Matemàtica Discreta

GRAU EN ENGINYERIA INFORMÀTICA

UNIVERSITAT DE BARCELONA

Matemàtica Discreta (364293)

Assignatura del Grau en Enginyeria Informàtica

Departament d'Àlgebra i Geometria

Coordinat per Laura Costa Farras

Impartit per Ricardo García López

Dossier redactat per Marcel Cases Freixenet

Quadrimestre de primavera,

Gener – Maig del 2014

Universitat de Barcelona

Índex

1. Aritmètica modular

1.1. Algorisme de la divisió entera

Definició BASE DE NUMERACIÓ → Sistema o forma de representar números i identificar-los. Per exemple, el sistema de numeració decimal (per definició, posicional), o la numeració romana (no posicional).

Definició SISTEMA DE PALS → I II III IIII 𝍸 𝍸I ... Consisteix en agrupar els pals de cinc en cinc, tatxant els quatre anteriors amb el pal que fa cinc. Serveix per facilitar-ne el recompte, en múltiples de cinc.

Definició DÍGIT → En llatí significa *dit*. És un símbol que, o bé sol o be en combinatòria amb altres símbols, ens serveix per representar números. Per exemple, són dígits: 0, 1, 2, 3B5, 𝍸, ...

Definició SISTEMA DECIMAL → És un número natural $n \in \mathbb{N}$, on n pot ser {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}. És una successió finita de dígits pel què fa a la seva representació. A partir de la seva expressió,

$$n = a_k \cdot 10^k + ... + a_0 \cdot 10^0$$

Proposició → Sigui *b* un número natural $b \in \mathbb{N}$, que anomenarem base. Donada una $n \in \mathbb{N}$ existeix una única forma de representar el número, que és la següent:

$$n = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + ... + a_0 \cdot 10^0$$
$$\text{on } a \in \{0, 1, 2, 3, 4, ..., b-2, b-1\}$$

Aleshores direm que $a_k a_{k-1} a_{k-2} ... a_0$ és la representació d'*n* en base *b*.

Exemple → Passar el número 7 en base 10 a base 2.
Cal identificar, primer, què és *n* i què és *b*. *n* = 7 i *b* = 2. $7=2\cdot3+1=2^2+2+1=1\cdot2^2+1\cdot2+1\cdot1$ → 111 en base 2.

Definició → Si *b* = 2 direm que treballem en el sistema *binari*, si *b* = 8 estem treballant en el sistema *octal* i si *b* = 16 treballem en el sistema *hexadecimal*.

Sistema hexadecimal = {1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F}

Les conversions son molt fàcils entre qualsevol de les bases binària, octal i hexadecimal.

Taula de conversió →

DECIMAL	BINARI	OCTAL	HEXADECIMAL
0	0000	0	0
1	0001	1	1
2	0010	2	2
3	0011	3	3
4	0100	4	4
5	0101	5	5
6	0110	6	6
7	0111	7	7
8	1000	10	8
9	1001	11	9

DECIMAL	BINARI	OCTAL	HEXADECIMAL
10	1010	12	A
11	1011	13	B
12	1100	14	C
13	1101	15	D
14	1110	16	E
15	1111	17	F

Exemple → 2154_8 a base 2. Mirant la taula de conversió i fent les equivalències,

OCTAL	2	1	5	2
HEXADECIMAL	010	001	101	100

Per tant, $2154_8 = 10001101100_2$

1.2. MCD i MCM. Identitat de Bézout

Definició → Siguin $m, u \in \mathbb{N}$,

i. Direm que *u* divideix a *m* i ho denotarem u|m si existeix una $k \in \mathbb{N}$ tal que m = k*u. En aquest cas, denotarem i direm també que *m* és múltiple d'*u* i ho anotarem m = ů.

m = ů significa que *m* és múltiple d'*u*,

u|m significa que *u* divideix a *m*.

ii. Siguin *a*, $u \in \mathbb{N}$, al major número natural *n* que compleixi que n|a i n|u l'anomenarem *màxim comú divisor* d'*a* i *u*. S'expressa MCD(a, u) = n, i en anglès, GCD(a, u) = n (*greatest common divisor*).

iii. Siguin les variables anteriors, al menor número natural *n* que compleixi que n = å i n = ů, l'anomenarem *mínim comú múltiple*. S'expressa MCM(a, u) = n, i en anglès, LCM(a, u) = n (*least common múltiple*).

Algorisme d'EUCLIDES → Ens serveix per trobar el MCD entre dos números. En pseudocodi informàtic, l'algorisme és el següent:

```
function gcd(a, b):
    while a > 0:
        a, b = b % a, a
    return b
```

Sigui $n \in \mathbb{N}$ tal que n|a i n|b, llavors n|a·b. L'algorisme diu que tenint *a*, $b \in \mathbb{N}$, MCD(a, b) = MCD(b, a) = MCD(b % a, a) = MCD(residu *r*, a) = ...

Lema → Si d|p i d|q, aleshores d|p-q.

En general, donades una *a*, $b \in \mathbb{N}$, definim q_i , $r_i \in \mathbb{N}$ recursivament mitjançant les següents equacions:

$$a = b \cdot q_1 + r_1 \quad (0 \le r_1 < b)$$

$$b = r_1 \cdot q_2 + r_2 \quad (0 \le r_2 < r_1)$$

$$r_1 = r_2 \cdot q_2 + r_3 \quad (0 \leq r_3 < r_2)$$

.....

Sabem del cert que aquesta recursiu acabarà en el 100% dels casos, ja que per força en algun moment el residu serà zero.

Teorema IDENTITAT DE BÉZOUT → Siguin $a, b \in \mathbb{N}$ i d = MCD(a, b). Existeixen una $m, n \in \mathbb{Z}$ tals que $d = m \cdot a + n \cdot b$.

Exemple → MCD(7, 20) = 1 = 7 · 3 + 20 · (-1).

Definició NÚMEROS COPRIMERS → Direm que dos números *a, b* són coprimers entre ells si es compleix que MCD(a, b) = 1.

Definició NÚMERO PRIMER → Direm que $p \in \mathbb{N}$ és un número primer si els únics divisors enters que té són l'ú i ell mateix.

Proposició → Sigui $p \in \mathbb{N}$ un número primer i $a_i \in \mathbb{N}$, si $p \nmid$ (no divideix) $a_1...a_i$, p és primer.

Teorema → Sigui $n \in \mathbb{N}$, amb $n \geq 2$, existeixen números primers diferents $p_1...p_k$ tals que $n = p_1^{a1}...p_k^{ak}$.

Demostració →

i. Per inducció, si n = 2, acabem. Només cal agafar k = 1, $p_1 = 2$ i $a_1 = 1$.
ii. Suposem el cas en el que n > 2. Si *n* és primer, es demostrarà el teorema, on k = 1, $p_1 = n$, $a_1 = 1$. Si *n* no és primer, es pot descompondre com a producte de dos nombres, on $2 \leq m < n$ i $2 \leq l < n$. *m* i *l* es descomposen com a producte de números primers.

Si *p*, *q* són números primers i p | q, sempre en resultarà que p = q.

Corol·lari → Tenint $m, n \in \mathbb{N}$, m·n = MCD(m, n) · MCM(m, n).

Corol·lari → Donades una $a, b \in \mathbb{N}$, a + b = màx{a, b} + min{a, b}.

1.3. Congruències

Definició CONGRUÈNCIA (i) → Siguin $x, y \in \mathbb{N}$, i m > 0, direm que x és congruent amb y mòdul m i ho escriurem $x \equiv y \pmod{m}$.

Definició CONGRUÈNCIA (ii) → Si $x \equiv y \pmod{m}$, significa que x (mod m) és igual que y (mod m), és a dir, un residu.
La relació ≡ és d'equivalència, i verifica el següent:

i. Propietat reflexiva → $x \equiv y \pmod{m}$ per qualsevol *x*
ii. Propietat somàtica → $y \equiv x \pmod{m}$
iii. Propietat transitiva → Si $x \equiv y \pmod{m}$ i $y \equiv z \pmod{m}$, $x \equiv z \pmod{m}$

Si $x \equiv y \pmod{m}$, $x - y = k \cdot m$, amb $k \in \mathbb{N}$.
Si $y \equiv z \pmod{m}$, $y - z = l \cdot m$, amb $l \in \mathbb{N}$.

Proposició → El càlcul d'un mòdul negatiu és diferent al del positiu. Per exemple, -5 ≡ 8 (mod 13).

Exemples →

7 ≡ 9 (mod 2) Veritat
7 ≡ 22 (mod 3) Veritat
7 ≡ 23 (mod 3) Fals

Sigui m = 2 i *A* el conjunt d' enters, veiem que la meitat d'*m* són parells i l'altra meitat, senars. Recordant que m = 2, parell amb parell és congruent, senar amb senar és congruent i parell amb senar no és congruent.
Aquesta divisió es pot fer per qualsevol mòdul, per exemple, m = 3. Llavors tenim més grups.

Tenint $n \in \mathbb{Z}$,

n = 2,

Parells	Imparells

n = 3,

Múltiples de 3	Múltiples de 3 + 1	Múltiples de 3 + 2

n = 4,

Múltiples de 4	Múltiples de 4 + 1	Múltiples de 4 + 2	Múltiples de 4 + 3

Qualsevol n,

Múltiples d'*n*	Múltiples d'*n* + 1	Múltiples d'*n* + 2	...	Múltiples d'*n* + *n* - 1

Definició CLASSE → El conjunt de residus (mod m), que denotarem $\mathbb{Z}_m$, és el conjunt de classes d'equivalència en la relació ≡ (congruència).
Si $x \in \mathbb{Z}$, denotarem $[x]_m$ la classe d'equivalència (mod m).

Exemple → A $\mathbb{Z}_2$, és a dir, quan m = 2, hi ha dues classes: parells i imparells. $\mathbb{Z}_2, \in$ {parells, imparells}. Agafat un número, per exemple, 4, classe del [4], tenim que [4] = [0] = [2] = [8] = ...

Exemple → A $\mathbb{Z}_3$, és a dir, quan m = 3, hi ha tres classes: la del zero, la de l'u i la del dos. $\mathbb{Z}_3 \in$ {[0], [1], [2]}. Agafat un número, per exemple, 2, classe del [2], tenim que [2] = [17] = ...

En qualsevol exemple, veiem que es compleix la propietat m | a – b.
Aquestes classes també es poden representar en forma de taula. En el cas de $\mathbb{Z}_2$, tenim les següents taules:

Suma

+	parell	imparell
parell	parell	imparell
imparell	imparell	parell

Producte

·	parell	imparell
parell	parell	parell
imparell	parell	imparell

En el cas de $\mathbb{Z}_3$, tenim la següent taula:

Suma

+	Múltiples de 3	Múltiples de 3, + 1	Múltiples de 3, + 2
Múltiples de 3	Múltiples de 3	Múltiples de 3, + 1	Múltiples de 3, + 2
Múltiples de 3, + 1	Múltiples de 3, + 1	Múltiples de 3, + 2	Múltiples de 3
Múltiples de 3, + 2	Múltiples de 3, + 2	Múltiples de 3	Múltiples de 3, + 1

I això passa amb qualsevol classe, i tant amb la suma com amb el producte.
Per saber a quina classe pertany un número a $\mathbb{Z}_m$, només cal fer n (mod m) i obtindrem la [classe] que busquem.

