donat un nombre natural,* n*, definim* $\Phi(n)$ *com la quantitat de nombres naturals menors que* n *que són relativament primers amb* n*. Notacionalment,*

$$\Phi(n) = \left|\{a \in \{1, 2, \ldots, n-1\} \text{ tal que m.c.d.}(a, n) = 1\}\right|.$$

L'aplicació Φ *s'anomena funció* Φ *d'Euler.*

Calculem la funció Φ d'Euler per a qualsevol nombre natural com a aplicació del Principi d'inclusió-exclusió (Teorema 1.4.1).

Teorema 4.5.6 *Siga $n \in \mathbb{N}$ amb $n = p_1^{\alpha_1}\, p_2^{\alpha_2} \ldots\, p_k^{\alpha_k}$ la seua descomposició en factors primers. Llavors*

$$\boxed{\Phi(n) = n \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right).}$$

Demostració. El que hem de calcular és el cardinal del conjunt de nombres naturals positius i menor o igual a n que són coprimers amb n, o equivalentment, el cardinal del conjunt de nombres naturals positius i menor o igual a n que no són divisibles per cap dels nombres primers $p_1, p_2, \ldots, p_k$.
Tenint en compte que si $a|b$ amb a, b naturals, el nombre de múltiples de a que no excedeixen a b és el quocient $\frac{a}{b}$, així doncs, per tal d'aplicar el Principi d'inclusió-exclusió, considerem els següents conjunts: $X = \{1, 2, \ldots, n\}$ i, per a tot $i = 1, 2 \ldots, k$,

$$A_i = \{x \in X \text{ tal que } p_i|x\} = \{\text{Conjunt de múltiples de } p_i \text{ que no excedeixen de } n\}.$$

El que hem de calcular és

$$|X - \bigcup_{i=1}^{k} A_i|.$$

Clarament tenim que

$$|X| = n, |A_i| = \frac{n}{p_i}, \quad |A_i \cap A_j| = \frac{n}{p_i p_j}, \quad |A_i \cap A_j \cap A_\ell| = \frac{n}{p_i p_\ell} \ldots$$

ja que, per exemple, per a $i \neq j$, p_i i p_j, són primers, i els múltiples de tots dos són els que siguen múltiples del producte $p_i \cdot p_j$. De la mateixa manera, $|A_i \cap A_j \cap A_\ell| = \frac{n}{p_i p_j p_\ell}$ per a $i \neq j \neq \ell$, i així successivament. Si apliquem ara la fórmula (1.2), tenim que

$$\begin{aligned} |X - \textstyle\bigcup_{i=1}^{k} A_i| &= n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \cdots + \frac{n}{p_k} - \frac{n}{p_1 p_2} - \cdots - \frac{n}{p_{k-1} p_k} + \cdots + (-1)^{k-1} \frac{n}{p_1 p_2 \cdots p_k}\right) \\ &= n\left(1 - \frac{1}{p_1} - \frac{1}{p_2} - \cdots - \frac{1}{p_k} + \frac{1}{p_1 p_2} + \cdots + \frac{1}{p_{k-1} p_k} + \cdots + (-1)^k \frac{1}{p_1 p_2 \cdots p_k}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) = \Phi(n) \end{aligned} .$$

□

Exemple 4.5.7 *Com que* $23760 = 2^4 \cdot 3^3 \cdot 5 \cdot 11$*, aleshores*

$$\begin{aligned} \Phi(23760) &= 23760\left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{3}\right)\left(1 - \tfrac{1}{5}\right)\left(1 - \tfrac{1}{11}\right) \\ &= 2^4 \cdot 3^3 \cdot 5 \cdot 11 \cdot \tfrac{1}{2} \cdot \tfrac{2}{3} \cdot \tfrac{4}{5} \cdot \tfrac{10}{11} \\ &= 2^3 \cdot 3^2 \cdot 2 \cdot 4 \cdot 10 \\ &= 2^7 \cdot 3^2 \cdot 5 \\ &= 5760. \end{aligned}$$

Les conseqüències immediates del teorema 4.5.6 són les següents:

Proposició 4.5.8 *1. Si p és un nombre primer, aleshores*

$$\boxed{\Phi(p) = p - 1}.$$

2. Si p és un nombre primer, aleshores

$$\boxed{\Phi(p^\alpha) = p^\alpha \left(1 - \frac{1}{p}\right)} = p^\alpha - p^{\alpha-1}.$$

3. Φ és una funció multiplicativa quan els factors són coprimers. És a dir, si m.c.d.$(m, n) = 1$, aleshores

$$\boxed{\Phi(mn) = \Phi(m)\Phi(n).}$$

4. Si p i q són nombres primers, aleshores

$$\boxed{\Phi(pq) = (p-1)(q-1).}$$

Demostració. Les dos primers resultats són immediats. Demostrem el tercer.
Si les descomposicions de m i n són respectivament:

$$m = p_1^{\alpha_1}\, p_2^{\alpha_2} p_3^{\alpha_3} \dots\, p_r^{\alpha_r} \quad \text{y} \quad n = q_1^{\beta_1} q_2^{\beta_2} q_3^{\beta_3} \dots q_s^{\beta_s},$$

com que cap factor de totes dues descomposicions coincideix es té que

$$m \cdot n = p_1^{\alpha_1}\, p_2^{\alpha_2} p_3^{\alpha_3} \dots\, p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} q_3^{\beta_3} \dots q_s^{\beta_s}$$

on tots els factors són primers diferents entre si. Per tant

$$\Phi(m \cdot n) = mn \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \prod_{j=1}^{s} \left(1 - \frac{1}{q_j}\right) = \Phi(m)\Phi(n).$$

El quart resultat és obvi aplicant l'anterior. □

En 1760, Euler va demostrar la següent generalització del primer Teorema de Fermat que es coneix com a Teorema d'Euler.

Teorema 4.5.9 (Teorema d'Euler)
Siga $a \in \mathbb{Z}$ tal que m.c.d.$(a, n) = 1$*, aleshores*

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

Demostració. La demostració és semblant a la primera de les demostracions del Primer Teorema de Fermat.
Considerem el conjunt

$$R = \{x \in \{1, 2, \ldots, n-1\} \text{ tal que } \text{m.c.d.}(x, n) = 1\}.$$

Noteu que R és el grup d'unitats de $\mathbb{Z}_n$ i que el seu cardinal és $|R| = \Phi(n)$.

Construïm ara dos conjunts de classes en $\mathbb{Z}_n$:

$$C_1 = \{\overline{ax} \ / \ x \in R\} \quad \text{i} \quad C_2 = \{\overline{x} \ / \ x \in R\}.$$

Anem a demostrar, de forma similar en què es va fer la demostració del Primer Teorema de Fermat, que tots dos conjunts són iguals en aquest cas.

Abans de res notem que tant a, com qualsevol $x \in R$, són elements invertibles en l'anell $\mathbb{Z}_n$, i anomenem aquests inversos a^{-1} i x^{-1}, respectivament.

$C_1 \subseteq C_2$: Siga $\overline{ax} \in C_1$, llavors podem triar com a representant d'aquesta classe y entre 0 i $n-1$, de manera que $ax \equiv y \pmod{n}$. Multiplicant aquesta relació per $x^{-1}a^{-1}$ obtenim $x^{-1}a^{-1}y \equiv 1 \pmod{n}$, és a dir y és invertible. és a dir, $\text{m.c.d.}(y, n) = 1$. Per tant $y \in R$, això és tant com dir que $\overline{ax} = \overline{y}$. Per tant, $\overline{ax} \in C_2$.