Proposició → A $\mathbb{Z}_m$ es poden definir la suma i el producte amb les següents propietats:

$$[x] + [y] = [x + y]$$
$$[x] \cdot [y] = [x \cdot y]$$

Proposicions →

i. SUMA:
Si $[x] = [x']$ i $[y] = [y']$, $[x + y] = [x' + y']$
Si $[x] = [x'] \rightarrow x - x' = k \cdot m$, i si $[y] = [y'] \rightarrow y - y' = l \cdot m$. Aleshores, $(x + y) - (x' + y') = (x - x') + (y - y') = (k - l) \cdot m$

ii. PRODUCTE:
Si $[x \cdot y] = [x' \cdot y']$, $x \cdot y - x' \cdot y' = x \cdot y - x' \cdot y - x' \cdot y' = (x - x') \cdot y + (y - y') \cdot y' = k \cdot m \cdot y + x' \cdot l \cdot m = (k \cdot y + x' \cdot l) \cdot m = [x \cdot y] = [x' \cdot y']$

Amb aquestes demostracions, verifiquem que

i. *Propietat commutativa* → $[x] + [y] = [y] + [x]$, $[x] \cdot [y] = [y] \cdot [x]$
ii. *Propietat associativa* → $([x] + [y]) + [z] = [x] + ([y] + [x]) + [z]$, $[x] \cdot ([y] \cdot [z]) = ([x] \cdot [y]) \cdot [z]$
iii. *Element neutre* → $[x] + [0] = [x]$, $[x] \cdot [1] = [x]$

iv. *Propietat distributiva* → $[x] \cdot ([y] + [z]) = [x] \cdot [y] + [x] \cdot [z]$

v. *Imatge de classe* → $[x] + [-x] = 0$

Només hi ha una propietat dels números reals que no es compleix en l'aritmètica modular.

vi. Si $x \cdot y = x \cdot z$, $y = z$, si x és diferent de 0. Això no es pot aplicar a les classes.

Teorema XINÈS DEL RESIDU → Sigui $n_1, n_2, \ldots \in \mathbb{Z}$, existeix una $x \in \mathbb{Z}$ tal que $[x]_{n1} = [a_1]_{n1}$.

Podem reescriure el teorema anterior com

$$\left\{ \begin{array}{c} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{array} \right\}$$

Sigui $n_1, n_2, \ldots n_k \in \mathbb{N}$, observem que $MCD(n_i, n_j) = 1$, amb $i \neq j$.
Sigui $a_1, a_2, \ldots \in \mathbb{Z}$, existeix una $x \in \mathbb{Z}$ tal que

$$\left\{ \begin{array}{c} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \ldots \\ x \equiv a_k \pmod{n_k} \end{array} \right\}$$

Demostració → en el cas que $k = 2$, tenim que, per la Identitat de Bézout,

$$\left\{ \begin{array}{c} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{array} \right\}$$

A més, $MCD(n_1, n_2) = 1$. Existeixen una $\alpha, \beta \in \mathbb{Z}$ que demostren que $1 = \alpha \cdot n_1 + \beta \cdot n_2$. Expressat d'una altra manera, $x = a_1 \cdot \beta \cdot n_2 + a_2 \cdot \alpha \cdot n_1$. També $x - a_1$ és múltiple d'n_1.

Exemple → Resoldre el següent sistema d'equacions:

$$\left\{ \begin{array}{c} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{array} \right\}$$

Extraient els valors, tenim que $a_1 = 3$, $a_2 = 2$, $n_1 = 5$, $n_2 = 7$. A més, $\alpha, \beta \in \mathbb{Z}$ i de moment no les sabem. Llavors, $1 = 5\alpha + 7\beta$, i per qualsevol real enter d'alfa i beta en traiem valors qualsevols que compleixin la igualtat. Per exemple, $\alpha = 3$ i $\beta = -2$. Substituint a l'expressió $x = a_1 \cdot \beta \cdot n_2 + a_2 \cdot \alpha \cdot n_1$, obtenim que $x = 3 \cdot (-2) \cdot 7 + 2 \cdot 3 \cdot 5$. La solució és $x = -12$. Fem la corresponent comprovació:

$$\left\{ \begin{array}{c} -12 \equiv 3 \pmod{5} \\ -12 \equiv 2 \pmod{7} \end{array} \right\}$$

I veiem que el resultat és compatible i coherent. Problema resolt.

En general, tenim l'anterior sistema d'equacions

$$\left\{\begin{array}{c} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \dots \\ x \equiv a_k \pmod{n_k} \end{array}\right\}$$

I en concluïm que $MCD(n_i, n_j) = 1$.
Siguin les $\alpha_i \in \mathbb{Z}$ tals que $[\alpha_i]_{ni} = [N/n_i]_{ni}^{-1}$, aleshores $x = \Sigma\, a_i \cdot (N/n_i) \cdot \alpha_i$. Llavors, $N/n_1 = n_2 \cdot n_3 \cdot n_{\dots} \cdot n_k$. Veiem que podem fer una modificació a la Identitat de Bézout.

Corol·lari → Identitat de Bézout modificada $1 = \alpha_i \cdot (n_2 \cdot n_3 \cdot n_{\dots} \cdot n_k) + \beta_1 \cdot n_1$.

Exemple → Resoldre el sistema d'equacions següent:

$$\left\{\begin{array}{c} x \equiv 1 \pmod{2} \\ x \equiv 0 \pmod{3} \\ x \equiv 4 \pmod{5} \end{array}\right\}$$

Extraient les dades de la fórmula, tenim que $a_1 = 1$, $a_2 = 0$, $a_3 = 4$, $n_1 = 2$, $n_2 = 3$, $n_3 = 5$, $N = n_1 \cdot n_2 \cdot n_3 = 2 \cdot 3 \cdot 5 = 30$.
Calculem α_1, que és l'equivalent a $MCD(n_1, n_2 \cdot n_3) = MCD(2, 15) = 1$. Llavors, per la Identitat de Bézout, per exemple, $1 = 1 \cdot 15 + (-7) \cdot 2$, on $\alpha_1 = 1$ (i $\beta_1 = -7$, tot i que no ens interessa per aquest problema).
Calculem α_2, que és l'equivalent a $MCD(n_2, n_1 \cdot n_3) = MCD(3, 10) = 1$. Llavors, per la Identitat de Bézout, per exemple, $1 = 1 \cdot 10 + (-3) \cdot 3$, on $\alpha_2 = 1$.
Calculem α_3, que és l'equivalent a $MCD(n_3, n_1 \cdot n_2) = MCD(5, 6) = 1$. Llavors, per la Identitat de Bézout, per exemple, $1 = 1 \cdot 6 + (-1) \cdot 5$, on $\alpha_3 = 1$.
Obtenim que $\alpha_1 = \alpha_2 = \alpha_3 = 1$.
La solució al sistema d'equacions de congruències és la següent:

$$x = \Sigma\, a_i \cdot (N/n_i) \cdot \alpha_i$$
$$x = a_1 \cdot (N/n_1) \cdot \alpha_1 + a_2 \cdot (N/n_2) \cdot \alpha_2 + a_3 \cdot (N/n_3) \cdot \alpha_3$$
$$x = 1 \cdot (30 / 2) \cdot 1 + 0 \cdot (30 / 3) \cdot 1 + 4 \cdot (30 / 5) \cdot 1$$

La solució al sistema és $x = 39$.

Definició SIMPLIFICACIÓ → A $\mathbb{Z}_m$ tenim dues operacions: suma i producte. Una diferència important entre $\mathbb{Z}_m$ i $\mathbb{Z}_m$ (mod *m*) és la possibilitat de simplificar. A $\mathbb{Z}$, si $x \cdot y = x \cdot z$ i $x \neq 0$, llavors $y = z$. A $\mathbb{Z}_m$ (mod m), això no es compleix.

Exemple → Si $m = 4$, a $\mathbb{Z}_4$ tenim que $[2] \cdot [2] = 0 = [2] \cdot [0]$, però si ens hi fixem, la classe del 2 és diferent que la classe del zero (mod 4).
No obstant, la simplificació de classes sí que funciona en algunes classes concretes, com podrien ser A $\mathbb{Z}_3$ i A $\mathbb{Z}_5$, entre altres.

Definició CLASSE INVERTIBLE → Es diu que $\alpha \in \mathbb{Z}_m$ és invertible si existeix una $\beta \in \mathbb{Z}_m$ tal que $\alpha \cdot \beta \pmod m = [1]$. En aquest cas, direm que β és l'invers d'α i ho expressarem $\beta = \alpha^{-1}$.

Exemples → Determinar si les següents classes són invertibles.

i. $\mathbb{Z}_2 = \{[0], [1]\}$. Existeix una n tal que $[0] \cdot [n] = [1]$? No, per tant, la classe del zero (mod 2) no és invertible.

ii. $\mathbb{Z}_2 = \{[0], [1]\}$. Existeix una n tal que $[1] \cdot [n] = [1]$? Sí, per tant, la classe de l'u (mod 2) és invertible.

En general, [0] mai és invertible i [1] sempre ho és.

iii. $\mathbb{Z}_3 = \{[0], [1], [2]\}$. Sabent que [0] no és invertible i [1] sí, hem d'esbrinar si [2] ho és. $[2] \cdot [n] = [3 + 1]$. Si n = 2, resolem la igualtat i veiem que [2] és invertible.

iv. $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$. Sabent que [0] no és invertible i [1] sí, hem d'esbrinar si [2] ho és. $[3] \cdot [3] = [1]$. Per tant, 2 no és invertible, però la del tres ja sí.

Proposició → Sigui $r \in \mathbb{Z}$, llavors [r] és invertible a $\mathbb{Z}_m$ si i només si MCD(r, m) = 1 i, per tant, *r* i *m* són coprimers.

Corol·lari → Sigui $r \in \mathbb{Z}$ i $p \in \mathbb{N}$, i *p* sigui un número primer, llavors [r] és invertible a $\in \mathbb{Z}_p$ si i només si *p* no divideix a *r* ($p \nmid r$). Per exemple, $\mathbb{Z}_4^* = \{[1], [3]\}$.

Notació → Denotarem $\mathbb{Z}_m^*$ el conjunt d'elements invertibles de $\mathbb{Z}_m$.

Demostració deductiva → Si la classe d'*r* ([r]) és invertible, existeix un número enter tal que $[r] \cdot [s] = [1]$, a $\mathbb{Z}_m$. Això significa que $[r \cdot s - 1] = [0]$ a $\mathbb{Z}_m$. Aleshores, $r \cdot s - 1 = \lambda \cdot m$. Altrament expressat, $r \cdot s - \lambda \cdot m = 1$. Si $q \in \mathbb{Z}$, $q \mid m$ i $q \mid r$, $q \mid r_s - \lambda \cdot m = 1$.