$C_2 \subseteq C_1$: Siga $x \in R$, vegem que $\overline{x} \in C_1$. Per a això siga $\alpha \in \{0, 1, \ldots, n-1\}$ tal que $a^{-1}x \equiv \alpha \pmod{n}$. Clarament α és invertible ja que $x^{-1}a\alpha \equiv 1 \pmod{n}$, la qual cosa ens permet afirmar que $\alpha \in R$. A més a més, $\overline{x} = \overline{a\alpha}$ per tant $\overline{x} \in C_1$.

Una vegada ja hem comprovat que $C_1 = C_2$, si multipliquem els elements de tots dos conjunts, i anomenant P al product dels elements en C_2, s'obté:

$$a^{\Phi(n)}P \equiv P \pmod{n}.$$

Per ser producte d'invertibles, P també és invertible. Aleshores $a^{\Phi(n)} \equiv 1 \pmod{n}$. □

Exemple 4.5.10 *Quin és el darrer dígit de* $2^{1000000}$ *quan s'escriu en base* 77*?*
Doncs bé, com que

$$\Phi(77) = \Phi(7 \cdot 11) = \Phi(7)\Phi(11) = 6 \cdot 10 = 60,$$

aleshores, donat que $\text{m.c.d.}(2, 77) = 1$*, el Teorema d'Euler afirma que*

$$2^{60} \equiv 1 \pmod{77}.$$

Com que $1000000 = 16666 \cdot 60 + 40$*, aleshores*

$$2^{1000000} \equiv 2^{40} \pmod{77}.$$

Ara és més senzill calcular $2^{40} \pmod{77}$*. Per exemple,* $2^{10} = 1024 = 13 \cdot 77 + 23 \equiv 23 \pmod{77}$*, i* $23^4 \equiv 23 \pmod{77}$*. Per tant, el darrer dígit de* $2^{1000000}$ *en base* 77 *és* 3*.*

Exemple 4.5.11 *Per a trobar els dos últims dígits de* 3^{1486}*, un possible enfocament és trobar el valor de la seua congruència mòdul 100. El número 100 no és primer, però sí que és cert que m.c.d.*$(3, 100) = 1$*, situació que ens permet fer ús del Teorema d'Euler. Aquest resultat afirma que*

$$3^{\Phi(100)} \equiv 1 \pmod{100}.$$

Ara, com que $100 = 2^2 \cdot 5^2$*, aleshores*

$$\Phi(100) = \Phi(2^2) \cdot \Phi(5^2) = (2^2 - 2)(5^2 - 5) = 40$$

i per tant, $3^{40} \equiv 1 \pmod{100}$*. D'aquesta manera, com que* $1486 = 40 \cdot 37 + 6$*, podem escriure*

$$\begin{aligned} 3^{1486} &= 3^6 \cdot (3^{40})^{37} \\ &\equiv 3^6 \cdot 1^{37} \pmod{100} \\ &\equiv 729 \pmod{100} \\ &\equiv 29 \pmod{100} \end{aligned}$$

Així, finalment, els dos últims dígits de 3^{1486} *són* 29*.*

4.6 Aplicació a la Criptografia

Criptografia de clau pública i privada

La criptografia constitueix el conjunt de procediments que s'utilitzen per a transformar informació, de tal manera que aquesta siga "invisible" per a observadors sense autorització. En criptografia, RSA (Rivest, Shamir i Adleman) és un sistema criptogràfic de clau pública desenvolupat en 1979. És el primer i més utilitzat algorisme d'aquest tipus per a la transmissió segura de dades a través de canals insegurs. En aquest sistema, cada usuari té una clau pública, que és, com el seu nom indica, de domini públic, que consisteix en una funció per a xifrar missatges i una clau privada, que només ell coneix.
Vegem com es poden usar els resultats obtinguts anteriorment per a la construcció d'un sistema que permeta la comunicació segura entre un emissor, que anomenarem E, i un receptor, R. Se suposa que tots dos poden executar en les seues respectives màquines les operacions que desitgen, i guardar la informació que precisen, sense que aquesta siga coneguda per ningú. No obstant això, quan l'emissor envie un missatge encriptat al receptor no pot estar segur que el canal no siga espiat, i per això el seu objectiu és que, encara que aquest missatge encriptat siga interceptat per un espia, aquest no podrà desencriptar-lo, ni per tant entendre-ho. Es creu que RSA serà segur mentre no es coneguen formes ràpides de descompondre un número gran en producte de primers.
El pas previ és convertir el missatge a manera numèrica, és a dir, representem cada lletra (incloent els espais i els signes de puntuació) per un número.
Els passos són:

1. En privat, el receptor R tria dos nombres primers p i q molt grans (d'unes 100 xifres cadascun), i els multiplica, obtenint $n = pq$ tals que n siga primer amb qualsevol *possible* paraula d'un text.

2. També en privat, el receptor obté el valor de la funció multiplicadora d'Euler, $\Phi(n)$, que com sabem, serà en aquest cas igual a $\Phi(n) = \Phi(pq) = \Phi(p)\Phi(q) = (p-1)(q-1)$, atés que p i q són primers entre si, i cadascun d'ells és primer.

3. En privat, el receptor R tria un nombre e tal que $1 < e < \Phi(n)$ de manera que siga primer relatiu amb $\Phi(n)$, i calcula el seu invers mòdul $\Phi(n)$, que anomenarem $d \equiv e^{-1} \pmod{\Phi(n)}$.

4. R es guarda en secret el parell de nombres (d, n), la qual cosa és l'anomenada **clau privada**, i fa públic el parell de nombres (e, n), als quals anomenarem la seua **clau pública**.

5. E, que desitja enviar-li el missatge confidencial x a R, l'encripta de la següent manera:

$$Enc(x) \equiv x^e \pmod{n}$$

   cosa que pot fer, perquè coneix els nombres e i n que R va fer públics. Ara, envia el nombre $Enc(x)$.

6. R rep un nombre $y = Enc(x)$ i executa amb ell la següent operació:

$$Des(y) \equiv y^d \pmod{n}$$

   cosa que pot fer, perquè ell mateix sí que coneix el valor de la seua pròpia clau privada, d. El que aconsegueix és:

$$Des(y) = Enc(x)^d \equiv (x^e)^d = x^{1+m\Phi(n)} = x \cdot (x^{\Phi(n)})^m \overset{\text{T.E.}}{\equiv} x \pmod{n}.$$

   ja que d i n eren inversos mòdul $\Phi(n)$, i per tant ed és un cert nombre que pertany a la classe de 1 mòdul $\Phi(n)$. (T.E. = Teorema d'Euler i en haver triat n primer amb qualsevol possible paraula del text, es podia aplicar el teorema d'Euler). En resum, R pot conéixer el missatge x que E li va enviar.

Ens queden encara alguns punts per aclarir que són necessaris per a la comprensió total de l'algorisme i del seu ús. Concretament:

1. Si l'espia intercepta el número y, no pot executar l'operació de desencriptat perquè no coneix d. L'única forma en què poguera conéixer-la és calculant-la com la inversa de e (que sí que és pública) en mòdul $\Phi(n)$, i això no és possible perquè no coneix $\Phi(n)$. Així i tot, l'alumne pensarà que no és difícil conéixer $\Phi(n)$ donat n (que és públic): es descompon n en factors primers, la qual cosa donaria $n = pq$, i es calcula $\Phi(n)$ com a $(p-1)(q-1)$. El problema està en el fet que descompondre un nombre molt gran en factors primers és molt complex (avui en dia, la descomposició d'un nombre de 200 xifres portaria un milió d'anys de càlcul, fins i tot al més potent ordinador en ús. La clau està precisament ací: calcular un nombre donada la seua descomposició en factors primers és trivial, perquè basta multiplicar els factors. No obstant això, donat un nombre natural, trobar els seus factors és costosíssim, en temps i en recursos.