Demostració inductiva → Suposem que MCD(r, m) = 1. Aplicant el teorema de Bézout, existeixen una *a*, $b \in \mathbb{Z}$ tals que $a \cdot r + b \cdot m = 1$. Agafant classes (mod m), tenim que $[a] \cdot [r] + [b] \cdot [m] = [1]$. Com a conclusió, [r] és invertible a $\mathbb{Z}_m$.

1.4. Xifratge afí

Definició CRIPTOGRAFIA → És l'estudi i la pràctica de tècniques per establir una comunicació segura i secreta a la presència de tercers (anomenats *adversaris*).

Definició XIFRATGE CÈSAR → És la forma més senzilla de xifratge, i consisteix en fer una translació dels caràcters en un número determinat d'unitats. Per exemple, podem numerar cada lletra de l'abecedari amb un número, i establim una clau d'encriptació. A cada número de caràcter, li sumem aquesta clau i obtenim un nou caràcter. Per desxifrar-ho, enlloc de sumar, restem la clau d'encriptació.

En forma de funció, per encriptar tenim la següent expressió:

$$E_n(x) = x + n$$

I per desencriptar,

$$D_n(x) = x - n$$

On *E* significa *encriptar*, *D* significa *desencriptar*, *n* és la clau d'encriptació i *x* és el missatge a processar.

Exemple → Xifrar el missatge "HOLA" amb una clau d'encriptació *n* = 15.
El primer pas és traduir el missatge a una seqüència numèrica. Farem servir l'abecedari anglès, assignant a cada caràcter un número del 0 al 26. "HOLA" equival a 7 14 11 0.
Apliquem la regla d'encriptació,

$$E_{15}(x) = (22\ 29\ 26\ 15) \pmod{26}$$
$$E_{15}(x) = 22\ 3\ 0\ 15$$

Ja tenim el missatge xifrat. Per desencriptar-lo,

$$D_{15}(x) = (7\ {-12}\ {-15}\ 0) \pmod{26}$$
$$D_{15}(x) = 7\ 14\ 11\ 0 = \text{"HOLA"}$$

Definició XIFRATGE AFÍ → Sigui $a \in \mathbb{Z}_{26}$ invertible, és a dir, que existeix una $b \in \mathbb{Z}$ tal que $[a]_{26} \cdot [b]_{26} = 1$, $a \cdot b - 1$ és múltiple de 26. El xifratge afí és el què s'obté utilitzant la clau de xifratge que ve donada per la fórmula

$$E_{a,n}(x) = a \cdot x + n \pmod{26}$$

I la desencriptació ve donada per

$$D_{a,n}(x) = a^{-1} \cdot (x - n) = a^{-1} \cdot x - a^{-1} \cdot n \pmod{26}$$

On la $b \in \mathbb{Z}$ verifica que $a \cdot b - 1$ és múltiple de 26.
Observació: si $y = a \cdot x + n$ s'hi aplica $D_{a,n}(y) = a^{-1} \cdot (a \cdot x + n - n) = x$.

1.5. Funció d'Euler i xifratge RSA

Definició FUNCIÓ PHI D'EULER → És una aplicació lineal $\phi: \mathbb{N} \longrightarrow \mathbb{N}$ definida per $\phi(m)$ = número d'enters positius $r \in \mathbb{N}$ tals que són iguals a la quantitat de números de $\mathbb{Z}_m^*$. MCD(r, m) = 1, amb $r \leq m$.

Exemples →

$\phi(2) = 1$, ja que $\mathbb{Z}_2 = \{[0], [1]\}$
$\phi(3) = 2$, ja que $\mathbb{Z}_3 = \{[0], [1], [2]\}$
$\phi(4) = 2$, ja que $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$
$\phi(5) = 4$, ja que $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$
...

Per calcular la ϕ en el xifratge d'Euler, tenim una *p* que pertany als números primers, i $\phi(p) = p - 1$ elements invertibles.

$$\mathbb{Z}_p = \{[0], \underbrace{[1], [2], ..., [p-2], [p-1]}_{\mathbb{Z}_p^*}\}$$

Donat el cas que *q* sigui una potència d'un número primer, per exemple, $q = 2^2 = 4$,

i. Si *p* és primer, i $k \geq 1$, llavors $\phi(p^k) = (p-1) \cdot p^{k-1}$.
ii. Si $m_1, m_2 \in \mathbb{N}$, és a dir, $MCD(m_1, m_2) = 1$, $\phi(m_1 \cdot m_2) = \phi(m_1) \cdot \phi(m_2)$

Demostració → Primera proposició: si *p* és primer, i $k \geq 1$, llavors $\phi(p^k) = (p-1) \cdot p^{k-1}$.

La seva demostració es basa en el teorema xinès del residu. Suposem que tenim una $m \in \mathbb{N}$. Llavors, $MCD(m, p^k)$ serà igual a algun valor dels $\{1, p, p^2, p^3, ..., p^{k-1}, p^k\}$.

Volem calcular $\phi(p^k)$, és a dir, el número d'enters $m < p^k$ tals que $MCD(m, p^k) = 1$. És el mateix que el número d'enters $m < p^k$ tals que $p \nmid m$. Els valors que divideixen a *m* són els múltiples de *p* menors que p^k, que són $\{1, p, 2p, 3p, ..., p^{k-1}\}$. Els menors de p^k que són primers amb p^k són $p^k - p^{k-1} = p^{k-1} \cdot (p-1)$ (factor comú).

Si $n \in \mathbb{N}$, sabem que $n = p_1^{a1} \cdot ... \cdot p_k^{ak}$, amb p_i diferents. Llavors, $a_i \in \mathbb{N}$, $a_i > 0$, $\phi(n) = \phi(p_1^{a1}) \cdot ... \cdot \phi(p_k^{ak}) = p_1^{a1-1} \cdot (p_1 - 1) ... p_k^{ak-1}$. $MCD(p_1^{a1}, p_2^{a2}) = 1$.

Teorema d'Euler → Si *y* és invertible a $\mathbb{Z}_m$, llavors $y^{\phi(m)} \equiv 1 \pmod p$.

Corol·lari TEOREMA PETIT DE FERMAT → Si $p \nmid y$, llavors $y^{p-1} \equiv 1 \pmod p$.

Demostració → Sigui *n* el número del producte de tots els elements de $\mathbb{Z}_m^*$, és a dir, $n = x_1 \cdot x_2 \cdot ... \cdot x_k$, on $\mathbb{Z}_m^* = \{ x_1 \cdot x_2 \cdot ... \cdot x_k \}$, $k = \phi \pmod m$. Tindrem que $y \cdot \mathbb{Z}_m^* = \{ y \cdot x_1, y \cdot x_2, ..., y \cdot x_k\} = \{ x_1, x_2, ..., x_k\} = \mathbb{Z}_m^*$. Si $x \{ y \cdot x_1, y \cdot x_2, ..., y \cdot x_k\}$, $y = y \cdot x_i$, $y \cdot x_i \cdot y^{-1} \cdot x_i^{-1} = 1$. Si $x \in \{ x_1, x_2, ..., x_k\}$, llavors $x = y \cdot y^{-1} \cdot x$, i per tant, $x \in y \cdot \mathbb{Z}_m^*$.

$n = x_1 \cdot x_2 \cdot ... \cdot x_k = (y \cdot x_1) \cdot (y \cdot x_2) \cdot ... \cdot (y \cdot x_k) = y^k \cdot x_1 \cdot x_2 \cdot ... \cdot x_k = y^k \cdot n \rightarrow n = y^k \cdot n \rightarrow y^k = 1 \pmod m$.

Exemples → Posem el cas que m = 3. El teorema petit de Fermat diu que si $y \in \mathbb{Z}_3^*$, $y^{\phi(3)} \equiv 1 \pmod 3$. Agafem que y = 4, ja que [4] = [1]. Aplicant el teorema d'Euler, $4^{\phi(3)} \equiv 1 \pmod 3$. $\phi(3) = 2$, $4^2 = 16 = 1 \pmod 3$. Es compleix el teorema.

Resum → [y] és invertible a $\mathbb{Z}_m$ si i només si $y^{\phi(m)} \equiv 1 \pmod m$.

Exemple → Agafem m = 5, per tant, $\phi(5) = 4$. [2] és invertible a $\mathbb{Z}_5$ i el teorema d'Euler ens diu que $2^4 \equiv 1 \pmod 5$. [3] és invertible a $\mathbb{Z}_5$ ja que $3^4 \equiv 1 \pmod 5$.

Definició CRIPTOGRAFIA RSA → Altrament anomenat *xifratge de clau pública*, és un sistema d'encriptació que es basa en què la clau d'encriptació i la de desencriptació són diferents. El primer sistema d'encriptació que feia servir aquest mètode és l'RSA (Rivest, Shamir, Adleman). Hi ha dues persones que volen transmetre's informació encriptada: el Bob (qui envia el missatge) i l'Alice (qui el rep). Per efectuar el xifratge RSA cal aplicar els següents passos:

i. L'Alice escull dos números primers *p* i *q* qualsevols, i una $n \in \mathbb{N}$ tal que la $n = p \cdot q$. Amb això, $\phi(n) = \phi(p) \cdot \phi(q) = (p - 1) \cdot (q - 1)$.
ii. L'Alice selecciona un enter $e \in \mathbb{N}$ tal que $1 < e < \phi(n)$, i a més que MCD(e, n) = 1. Llavors, calcula $d \in \mathbb{N}$ tal que $[d]^{-1} = [e]$, a $\mathbb{Z}_{\phi(n)}$.
iii. L'Alice envia a el Bob dos números: *n* i *e*. S'anomena a *e exponent de clau pública*. El valor de *d*, que s'anomena *exponent de clau privada*, se'l guardarà l'Alice.
iv. El Bob vol enviar un missatge qualsevol, que transforma a un número enter *m* comprès entre 0 i n. És a dir, $0 \leq m < n$. Calcula *c*, que és igual a $c = m^e \pmod n$ i l'envia a l'Alice. Ara ja no hi hauran més intercanvis d'informació.
v. L'Alice calcula l'enter *m* fent c^d, és a dir, $m \equiv c^d \pmod n$.

Exemple → Suposem que Bob vol enviar el missatge m = 1211.

i. L'Alice tria els números primers p = 541, q = 1223. Calcula el producte $n = p \cdot q = 661643$. Calcula $\phi(n) = 540 \cdot 1222 = 659880$.
ii. Agafem e = 131. Calculem $d = 131^{-1} \pmod{\phi(n)}$. Obtenim que d = 639731.
iii. L'Alice li envia al Bob n = 661643 i e = 131.
iv. El Bob calcula $c = m^e \pmod n = 1211^{131} \pmod{661643} = 109073$. El Bob li envia a l'Alice aquesta *c*.
v. L'Alice calcula $109073^d = 1211 \pmod n$, i obté el missatge m = 1211.