2. p i q han de ser primers. Com sabem que ho són? Una possibilitat és efectivament descompondre'ls. Encara que hàgem vist que això és en la pràctica impossible per a n, pot encara estar al nostre abast per a p i q, que són molt més xicotets. En qualsevol cas, i fins i tot si no fora així, existeixen tests probabilístics que decideixen, en un temps lineal amb la grandària del nombre, si aquest és o no primer amb ínfima probabilitat d'equivocar-se. La forma exacta de tals tests queda fora de l'abast d'aquest tema.

3. En el tercer pas de l'algorisme que executa el receptor per a generar la seua clau pública hem dit que donat $\Phi(n)$ es tria un nombre e primer relatiu amb ell. Això es pot fer prenent e a l'atzar, i calculant mitjançant l'algorisme d'Euclides el màxim comú divisor de e i $\Phi(n)$. Si és 1, els nombres són primers entre si; si no, haurem de triar un altre e. Com vam dir, l'algorisme estés d'Euclides és de cost lineal amb la grandària de e, i això és per tant factible.

4. En el mateix pas es calcula la inversa de e mòdul $\Phi(n)$. Una possibilitat de calcular inverses és usar l'algorisme estés d'Euclides, el qual, donats e i $\Phi(n)$, ens retorna el seu m.c.d., que serà 1, ja que e i $\Phi(n)$ van ser triats com a primers entre si, i també els dos nombres d i h tals que $d \cdot e + h \cdot \Phi(n) = 1$. d serà llavors invers de e mòdul $\Phi(n)$, atés que el seu producte amb e és múltiple de $\Phi(n) + 1$. Si la d retornada per l'algorisme fóra negativa, podem sumar-li $\Phi(n)$ per a obtindre el representant positiu més xicotet de la seua classe, el qual per descomptat també dona 1 en multiplicar-lo per e. En principi, una possibilitat alternativa de calcular l'invers seria usar el teorema d'Euler, amb el que $d \equiv e^{\Phi(\Phi(n))-1} \pmod{\Phi(n)}$. No obstant això, això requeriria el càlcul de $\Phi(\Phi(n))$, i per tant, la descomposició en factors primers de $\Phi(n)$, la qual cosa és impracticable, perquè $Phi(n)$ és un nombre quasi del mateix ordre que n; segons hem argumentat en el primer aclariment, això seria costosíssim.

5. En la pràctica, l'operació de desencriptat es pot realitzar de manera més eficient guardant en la clau privada no sols d, sinó també p i q, la qual cosa transforma aquesta operació en la resolució d'un sistema de dues equacions en congruències amb dues incògnites; per a això es fa servir el Teorema Xinés del Residu.

4.7 Exercicis

1. Per a les següents parelles de nombres enters, trobeu el màxim comú divisor fent servir l'algorisme d'Euclides i trobeu la combinació lineal d'ambdós que dóna lloc al màxim comú divisor:

$$(a)\ 26, 19; \quad (b)\ 187, 34; \quad (c)\ 841, 160; \quad (d)\ 2613, 2171.$$

2. Comproveu que m.c.d.$(43247, 273240) = 1$ i calcula l'invers de 43247 mòdul 273240,
(Sol.: 113423.)

3. Resoleu les equacions:
   (a) $3x \equiv 4 \pmod{7}$.
   (b) $3x \equiv 4 \pmod{12}$.
   (c) $9x \equiv 12 \pmod{21}$.
   (d) $27x \equiv 25 \pmod{256}$.
   (e) $27x \equiv 72 \pmod{900}$.
   (f) $103x \equiv 612 \pmod{676}$.

4. Repassarem alguns dels criteris de divisibilitat que vàrem aprendre a l'escola.

   Demostreu que un nombre enter, escrit en base 10, és divisible...

   (a) per 2 si i només si l'última xifra és divisible per 2.

   (b) per 3 si i només si la suma dels seus dígits és divisible per 3.

   (c) per 4 si i només si el nombre determinat per les dues últimes xifres és divisible per 4.

   (d) per 5 si i només si l'última xifra és 0 o 5.

   (e) per 6 si i només si és divisible per 2 i per 3.

   (f) per 7 si i només si quan se li lleva la xifra de les unitats i al resultat se li resta el doble d'eixa xifra eliminada, llavors el resultat és divisible per 7. (Per exemple, per a saber si 266 és divisible per set, reduïm el problema a $26 - 2 \cdot 6 = 26 - 12 = 14$, i 14 síque és divisible per 7, per tant 266 també.)

   (g) per 8 si i només si és divisible tres vegades per 2.

   (h) per 9 si i només si la suma dels seus dígits és divisible per 9.

   (i) per 10 si i només si l'última xifra és 0.

   (j) per 11 si i només si la suma de les xifres en les posicions senar menys la suma de les xifres en les posicions parelles és divisible per 11.

   (k) per 12 si i només si és divisible per 4 i per 3.

   (l) per 13 si i només si quan se li lleva la xifra de les unitats i al resultat se li suma quatre vegades eixa xifra eliminada, llavors el resultat és divisible per 13. (Per exemple, per a saber si 351 és divisible per tretze, reduïm el problema a $35 + 4 \cdot 1 = 35 + 4 = 39$, i $39 = 3 \cdot 13$ síque és divisible per 13, per tant 351 també.)

   (Noteu que els criteris per al 7 i per al 13 són recursius. El que es fa és reduir el nombre a estudiar en cada pas a un altre nombre de menor magnitud. Aquests dos criteris els he d'agrair als estudiants de la III Escola Conjunta de Matemàtiques Universidad Autònoma de San Luis Potosí(Mèxic) - Universitat de València.)

5. Demostreu que $n^5 - n$ sempre és divisible per 30.

6. Demostreu que si p és un nombre primer major que 5, aleshores $p^7 - p^3$ sempre és divisible per 240.

   (Ajuda: $p^7 - p^3 = p^3(p^4 - 1)$ i només ens hem de preocupar de $p^4 - 1 = (p^2 + 1)(p^2 - 1) = (p^2 + 1)(p + 1)(p - 1)$. Pel teorema de Fermat, $p^4 - 1$ és divisible per 5 i $p^2 - 1$ és divisible per 3. A més $p^2 + 1$, $p + 1$ i $p - 1$ són divisibles per 2. Com que $5 \cdot 3 \cdot 2^3 = 120 = \frac{240}{2}$, veiem que encara falta un 2. Aquest factor es pot trobar argumentant que $p + 1$ i $p - 1$ són dos nombres parells "consecutius", aleshores algun dels dos, a més de ser divisible per 2, ho ha de ser també per 4.)

7. Quin pot ser el darrer dígit del quadrat d'un nombre hexadecimal? (és a dir, escrit en base 16.) (Sol.: $0, 1, 4, 9$.)

8. Un nombre natural, n, es diu que és un nombre perfecte si és igual a la suma de tots els seus divisors propis. Per exemple el 6 i el 28 són nombres perfectes ja que $6 = 1+2+3$ i $28 = 1+2+4+7+14$.

   Demostra el resultat següent ja conegut per Euclides: si p és un nombre natural tal que $2^p - 1$ és un nombre primer, aleshores $n = 2^{p-1}(2^p - 1)$ és un nombre perfecte.

9. Ara un problema relacionat amb l'anterior. Demostra que si $2^p - 1$ és un nombre primer, aleshores p és un nombre primer. Aquests nombres s'anomenen nombres primers de Mersenne.

   (Ajuda: Suposem que $p = ab$. Recorda quin era el valor de la suma $1 + x^a + x^{2a} + \cdots + x^{a(b-1)}$.)

10. Hem comprat 72 unitats d'un determinat producte a un preu unitari que no recordem. Només sabem que en total hem pagat menys de 100 euros. En el tiquet de compra que conservem només podem llegir dos dels dígits: "?0.6?". Quin era el preu unitari?

    (Sol.: 1.12.)