Per què és segur l'RSA? Si a partir d'*n* som capaços de calcular $\phi(n)$, llavors som capaços de calcular *d*, que és igual a l'exponent de clau privada.

$$\left\{ \begin{array}{c} n = x \cdot y \\ \phi(n) = (x - 1) \cdot (y - 1) \end{array} \right\}$$

De la primera equació en traiem que y = n/x. A la segona equació, $\phi(n) = (x - 1) \cdot (n/2 - 1)$ i, reordenant, $x^2 + (\phi(n) - n - 1) \cdot x + n = 0$. Veiem que si sapiguéssim calcular $\phi(n)$ a partir d'*n*, podríem calcular la factorització molt fàcilment. Per desxifrar missatges hauríem de conèixer la factorització de números primers $n = p \cdot q$. Si no es fa per força bruta, és gairebé impossible resoldre-ho. És aquesta l'explicació per el qual com més grans siguin els primers *p* i *q* més difícil serà de trobar-los per força bruta.

Per exemple, si $n = p \cdot q$ té més o menys 400 dígits, el temps que tardaria un ordinador a trobar la factorització és més gran que la vida del Sol.

Agafem $n = p \cdot q$ (*p* i *q* són números primers). Aleshores, $\phi(n) = (p - 1) \cdot (q - 1)$.

Agafem $e \in \mathbb{N}$, $1 < e < \phi(n)$ tal que MCD(e, n) = 1.

Agafem $d \in \mathbb{N}$, $1 < e < \phi(n)$ tal que $d^{-1} \equiv e \pmod{\phi(n)}$.

Si el missatge $m \in \mathbb{N}$, $0 < m < n$, agafem una $c = m^e$. El receptor del missatge calcula c^d. Obtenim que $c^d \equiv m \pmod n$.

El sistema RSA funciona, ja que es pot verificar que la proposició de la línia anterior és certa.

Proposició → $e \cdot d = 1 \pmod{\phi(n)}$. Per tan, existeix una $\lambda \in \mathbb{Z}$ tal que $e \cdot d = 1 + \lambda \cdot \phi(n)$. Es poden donar dos casos:

i. MCD(m, n) = 1. Llavors, $c^d = (m^e)^d = m^{e \cdot d} = m^{1 + \lambda \cdot \phi(n)}. = n \cdot (m^{\phi(n)})^{\lambda}$. Per tan, $m \cdot 1^{\lambda} \equiv m \pmod{n}$.
ii. MCD(m, n) ≠ 1. Com que $n = p \cdot q$ i $m < n$, o bé MCD(m, n) = p o bé MCD(m, n) = q. Si es dóna aquest segon cas, n'hi ha prou en resoldre o bé *p* o bé *q* i ja podem saber l'altra, ja que $n = p \cdot q$.

Volem comprovar que $c^d \equiv m \pmod{n}$. Com que $n = p \cdot q$, n'hi ha prou en comprovar

i. $c^d \equiv m \pmod{p}$
ii. $c^d \equiv m \pmod{q}$

Llavors, es pot escriure $m^{e \cdot d} \equiv m \pmod{p}$.

Recordatori → Si $a \equiv b \pmod{m}$, $m \mid a - b$.

$c^d = m^{e \cdot d} \equiv m \cdot (m^{q-1})^{\lambda \cdot (p-1)} \equiv m \cdot 1^{\lambda \cdot (p-1)} = m \pmod{q}$.

2. Combinatòria

2.1. Principis bàsics de combinatòria

Siguin *x*, *r* conjunts de l'aplicació lineal f: X ⟶ r ,

i. Es diu que *f* és *injectiva* si existeixen una *x*, *y* ∈ X tals que f(x) = f(y). Per tant, x = y.
ii. Es diu que *f* és *exhaustiva* si existeixen una x ∈ X i y ∈ V tal que f(x) = y.
iii. Es diu que *f* és *bijectiva* si és simultàniament injectiva i exhaustiva.

2.2. Permutacions

Definició PERMUTACIÓ → Sigui X un conjunt de finits, es diu que una permutació de X és una aplicació lineal bijectiva f: X ⟶ X. Habitualment, X = {1, 2, 3, ..., n}, on *n* és el número (#) de cada element.

Anotació → Denotarem G_n el conjunt de permutacions de {1, 2, 3, ..., n}.

Exemple → Donada n = 3, trobar totes les permutacions G_3, és a dir, les permutacions que en surten del conjunt {1, 2, 3}.
El fet de ser un número petit d'elements, es pot fer a vista sense aplicar grans operacions. Veiem que les permutacions corresponents són:

{1, 2, 3}
{2, 3, 1}
{3, 1, 2}

Observacions →

i. Una permutació és una reordenació dels elements del conjunt X.
ii. Si el número d'elements és diferent de zero, llavors el conjunt $G_n = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1$, és a dir, n! permutacions.
iii. Si sigma $\sigma \in G_n$, llavors denotarem una matriu

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ a1 & a2 & a3 & \ldots & an \end{pmatrix}$$

Exemple →

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Definició PRODUCTE DE PERMUTACIONS → Siguin σ i τ el següent,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ i } \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} ,$$

anomenarem *composició* o *producte de permutacions* la següent idea:

	σ		τ	
{1, 2, 3}	→	{1, 2, 3}	→	{1, 2, 3}
1	→	2	→	3
2	→	1	→	2
3	→	3	→	1

de manera que

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Cal remarcar que $\sigma \cdot \tau$ no sempre serà igual que $\tau \cdot \sigma$. Aquest tipus de composicions no té la propietat commutativa.

Definició COMPOSICIÓ DE PERUTACIONS → Siguin $\sigma, \tau \in G_n$, denotarem $\sigma \circ \tau$ la composició {1, 2, 3} → {1, 2, 3}. Denotarem *id*entitat $\in G_n$ la permutació id(i) = i.

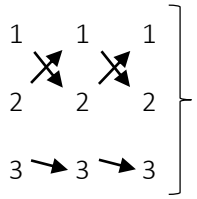
Proposició → Podem verificar les següents proposicions:

i. Propietat *commutativa*. Si $\sigma, \tau, \pi \in G_n$, llavors $(\pi \circ \sigma) \circ \tau = \pi \circ (\sigma \circ \tau)$.
ii. Element *neutre*. $\sigma \circ id = id = id \circ \sigma$.
iii. Element *invers*. Per tot $\sigma \in G_n$ existeix $\sigma^{-1} \in G_n$ tal que $\sigma \circ \sigma^{-1} = id = \sigma^{-1} \circ \sigma$.

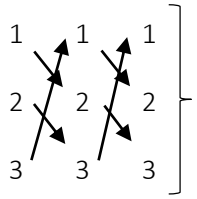
Demostració →

i. Si $k \in \{1, 2, 3, ..., n\}$, $(\pi \circ \sigma) \circ \tau(k) = \pi \circ (\sigma \circ \tau(k)) = \pi \circ (\sigma \circ \tau)(k)$.
ii. Si $\sigma \in G_n$, llavors σ és $\{1, 2, ..., n\} \longrightarrow \{1, 2, ..., n\}$ una aplicació lineal bijectiva. Donada una $k \in \{1, 2, 3, ..., n\}$, existeix un únic h_k tal que $\sigma(h_k) = k$. Definim $\sigma^{-1}(k) = h_k$. Llavors, $\sigma \circ \sigma^{-1}(k) = \sigma \cdot h_k = k$.

Exemples →



Aplicant dues vegades σ tenim σ^2, que és igual que id.



$\tau^2 \neq id$, però $\tau^3 = id$.

Definició CICLE → Es diu que $\sigma \in G_n$ és un cicle d'ordre $r \geq 2$ si existeixen $a_1, a_2, ..., a_r \in \{1, 2, ..., n\}$ diferents que verifiquen

i. $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, ..., $\sigma(a_r) = a_1$.
ii. Si $a \neq a_i$, $\sigma(a) = a$.

Un cicle d'ordre r = 2 se l'anomena *transposició*.

Exemple → Quin ordre té el següent cicle?

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 2 & 5 & 6 \end{pmatrix}$$

Veiem que és un cicle d'ordre r = 4, ja que observem les següents seqüències:
1 → 4 → 2 → 3 → 1, la més llarga, que engloba 4 valors fins tornar a 1.
5 → 5
6 → 6

Exemple →

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

No és un cicle.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

És una transposició (ordre r = 2).

Notació → Sigui $\sigma \in G_n$ un cicle d'ordre r, és a dir, $a_1 \to a_2 \to \ldots \to a_r \to a_1$, denotarem $\sigma = (a_1, a_2, \ldots, a_r)$.

Exemple →

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 2 & 5 & 6 \end{pmatrix} \quad \sigma = (1, 4, 2, 3)$$

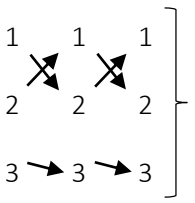
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad \sigma = (1, 3)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \sigma = (1, 2) \cdot (3, 4)$$

Proposició → Tota permutació σ es pot expressar com a producte de transposicions. Aquestes descomposicions no són úniques.

Exemple →

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3) = (1, 2) \cdot (2, 3)$$



$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1, 3, 4, 2) = (1, 3) \cdot (3, 4) \cdot (4, 2)$$

Proposició → Si $(a_1, ..., a_r)$ és un cicle, aleshores $(a_1, ..., a_r) = (a_1, a_2) \cdot (a_2, a_3) \cdot ... \cdot (a_{r-1}, a_r)$. Aquest exercici demostra que tota permutació és un producte de cicles.

Exemple → Exemple de descomposició múltiple. Si n = 3, tenim que (1, 2) = (1, 2) · (1, 3) · (1, 3).

Proposició → Sigui $\sigma \in G_n$, i $\sigma = a_1 ... a_r$ i $\sigma = p_1 ... p_r$, llavors:

i. O bé r i s són parells, i es diu que σ és parell, o bé
ii. r i s són imparells, de manera que σ és imparell.

Definició SIGNATURA DE SIGMA →

$$\text{Sign}(\sigma) = \begin{cases} +1, \text{ si } \sigma \text{ és parell.} \\ -1, \text{ si } \sigma \text{ és imparell.} \end{cases}$$

Exemple → Calcular les següents signatures.

Sign((1, 2)) = -1

Sign((1, 2) · (2, 3)) = +1

Idea → Donat un conjunt X, de quantes maneres es pot seleccionar r elements entre els elements d'X?

Exemple → X = {a, b, c, d}. Quants subconjunts de 2 elements es poden formar?

Suposem que X és un conjunt amb n elements (n ≥ 1). Sigui 1 ≤ r ≤ n, quants subconjunts d'r elements té X?

Denotarem aquest número de la forma

$$\begin{pmatrix} n \\ r \end{pmatrix}$$

"n sobre r", i s'anomena *número binomial*.
{a, b}, {a, c}, {a, d}, {b, c}, {b, d}, {c, d} =

$$\begin{pmatrix} 4 \\ 2 \end{pmatrix}$$

= 6.
Exemple →

$$\begin{pmatrix} n \\ n \end{pmatrix} = 1$$

{a, b, c, d} = de quantes maneres puc seleccionar el conjunt d'n elements en grups d'n elements?