11. (Extret de "La Vie mode d'emploi" ("La vida. Instruccions d'ús") de Georges Perec)
    El nombre més enorme que es pot escriure amb només tres dígits és el 9^{9^9}. Donat la seua magnitud hi ha pocs ordinadors que el puguen escriure totalment. El que sí que podeu fer és calcular algunes de les seues congruències. Comproveu que

    (a) $9^{9^9} \equiv 1 \pmod 7$,

    (b) $9^{9^9} \equiv 5 \pmod{11}$,

    (c) $9^{9^9} \equiv 1 \pmod{13}$.

    Per cert, una pregunta sobre notacions. És clar que $9^{9^9} \neq \left(9^9\right)^9$, o no?, però... per què no cal posar parèntesi quan s'escriu $9^{9^9} = 9^{\left(9^9\right)}$?

12. Demostra que si p és un nombre primer, aleshores

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

    (Ajuda: Per una banda $p - 1 \equiv -1 \pmod p$, i per una altra banda, els factors $2 \cdot 3 \ldots (p-2)$ són tots invertibles, però cap d'ells és de grau 2. Per tant, cada factor del producte $2 \cdot 3 \ldots (p-2)$ té el seu invers (que no és ell mateix) en eixe producte. Així $2 \cdot 3 \ldots (p-2) \equiv 1 \pmod p$.)

13. Resoleu el problema dels pirates i el seu cuiner xinès, Exemple 4.2. (Sol.: 785.)

14. Trobeu el menor enter positiu que té residu igual que 1 quan el dividim per 11, igual que 2 quan el dividim per 12 i igual que 3 quan el dividim per 13.

15. Trobeu la menor solució entera de

$$\begin{cases} x & \equiv 2 \pmod 3, \\ x & \equiv 3 \pmod 5, \\ x & \equiv 4 \pmod{11}, \\ x & \equiv 5 \pmod{16}. \end{cases}$$

16. Trobeu la menor solució entera de

$$\begin{cases} 19x & \equiv 103 \pmod{900}, \\ 10x & \equiv 511 \pmod{841}. \end{cases}$$

(Sol.: $x = 58837$.)

17. Donat el sistema

$$\begin{cases} x & \equiv 4 \pmod 8, \\ x & \equiv a \pmod 6, \\ x & \equiv -1 \pmod{15}, \end{cases}$$

determineu el valor de $a \in \mathbb{Z}$ perquè tinga solució.

(Sol.: $a \equiv 2 \pmod 6$.)

18. Aquest és el trist final d'un avantpassat meu que va nàixer un diumenge. Per celebrar un dels seus aniversaris va viatjar a Nova York i va tenir la mala sort de morir allà, l'endemà del seu aniversari, a les torres Bessones. Aquest avantpassat tenia el costum de celebrar també cada mes de vida (i aquests els contava de 31 dies). Doncs bé, el dia que va faltar li mancaven exactament 3 setmanes per a una altra celebració d'aquestes. Amb les dades que us he donat, i suposant que un any té 365 dies, podeu dir-me quants anys tenia?

(Sol.: Siga x el nombre de dies que va viure. Si va faltar l'endemà del seu aniversari, això vol dir que $x \equiv 1 \pmod{365}$. Com que l'onze de setembre era dimarts, i ell va nàixer un diumenge, aleshores, $x \equiv 2 \pmod 7$. La informació sobre els mesos diu que $x \equiv -21 \pmod{31}$, o equivalentment, $x \equiv 10 \pmod{31}$. Amb tot això, tenim que $x = 15696$. Per tant, va viure 43 anys.)

19. Ha caigut en les meues mans, no diré com, un bitllet del qual em vull desprendre com abans millor. Si convide els meus amics a un sopar de 23 euros per cap, podré deixar una propina de 17 euros. Si el sopar fóra de 37 euros, aleshores la propina seria de 19, i si fóra de 51, puc arribar a ser així d'esplèndid, la propina seria de 41 euros. De quants euros era el bitllet?

20. Comproveu si les equacions diofàntiques lineals següents són resolubles i, en cas afirmatiu, trobeu les solucions corresponents:

$$153x - 85y = 102; \quad 153x - 85y = 101; \quad 172x - 88y = 808.$$

21. Sabem que les tecles blanques d'un piano reprodueixen periòdicament les set notes de l'escala musical Do, Re, Mi, Fa, Sol, La i Si. Per tant, encara que el piano tinga moltes tecles, només podem sentir les set notes de l'escala, això sí, en diverses octaves. Els pianos reals tenen un nombre limitat de tecles, però per al nostre problema ens imaginarem un piano amb un teclat tan llarg com calga. Suposarem també que pitgem només les tecles blanques.

    Primer pitgem el primer Do que tenim per l'esquerra. A continuació, toquem la tecla següent, la qual naturalment serà un Re. Després ens saltem una tecla i toquem el Fa. Ara saltem dues tecles i toquem el Si. Seguidament saltem tres tecles i toquem el Fa, ja en la segona octava. I continuem el procés saltant cada vegada una tecla més que la vegada anterior. Suposem que hem arribat a tocar 7.000 tecles (recordeu que hem suposat que el nostre piano té tantes tecles com vulguem). I plantegem tres preguntes:

    (a) Quina és l'última nota que hem tocat?

    (b) Quantes vegades haurem tocat la nota Do?

    (c) Hi ha alguna nota que no s'haja tocat mai?

    (Sol.: Primer fem la correspondència

    $$\begin{aligned} \text{Do} &\leftrightarrow 0, \\ \text{Re} &\leftrightarrow 1, \\ \text{Mi} &\leftrightarrow 2, \\ \text{Fa} &\leftrightarrow 3, \\ \text{Sol} &\leftrightarrow 4, \\ \text{La} &\leftrightarrow 5, \\ \text{Si} &\leftrightarrow 6. \end{aligned}$$

    Segon, definim la successió per l'equació en diferències finites de primer ordre

    $$a_{n+1} = a_n + n,$$

    amb la condició inicial $a_1 = 0$. En realitat, la successió que volem és $a_n \pmod 7$.

    El terme general de la successió és

    $$a_n = \frac{(n-1)n}{2}.$$

    Per tant,

    $$a_{7000} = 6999 \cdot 3500 \equiv 0 \pmod 7,$$

    i això vol dir que la nota tocada torna a ser un Do.

    A més, noteu que

    $$\begin{aligned} a_{n+7} &= a_{n+6} + (n+6) \\ &= a_{n+5} + (n+5) + (n+6) \\ &= \cdots \\ &= a_n + n + (n+1) + \cdots + (n+6) \\ &= a_n + 7n + 1 + 2 + \cdots + 6 \\ &= a_n + 7n + 3 \cdot 7 \\ &\equiv a_n \pmod 7 \end{aligned}$$

Això vol dir que els residus mòdul 7 de la successió $\{a_n\}$ es van repetint de 7 en 7. Com que els 7 primers són

$$0, 1, 3, 6, 3, 1, 0$$

això vol dir que en cada grup de 7 es toca dues vegades la nota Do. Per tant, si toquem 7000 tecles, haurem tocat 2000 vegades la nota Do.

A més, deduïm també que hi ha residus que no apareixeran mai: 2, 4 i 5. Això vol dir que les notes Mi, Sol i La no es tocaran mai.

22. Demostreu que el 4 d'abril (4 /4), el 6 de juny (6/6), el 8 d'agost (8/8), el 10 d'octubre (10/10), el 12 de desembre (12/12) i el 28 o 29 de febrer de cada any cauen tots en el mateix dia de la setmana.

23. Demostreu que l'equació diofàntica no lineal

$$\frac{1}{x} + \frac{1}{y} = 1,$$

amb $x, y \in \mathbb{Z}$, només té una solució.

(Ajuda: Reescrivim l'equació com a $x + y = xy$. Si $x, y \in \mathbb{Z}$, aleshores $x \mid y$ i $y \mid x$. Per tant $x = y$.)