Definició →

$$\binom{n}{r} = \binom{n}{n-r}$$

Exemple → X = {a, b, c, d}, per tant, n = 4.

Si r = 2, $\binom{4}{2}$ = 6, ja que es calcula (4!)/((4-2)!·2!).

Observacions →

i. n sobre 0 = 1.
ii. n sobre 1 = n.
iii. n sobre n = 1.
iv.

$$\binom{n}{r} = \binom{n}{n-r}$$

Imaginem que agafem els subconjunts d'X amb r elements, i d'altra banda, els subconjunts d'X amb n – r elements.

$\binom{n}{r}$ ∈{subconjunts d'X amb r elements} = A.

$\binom{n}{n-r}$ ∈{subconjunts d'X amb n – r elements} = B.

X = {a, b, c, d}

Si n = 1, {a}, {b}, {c}, {d}

Si fem n – r = 4 – 1 = 3, {a, c, d}, {a, b, d}, {b, c, d}

La correspondència és bijectiva, de manera que els dos conjunts A i B tenen el mateix número d'elements, i aplicant el *Teorema de Grassmann*, vist a Àlgebra,

$$\#A = \binom{n}{r} = \binom{n}{n-r} = \#B$$

Teorema → Siguin n, r ∈ ℕ, 1 ≤ r ≤ n – 1, llavors

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$$

Això es pot demostrar amb el triangle de Pascal-Tartaglia.

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 **10** 5 1

Agafant, per exemple, el **10**, veiem que s'obté de la següent manera:

$$\binom{4}{2} + \binom{4}{3} = \binom{5}{3} = 6 + 4 = (5!)/((5 - 3)!*3!) = 10$$

Demostració → Sigui X un conjunt amb *n* elements, i siguin U = {subconjunts Y d'X amb *r* elements, X_0 pertany a Y} i V = {Subconjunts Y d'X amb *r* elements, X_0 no pertany a Y}, si Y ∈ U, Y – {X_0} ∈ X – {X_0}, que és el mateix que dir que #(r – 1) ∈ #(n – 1). El número de subconjunts que són d'U coincideix amb el número de subconjunts de X – {X_0}, amb r – 1 elements.

Si Y ∈ V, el número de subconjunts d'X que estan a U és el número de subconjunts en X – {X_0}, que té n – 1 elements. Aquest número és

$$\binom{n-1}{r}$$

Llavors, el subconjunt d'X amb r elements = U ∪ V. Dit d'una altra manera, no hi ha cap element que estigui alhora als dos conjunts. Hi ha tants elements com n sobre r.

Teorema → Siguin n, r ∈ ℕ, $1 \leq r \leq n - 1$, llavors

$$\binom{n}{r} = (n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n - r + 1))/(r!) = (n!)/(r! \cdot (n-r)!)$$

Demostració → Per inducció sobre *n*,
n = 1, per tant 1 sobre 1 = (1!)/(1! · 0!) ---0! És 1--- = 1/(1 · 1) = 1

Proposició → El número de seleccions no ordenades amb repetició d'*r* elements d'un conjunt d'*n* elements és

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

Exemple → Tenim X el conjunt {'a', 'b', 'c'} lletres. De quantes maneres podem seleccionar quatre lletres?

Obtenim que n = 3 i r = 4. D'aquesta manera,

$$\binom{-1+n+r}{r} = \binom{3+4-1}{4} = \binom{6}{4} = 15 \text{ maneres.}$$

Exemple → Quants resultats possibles podem obtenir al tirar tres daus?

1 1 1
1 1 2
1 1 3
.....
6 6 6

Per força bruta = 56 resultats diferents, ja que es té en compte que els daus són indistingibles entre ells, és a dir, 1 1 2 = 1 2 1 = 2 1 1, 2 3 6 = 2 6 3 = 3 2 6 = 6 2 3 = ..., etcètera.

Analíticament, és 8 sobre 3 que és igual a 56.

A l'exemple de les lletres, un possible resultat és

a		b		b		c
1	0	1		1	0	1

A cada resultat li podem assignar un número binari.

El problema es converteix en intercalar dos zeros en una tira de quatre uns en les possibles següents posicions:

També es pot expressar dient que tenim sis posicions en dues de les quals hi hem d'afegir dos uns i a les restants, zeros.

De quantes maneres es pot fer?

$\binom{6}{2}$ = (6!)/((6-2)! · 2!) = 15

Proposició → Recordem que en número de seleccions no ordenades amb repetició d'*r* objectes en un conjunt d'*n* elements són

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

Com que aquestes seleccions no són ordenades, podem suposar que els elements del mateix tipus estan junts. A cada selecció de li assigna una paraula de longitud n + r – 1 de l'alfabet {0, 1}, segons el mètode anterior de les caixes.

Si hi ha *k* objectes de tipus *i*, primer tindrem k_1 uns, llavors un 0, llavors k_2 uns...

El número de zeros a escriure és n – 1, ja que poden ocupar qualsevol de les n + r – 1 posicions. Finalment, el número de seleccions serà

$$\binom{n+r-1}{n-1} = \binom{n+r-1}{n+r-1-(n-1)} = \binom{-1+n+r}{r}$$

Resum →

	ORDENADES	SENSE ORDENAR
SENSE REPETICIÓ	$n \cdot (n-1) \cdot \ldots \cdot (n-r+1)$	n sobre r
AMB REPETICIÓ	n^r	(n + r – 1) sobre r

Exemple → Volem estudiar seleccions amb repetició prescrita. Quantes paraules puc escriure amb les lletres de la paraula "ABRACADABRA"?

Les paraules de la selecció seran de la forma

$$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}$$

La lletra A surt 5 vegades.

La lletra B surt 2 vegades.

La lletra R surt 2 vegades.

La lletra C surt 1 vegada.

La lletra D surt 1 vegada.

D'aquesta manera podem extreure'n que són 11! Permutacions dividit per 5! permutacions de les A's, 2! permutacions de les B's, 2! permutacions de les R's, i 1! de la C i la D, que no es compten ja que 1! = 1.

Llavors, fent la operació (11!)/(5! · 2! · 2! · 1! · 1!) obtenim un resultat, que són 83160 permutacions.

Definició → Siguin $n_1, \ldots, n_r \in \mathbb{N}$, i $n = n_1 + \ldots + n_r$, definim

$$\binom{n}{n1 \ \ldots \ nr}$$

que és igual que $(n!)/(n_1! \cdot n_2! \cdot \ldots \cdot n_r!)$ i s'anomena *número multinomial*.

Observacions →

$\binom{n}{n1 \ \ldots \ nr}$

i. La figura representa el número de possibles permutacions d'n objectes en r grups de tamany n_1, n_2, ..., n_r. Això es pot representar com si tinguéssim r caixes en les que hi hem de col·locar n objectes (n_1 objectes a la primera caixa, n_2 objectes a la segona...).

ii. Els números binomials apareixen al desenvolupar $(x + y)^n$ de la següent manera:

$$\sum_{i \geq 0}^{n} \binom{n}{i} x^i \cdot y^{n-i}$$

Exemple → Si n = 3, llavors $(x + y)^3 = x^3 + 3 \cdot x^2 \cdot y + 3 \cdot x \cdot y^2 + y^3$.

2.3. Successions en forma recurrent

Idea → Hi ha problemes que tracten de calcular una successió $U_0, U_1, U_2, ..., U_n$ i sabem que U_n es pot calcular a partir de $U_{n-1}, U_{n-2}, ...$

Proposicions →

i. *Progressions asimètriques*: és una successió $\{U_n\}_{n \geq 0}$ tal que existeix una d fixada (*diferència*) de manera que

$$U_{n+1} = U_n + d$$

ii. *Progressions geomètriques*: és una successió $\{U_n\}_{n \geq 0}$ tal que existeix una r fixada (*raó*) de manera que

$$U_{n+1} = r \cdot U_n$$

iii. *Successions (exemple)*: calcular el número de successions de longitud n formades per zeros i uns sense que hi hagi dos zeros consecutius. Es resol de la següent manera: sigui U_n el número buscat, una tira del problema és

$$x_1, x_2, ..., x_n, \quad x_i \in \{0, 1\}$$

Primer cas: $x_n = 1$. Llavors la successió $x_1, x_2, ..., x_n$ no té zeros consecutius.
Segon cas: $x_n = 0$. Llavors, tenim que $U_n = U_{n-1} + U_{n-2}$, com per exemple, la seqüència de Fibonacci.

Definició → La successió $\{F_n\}_{n \geq 0}$ que verifica que $F_0 = 0$, $F_1 = 1$, i $F_{n+2} = F_{n+1} + F_n$ s'anomena *Successió de Fibonacci*.

Definició → Sigui $\{U_n\}_{n \geq 0}$ una successió, direm que $\{U_n\}_n$ verifica una recurrència lineal homogènia d'ordre *k* (o *gran k*) si existeixen constants $a_1, ..., a_k \in \mathbb{R}$ tals que

$$U_{n+k} + a_1 \cdot U_{n+k-1} + ... + a_k \cdot U_n = 0$$

és a dir, que U_k és combinació lineal d'$U_n, U_{n+1}, ..., U_{n+k-1}$.

Exemple → Si l'ordre k = 1, $U_{n+1} + a_1 \cdot U_n = 0$. Si $r = -a_1$, tenim que $U_{n+1} = r \cdot U_n$.

Si l'ordre k = 2, tenim que $U_{n+2} + a_1 \cdot U_{n+1} + a_2 \cdot U_n = 0$. Llavors, $U_{n+2} = -a_1 \cdot U_{n+1} - a_2 \cdot U_n$. Si $-a_1 = -a_2 = 1$, obtenim la Recurrència de Fibonacci.

Definició → Donada una successió $\{U_n\}_n$ que verifica una recurrència, direm que s'ha resolt si es té una expressió de la forma

$$U_n = f(n) \text{ per tota } n \geq 0$$

Exemples →

i. Aritmètica
$U_{n+1} = U_n + d$
$U_0 = 0, U_1 = d, U_2 = 2d, \ldots \quad U_n = n \cdot d$

ii. Geomètrica
$U_{n+1} = r \cdot U_n$
$U_0 = 1, U_1 = r, U_2 = r^2, \ldots \quad U_n = r^n$

Teorema → Sigui $\{U_n\}_n$ una successió que verifica una recurrència lineal i homogènia d'ordre 2,

$$U_{n+2} + a_1 \cdot U_{n+1} + a_2 \cdot U_n = 0, \text{ per tota } n \geq 0$$

Siguin α, β les arrels de l'equació auxiliar

$$t^2 + a_1 \cdot t + a_2 = 0$$

Si $\alpha \neq \beta$, llavors existeixen constants A i B tals que

$$U_n = A \cdot \alpha^2 + B \cdot \beta^2$$

Si $\alpha = \beta$, llavors existeixen constants C i D tals que

$$U_n = (C \cdot n + D) \cdot \alpha^n$$

Les constants A, B o C, D es determinen a partir de U_0 i U_1.

Exemple → La successió de Fibonacci és

$$F_{n+2} = F_{n+1} + F_n, \text{ amb } F_0 = 0 \text{ i } F_1 = 1$$

L'equació auxiliar, polinòmica, és

$$t^2 - t - 1 = 0$$

perquè $F_{n+2} + (-1) \cdot F_{n+1} + (-1) \cdot F_n = 0$

Les arrels de $t^2 - t - 1 = 0$ són

$$\frac{1}{2}\left(1 \pm \sqrt{5}\right)$$

El teorema segueix i diu que

$$F_n = A \cdot ((1 + \text{sqrt}(5))/2)^n + B \cdot ((1 - \text{sqrt}(5))/2)^n$$

Obtenim un sistema d'equacions que, al resoldre'l,

A = $\frac{1}{\sqrt{5}}$

B = - $\frac{1}{\sqrt{5}}$

Llavors, F_n = $\frac{1}{\sqrt{5}}$ · $((1 + \text{sqrt}(5))/2)^n - (1 - \text{sqrt}(5))/2)^n)$

$\frac{1}{\sqrt{5}}$ S'anomena *número auri* o *número d'or*.

Definició → Direm que una successió $\{U_n\}_n$ verifica una relació de recurrència lineal i no homogènia si existeixen constants $a_1, ..., a_k \in \mathbb{R}$ tals que

$$f(n) = U_{n+k} + a_1 \cdot U_{n+k-1} + ... + a_k \cdot U_n, \text{ on } f(n) \text{ és una funció.}$$

Teorema → Sigui $\{U_n^{(p)}\}_n$ una solució particular de la relació de recurrència $U_{n+k} + a_1 \cdot U_{n+k-1} + ... + a_k \cdot U_n$, llavors qualsevol altra solució al sistema d'equacions

Sistema homogeni

$$\left\{\begin{matrix} 2x + 3y = 0 \\ 7x + 5y = 0 \end{matrix}\right\}$$

Sistema no homogeni

$$\left\{\begin{matrix} 2x + 3y = 0 \\ 7x + 5y = 1 \end{matrix}\right\}$$

és de la forma $\{ U_n^{(p)} + U_n^{(h)}\}_{n \geq 0}$, on $\{U_n^{(h)}\}_h$ és una solució de la relació homogènia associada.

Exemple → Resoldre la recurrència $U_{n+1} - 3 \cdot U_n = 2n + 2$.
Veiem que l'equació associada és $t - 3 = 0$, i la solució general és $U_n = A \cdot 3^n$. Cal buscar una solució particular de $U_{n+1} - 3 \cdot U_n = 2n + 2$. Mirem si existeix alguna solució de la forma $U_n = c \cdot n + d$.

En cas de que existeixi, $(c \cdot (n + 1) + d) - 3 \cdot (n + d) = 2n + 2$, que reordenant queda $(-2c - 2) \cdot n + (c + d - 3d - 2) = 0$.
Extraiem que $c = -1$, $c - 2d - 2 = 0$, i $d = -3/2$.
Per tant, la solució general a la recurrència és $U_n = A \cdot 3^n + (-n - 3/2)$. Caldrà definir el valor d'A. Sabem que $U_0 = A \cdot 3^n - 3/2$, per tant, $A = U_0 + 3/2$.

Teorema → Donada una seqüència lineal $U_{n+k} + a_1 \cdot U_{n+k-1} + ... = f(n)$, on $f(n)$ és un polinomi de grau *t*, llavors existeix una solució particular U_n que és un polinomi en n de grau *t*.

Exemple → Les Torres de Hanoi. Sigui H_n el número de moviments per resoldre el puzle, deduïm que $H_2 = 3$. És a dir, si tenim dues peces haurem de fer tres moviments. $H_{n+1} = 2 \cdot H_n + 1$, $H_n = -1$ és una solució particular. La solució general és $H_n = A \cdot 2^n - 1$, tals que $H_2 = 3$, i llavors $A = 1$. Obtenim, com a solució general, que $H_n = 2^n - 1$.

3. Teoria de grafs

3.1. Definicions bàsiques

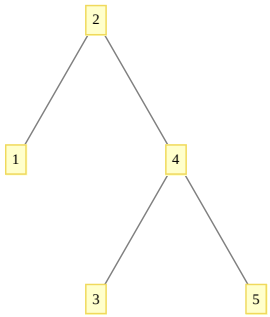
Definició GRAF → És una parella G = (V, E) on:

i. 'V' és un conjunt d'elements, que se'ls anomena *vèrtexs*, i

ii. 'E' és un conjunt de parells no ordenats de vèrtexs diferents entre ells. Els seus elements se'ls anomena *arestes* de G.

Observacions →

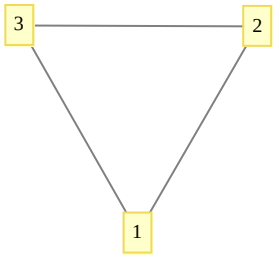
1. En el següent graf,



V = {1, 2, 3, 4, 5}

E = {1→2, 2→4, 3→4, 4→5}

2. Es permeten grafs amb bucles, com



Exemples →

i. V = pàgines web, on dues pàgines estan unides si hi ha un *link* entre una web i una altra.

ii. V = ciutats d'una regió, on dues ciutats estan unides si hi ha una autopista que va d'una ciutat a una altra (problema del viatjant de comerç, Algorísmica).

iii. V = xarxes telefòniques, on les línies es connecten entre sí.

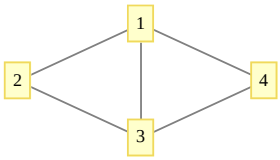
Definició VÈRTEXS ASJACENTS → Són aquells vèrtexs que estan units per una aresta. En cas contrari, s'anomenen *independents*.

Definició GRAU DEL VÈRTEX → Si v_i és un vèrtex del conjunt V = $\{v_1, ..., v_n\}$, el grau del vèrtex v_i, que denotarem $d(v_i)$, és el número de vèrtexs adjacents a vi, és a dir, el número d'arestes que surten de v_i.

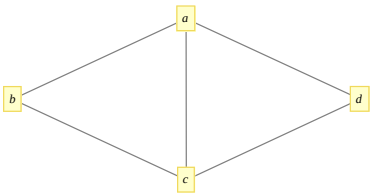
Definició GRAF ISOMORFE → Siguin els parells $G_1 = (V_1, E_1)$ i $G_2 = (V_2, E_2)$, es diu que G_1 i G_2 són isomorfes si existeix una aplicació lineal bijectiva $f: V_1 \longrightarrow V_2$ que preserva adjacències, és a dir, u, v $\in E_1$ sí i només sí f(u), f(v) $\in E_2$. Es diu que *f* és un *isomorfisme de grafs*.

Exemple → Donats els grafs

(a)



(b)



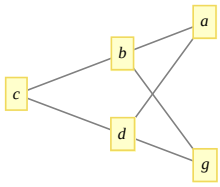
veiem que són isomorfes (equivalents), ja que

	f	
1	→	a
2	→	b
3	→	c
4	→	d

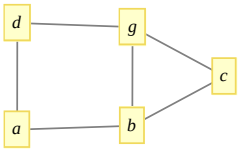
Tot i així, la seva representació pot ser molt diferent entre dos dibuixos del mateix graf.

Definició INVARIANT DEL GRAF → Una variant associada al graf G = (V, E) és un número i(G) associat a G tal que G és isomorf a G_1 si i només si i(G) = i(G_1).

Exemple → i = número de vèrtexs del graf, o un altre exemple, i = número d'arestes, o i = número de vèrtexs el gran dels quals $d_0 \in \mathbb{N}$ està fixat.



i(g) = 2



i(g) = 3

Proposició → Sigui G = (V, E) un graf i $v \in V(G)$, aleshores

$$\Sigma d(v) = 2 \cdot \#E(G)$$

Demostració → Cada aresta es compta dues vegades al calcular els graus dels vèrtexs.

Corol·lari → El número de vèrtexs de qualsevol grafs amb grau imparell és parell.

Demostració → Sigui G = (V, E) un graf,

$$2 \cdot \#E(G) = \Sigma d(v) = \Sigma d(v_{parell}) + \Sigma d(v_{imparell})$$

D'aquí, la suma de totes les d(v) és parell. $\#\{v \in V \mid d(v) \text{ és imparell}\}$ resulta ser parell.

Proposició → En tot graf, sempre hi ha com a mínim dos vèrtexs amb el mateix grau.

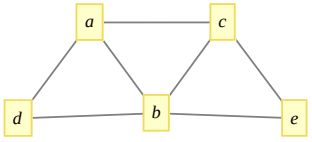
Demostració → Suposem que G = (V, E) és un graf amb vèrtexs $B = \{v_1, ..., v_n\}$, $n \in \mathbb{N}$, tindrem que $d(v_1), ..., d(v_n) \in \{0, 1, ..., n - 1\}$. Si no hi ha repeticions entre els números $d(v_1), ..., d(v_n)$, llavors ha d'existir un vèrtex de grau i per tota i que pertany a $\{0, 1, ..., n - 1\}$. Existeix una v_i de grau 0, existeix una v_j de grau $n - 1$. En aquest últim cas, v_j està connectat amb tots els altres vèrtexs.

3.2. Representació matricial

Definició MATRIU D'ADJACÈNCIA → La matriu d'adjacència d'un graf g = (V, E) amb vèrtexs $V = \{v_1, ..., v_n\}$, és la matriu quadrada $A(G) \in M_{n \times n}(\mathbb{R})$ definida per

$$A(G)_{ij} = \begin{cases} 1, \text{ en cas que } v_i, v_j \in E(G) \\ 0, \text{ en un altra cas} \end{cases}$$

Exemple → Trobar la matriu d'adjacència del següent graf.



$A(G) =$

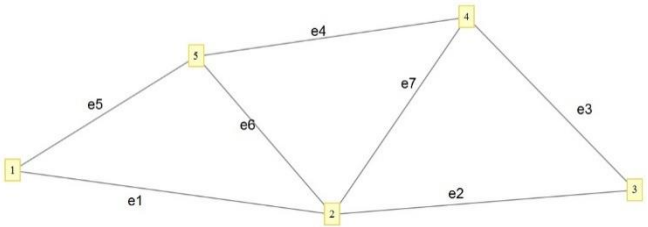
	a	b	c	d	e
a	0	1	0	0	1
b	1	0	1	1	1
c	0	1	0	1	0
d	0	1	1	0	1
e	1	1	0	1	0

La matriu A(G) sempre té zeros a la diagonal principal i és simètrica, ja que $A = A^t$.

Definició MATRIU D'INCIDÈNCIA → Donat un graf G = (V, E), $V(G) = \{v_1, ..., v_n\}$, $E(G) = \{e_1, ..., e_n\}$, la matriu d'incidència és $B(G)_{m \times n}$ definida per

$B(G)_{ij}$ = { 1, en cas que v_i sigui un extrem d'e_j ; 0, en un altra cas

Exemple → Trobar la matriu d'incidència del següent graf.



B(G) =

	e1	e2	e3	e4	e5	e6	e7
1	1	0	0	0	1	0	0
2	1	1	0	0	0	1	1
3	0	1	1	0	0	0	0
4	0	0	1	1	0	0	1
5	0	0	0	1	1	1	0

3.3. Camins. Recorreguts eulerians i hamiltonians

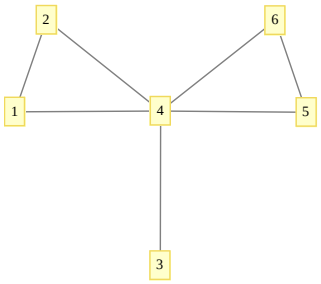
Definició RECORREGUT → Donat un graf G = (V, E), una seqüència de vèrtexs U_0, ..., U_e, on $U_{i-1}U_E \in E(G)$ per totes les $i \in \{1, ..., e\}$, i on $U_i U_{i+1} \neq U_j U_{j+1}$ si $i \neq j$, s'anomena recorregut R de longitud L entre U_0 i U_e.

Definició CIRCUIT → És un recorregut tancat, és a dir, $U_0 = U_e$.

Definició CAMÍ → Quan tots els vèrtexs d'un recorregut R són diferents entre ells.

Definició CICLE → És un camí tancat.

Exemple →



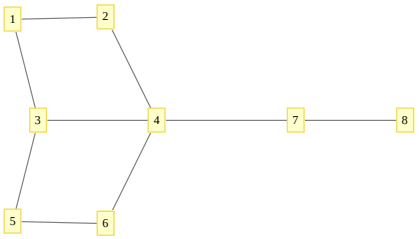
Un exemple de recorregut en el graf seria el següent: 1→2→4→5

Definició DISTÀNCIA → Sigui G un graf, i u, v ∈ V(G), suposem que existeix algun camí entre u i v. Llavors, definirem la distància entre u i v, que denotarem d(u, v) com la longitud mínima d'un camí entre u i v.

Definició GRAF CONVEX → Es diu que un graf G és convex si per cada u, v ∈ V(G) existeix un camí entre u i v.

Definició DIÀMETRE → Si G és un graf convex, el diàmetre de G és la major de les distàncies entre dos vèrtexs de G. D(G) = màx{d(u, v)}.

Exemple → Per anar del punt 1 al punt 8, agafem la major de les distàncies, que és d(1, 8), d(1, 6), ... i l'anomenarem *diàmetre*.



Definició EXCENTRICITAT → Sigui G un graf convex, es defineix l'excentricitat d'aquest com un vector v ∈ V(G), per

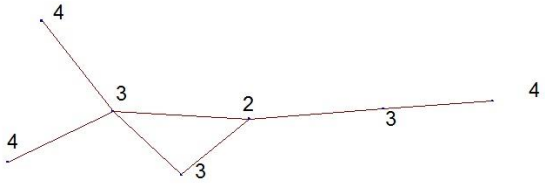
$$e(v) = \max\{d(v, w) \mid w \in V(G)\}$$

Definició RADI → r(G) = min{e(v)}, v ∈ V(G).

Definició CENTRE → Conjunt dels vèrtexs d'excentricitat mínima. Z(G) = {v ∈ V(G) | e(v) = r(G)}.

Definició PERIFÈRIA → Conjunt de vèrtexs on l'excentricitat és màxima. P(G) = {v ∈ V(G) | e(v) = D(G)}.

Exemple → Buscar dades en el següent graf.
Excentricitats dels vèrtexs:



Per tant, el radi del graf, que és la menor de les excentricitats, és 2.
r(G) = 2, D(G) = 4.
El centre del vèrtex és el vèrtex marcat com a "2" en el dibuix.
Les perifèries del graf són els 4 4 4.

Definició TIPUS DE GRAFS →

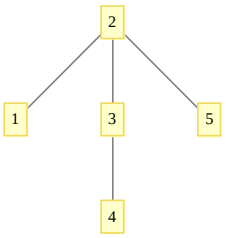
i. Un cicle és un graf en el què tots els vèrtexs són de grau 2 (triangle, quadrat, ...).
ii. Es diu que un graf és complet quan qualsevol dels vèrtexs determina una aresta que els determina.
iii. Un graf connex que no conté camins tancats (cicles), s'anomena arbre.

iv. Un graf bipartit és aquell que el conjunt de vèrtexs es pot descompondre en una unió de dos vèrtexs de manera que tota aresta de G = (V, E) connecta un vèrtex V_1 a un altre V_2.

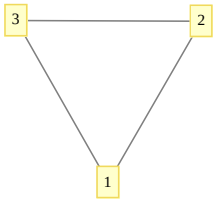
$V = V_1 \cup V_2$, $V_1 \neq 0$, $V_2 \neq 0$, intersecció entre V_1 i $V_2 = 0$.

v. Sigui G = (V, E) un graf bipartit amb parts V_1 i V_2, es diu que G és bipartit complet si tot el vèrtex de V_1 és adjacent a tots els vèrtexs de V_2.

Exemple →



És bipartit

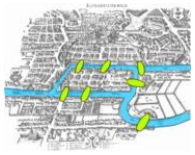


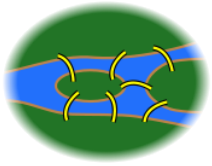
No és bipartit

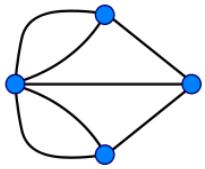
Teorema → Sigui G = (V, E) un graf i sigui A = A(G), és a dir, la matriu d'adjacència. Donada una $k \geq 1$, $(A^k)_{ij}$ = número de recorreguts entre v_i i v_j de longitud k. Es poden repetir arestes i/o vèrtexs.

Demostració → Si k = 1, per definició sobre la matriu A, tenint en compte que no hi ha bucles ni més d'un vèrtex entre dos punts. k – 1 implica que, per definició del producte de matrius, $(A^k)_{ij} = (A^{k-1} \cdot A)_{ij} = \Sigma$ d'l = 1 fins a l = n de $(A^{k-1})\ l_j\ A_i\ l$. El terme l-èssim només és diferent de zero si $(A^{k-1})\ l_{ij} \neq 0$, $A_{il} = 1$. Per hipòtesis d'inducció, so $m = (A^{k-1})l_j$, existeixen n camins de longitud k – 1 entre v_i i v_j.

Definició GRAFS EULERIANS → Problema dels ponts de Könisberg. És possible trobar un recorregut que passi només una vegada per cada pont però que passi per tots?







Euler va trobar la solució a aquest problema real de la ciutat russa pertanyent a Kaliningrad, un enclavament rus al mar bàltic. La resposta és que no és possible. El problema de Kaliningrad va portar a l'inici de la teoria de grafs.

Definició MULTIGRAF → Graf on hi poden existir bucles i/o diferents arestes que uneixen els vèrtexs.

Definició RECORREGUT EULERIÀ → És un circuit que passa una i només una vegada per cada una de les arestes del multigraf.

Definició MULTIGRAF EULERIÀ → Graf que admet un recorregut eulerià.

Teorema d'EULER → Sigui G un multigraf connex. Llavors, G és eulerià si i només si tots els vèrtexs de G tenen el grau parell. El graf dels ponts de Könisberg no té solució perquè no compleix el teorema d'Euler.

Demostració → Al recórrer un circuit eulerià, cada vegada que arribem a un vèrtex, hem de sortir per una aresta diferent a la d'entrada, de manera que el vèrtex ha de ser parell.

Per altra banda, suposem que G és connex i tots els vèrtexs són de grau parell. Sigui $v_0 \in V(G)$ un vèrtex arbitrari i fixat, construïm un recorregut a partir de v_0 sense utilitzar dues vegades la mateixa aresta. Si l'extrem és $x \neq v_0$, com que d(x) és parell, podem sortir d'x i continuar el recorregut. Així, podem suposar que el recorregut acaba a v_0. Al recorregut així obtingut l'anomenarem c_0. Si c_0 conté totes les arestes del graf, llavors, sigui G el graf que s'obté traient-li a G les arestes de c_0, pot no ser convex. Sigui H una component connexa de G' que contingui alguna aresta. Com que G és connex, H ha de contenir algun vèrtex v que està a c_0.

Igual que abans, construïm un circuit en H amb inici i final a c_1, veient que no conté arestes de c_0. $c_0 \in c_1 = (V(c_0) \cup V(c_1), E(c_0) \cup E(c_1))$. Llavors, c_0 i c_1 determina un circuit que no repeteix arestes, que té més arestes que c_0, que són les de c_1. Si $c_0 \cup c_1$ conté totes les arestes de G, hem acabat. Sinó, repetim aquest procés. Com que el número d'arestes és finit, al final tindrem un recorregut eulerià.

Aquesta demostració es pot utilitzar com un algorisme. S'anomena *Algorisme de Hierhotzer*.

Teorema → Sigui G un multigraf convex, llavors G conté un recorregut eulerià si i només si el número de vèrtexs de grau imparell és o 0 o 2.

Demostració → Suposem que G conté un recorregut eulerià u, ... v ($u, v \in V(G)$). Si aquest recorregut no és un circuit, sigui G' = G + uv (afegim una aresta entre u i v) ja tenim un circuit eulerià. Llavors, G' és un multigraf connex i eulerià si i només si tots els vèrtexs de G' tenen grau parell. Aleshores, tots els vèrtexs de G tenen grau parell excepte u i v.

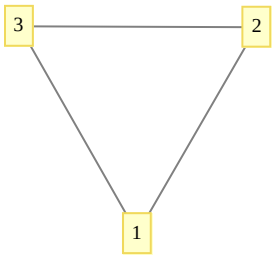
Si no hi ha vèrtexs de gra imparell, llavors tots són de grau parell i G conté un circuit eulerià. Si hi ha dos vèrtexs de grau imparell, i siguin u i v, agafem G' = G + uv. G' conté un circuit eulerià, ergo G també conté un circuit eulerià, que passa per totes les arestes.

Definició CICLE HAMILTONIÀ → Un cicle hamiltonià en un graf G és un camí tancat que passa només una vegada per tots i cada un dels vèrtexs de G, exceptuant el vèrtex inicial, que és també el final.

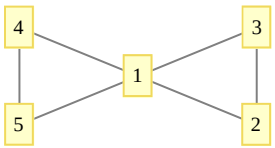
Definició GRAF HAMILTONIÀ → Es diu que un graf G és hamiltonià si conté un cicle hamiltonià.

Definició CAMÍ HAMILTONIÀ → És un camí que passa una i només una vegada per cada un dels vèrtexs, però el vèrtex inicial és diferent que el vèrtex final.

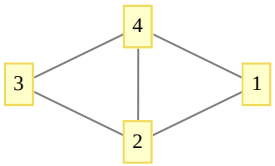
Exemples →



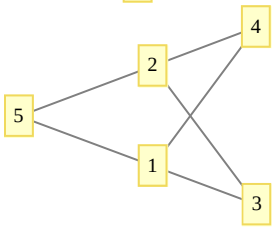
Eulerià i hamiltonià alhora.



Eulerià però no hamiltonià.



No eulerià però hamiltonià.



Ni eulerià ni hamiltonià.

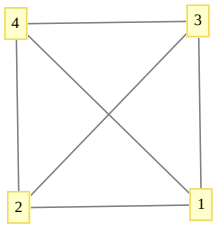
Teorema DE ORE → Sigui G un graf d'n vèrtexs, amb n ≥ 3, si per cada parell de vèrtexs no adjacents u, v es compleix que d(v) + d(u) ≥ n, llavors G és hamiltonià.

Teorema DE DIRAC → Sigui G un graf amb n vèrtexs, n ≥ 3, si

$$\min \{d(v)\} \geq n/2$$

llavors G és hamiltonià.

Exemple → Donat el graf G,



d(1)=d(2)=d(3)=d(4)=3. min {d(v)} = 3 ≥ 2.

Confirmem que G és hamiltonià.

3.4. Coloracions

Problema → Donat un mapa pla, hi ha alguna manera de colorejar països amb fronteres contigües amb menys de quatre colors?.

Observació → Cada país és un vèrtex. Cada frontera comuna entre dos països és una aresta.

Història → L'any 1879, Kempe va demostrar que 4 colors és el mínim per colorejar un mapa. Però va ser al 1890 quan Heamwood va dir que l'afirmació era falsa. Al 1977, un grup de científics de la computació anomenats Appel, Hakem i Koch van estar 1200 hores computant el problema.

Demostració → Per inducció, la demostració es basa en dues nocions: el conjunt inevitable de configuració i la configuració reduïble. Complerts aquests requisits, els tres científics van trobar 1936 configuracions. Al 1996 aquestes 1936 configuracions es van reduir a 633.

Per tant, és fàcil demostrar que amb cinc colors es pot colorejar qualsevol mapa però és molt difícil demostrar que amb quatre colors es pot colorejar qualsevol mapa.

Actualment, s'accepta que amb quatre colors n'hi ha prou, però pot ser que d'aquí a un cert temps es demostri el contrari.

Definició COLORACIÓ → Sigui G = (V, E) un graf. Una coloració dels vèrtexs de G és una funció aplicació lineal $c : V \longrightarrow \mathbb{N}$ tal que si x, y ∈ E, llavors c(x) ≠ c(y).

Definició NÚMERO CROMÀTIC → El número cromàtic d'un graf G, que es denota X(G), és el menor enter k ∈ ℕ tal que existeix una coloració de G

$$c : V(G) \longrightarrow \mathbb{N}$$

tal que c(V(G)) ∈ {1, 2, ..., k}.

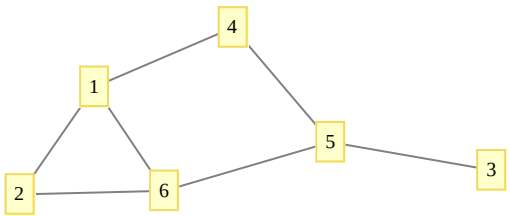
Observació → Teorema dels quatre colors: G és pla, llavors X(G) ≤ 4.

Exemple → S'han de programar sis conferències d'una hora cada una. Siguin v_1, ..., v_6 les conferències, sabem que hi ha persones que volen escoltar les següents configuracions:

$$(v_1, v_2), (v_1, v_4), (v_3, v_5), (v_2, v_6), (v_4, v_5), (v_5, v_6), (v_1, v_6)$$

Quantes hores seran necessàries, com a mínim?

Podem transformar el problema en el següent graf:



Amb:

1: de nou a deu

2, 5: de deu a onze

3, 4, 6: d'onze a dotze

Definició ARBRE → És un graf connex que no conté cicles, la forma del qual s'assembla a un arbre d'on en surten branques i cap branca s'ajunta a una altra branca.

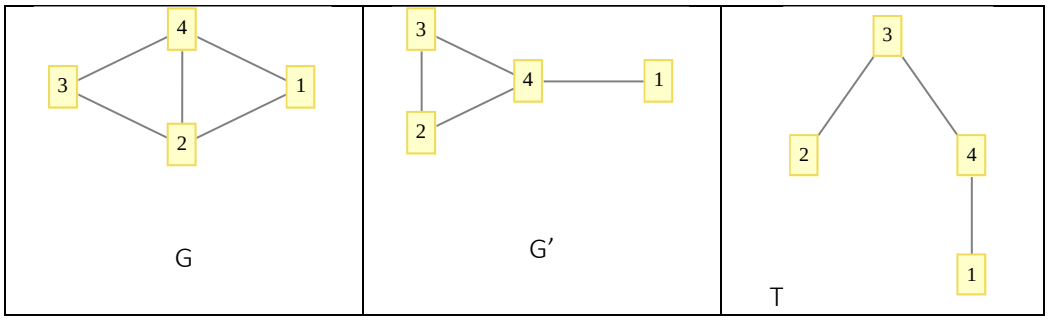
Teorema → Són equivalents per a un graf G = (V, E).

i. G és un arbre.
ii. Entre cada parell de vèrtexs de G, existeix un únic camí.
iii. G és connex i #V = #E + 1.
iv. G és connex però si li traiem una aresta ja no ho és.

Demostració → Idea de que l'apartat (i) implica (ii). Si G és un arbre, donades v, u existeixen dues maneres d'anar de v a u. Com que existeix un cicle, ja tenim una de les aplicacions. Suposem que existeix un cicle dintre del graf. Es compleix el mateix però al revés.

Definició ARBRE GENERADOR → Sigui G = (V, E) un graf. Es diu que un graf G' = (V', E') és un subgraf de G si V' ∈ V i E' ∈ E. També es diu que G' és un subgraf generador de G si V' = V i E' ∈ E. També es diu que un arbre T és generador d'un graf G si és un subgraf generador de G.

Exemple →



Teorema → Tot graf connex té un graf arbre generador.

Demostració → Sigui G = (V, E) un graf connex, i sigui u ∈ V(G) un vèrtex, per cada v ∈ V(G), amb u ≠ v, tindrem un vèrtex w tal que d(v ,w) = d(u, v) = 1.

Sigui E' el conjunt d'arestes de G, llavors T = (V, E') és un arbre generador de G. Aquesta demostració també és un algorisme.

Definició GRAF AMB PESES → És un graf G = (V, E) i una aplicació lineal w: E $\longrightarrow$ $\mathbb{R}$ (és a dir, assignem un número a cada una de les arestes).

Definició PES DE L'ARBRE → Sigui G = (V, E) un graf connex i T un arbre generador, anomenarem pas de l'arbre T a w(T) = suma de totes les peses de les arestes que apareixen a T.

Problema → Donat un graf connex, amb peses, trobar un arbre generador de mes mínim (o màxim).

Una aplicació seria com donar servei de fibra òptica a un barri sencer amb el mínim cost.

Algorisme DE GREEDY → Trobar una bona solució localment, despreocupant-se de futurs costos d'ampliació del graf. No és una solució aplicable a tot arreu.

Algorisme DE KRUSKAL →

ENTRADA: Un Graf connex expressat amb peses.

SORTIDA: Un arbre generador minimal.

1. Ordenar les arestes del graf G en ordre creixent en quant a número de peses.
2. Considerar el graf T = vèrtexs e G sense les arestes.
3. Afegir a T la primera aresta de la llista.
4. Considerem la següent aresta de la llista. Si aquesta forma un cicle amb les que tenim, la ignorem. Si no forma un cicle, l'agafem i l'afegim a T.
5. Repetim el pas 3 fins a obtenir un graf T connex.

El resultat d'aquest algorisme és un arbre generador minimal de G.

Teorema → Si G = (V, E) és un graf connex, l'algorisme de Kruskal produeix un arbre generador de pes mínim.

Demostració → El graf obtingut a través de l'algorisme no conté cicles i és connex, ergo és un arbre. L'arbre obtingut conté el graf inicial format pels vèrtexs de G, cosa que implica que és un graf generador.

Suposem que l'arbre obtingut T no és minimal. Sigui T' un arbre generador minimal,

$$w(T') < w(T)$$

Sigui *d* la primera aresta, en l'ordre fixat que no està als dos arbres, més concretament, que és de T però no de T'.

Considerem T' – d' + d, es té que aquest graf és arbre generador i minimal.

LLISTES D'EXERCICIS

Matemática Discreta

Quatrimestre de Primavera 2014

Lista 1 - Aritmética entera y modular

1. Convertir los siguiente números de base decimal a base binaria: 999_{10}, 1984_{10}. Convertir 10101111_2 i 101001000_2 de base binaria a decimal.

2. Expresar 706113_8 en base decimal y 89156_{10} en base octal.

3. La conversión del sistema binario al octal o al hexadecimal se puede hacer de una forma sencilla teniendo en cuenta que 8 i 16 son potencias de 2; encontrarla.

a) Convertir 2154_8 al sistema binario. Expresar 110100101_2 en base octal.

b) Convertir 100011110101_2 y 11101001110_2 al sistema hexadecimal. Expresar los números hexadecimals $ABCDEF_{16}$ y $9A0B_{16}$ en el sistema binario.

4. Sabemos que el número 136_{10} se expresa en la base b como 253. Encontrar la base b.

5. Buscar el MCD de las parejas de números siguientes usando el algoritmo de Euclides: (45, 75), (252, 198), (162, 222), (666, 1414), (721, 448) y (20785, 44350).

6. Expresar el MCD de 45 y 75 de la forma $45m + 75n$ con $m, n \in \mathbb{Z}$. Haced lo mismo con las demás parejas del problema anterior.

7. Calcular el MCM de 721 y 448 y de 20785 y 44350.
(Recordad: $\text{MCM}(a, b)\text{MCD}(a, b) = ab$.)

8. Dados dos números $a, b \in \mathbb{Z}$ coprimos, demostrar que el MCD de $a + b$ y $a^2 + b^2$ es 2 si a y b son impares y 1 en caso contrario.

9. Hemos instalado el sistema operativo Linux en dos particiones distintas: hda1 y hda2. Cada cierto número de veces que encendemos el ordenador se comprueban estas particiones. La partición hda1 se comprueba cada 31 veces y la partición hda2 cada 22 veces. Demostrar que alguna vez se comprueban ambas particiones simultáneamente. Calcular la frecuencia con la que se comprueban simultáneamente.

10. Buscar números enteros m, n tales que $966m + 686n = 70$.

11. El Dr. Fliess (conocido per su amistad y correspondencia con S. Freud) explica, en su libro *Der Ablauf des Lebens: Grundlegung zur exakten Biologie* que la vida humana está regida por un ciclo masculino de 23 dias y un ciclo femenino de 28. Este es el origen de la célebre teoría de los bioritmos. Concretamente, Fliess explica en su libro como muchos momentos críticos de la vida de una persona se pueden explicar sumando o restando un número entero de ciclos femeninos y masculinos. Demostrar que, en el momento en que el propio Fliess murió, el número de cabellos que tenía en la cabeza era suma o resta de un múltiplo de 23 y un múltiplo de 28, confirmando así su teoría.

12. Construir las tablas de sumar y de multiplicar de $\mathbb{Z}/8$.

13. Decir qué elementos son invertibles y cuáles son divisores de cero en $\mathbb{Z}/8$, $\mathbb{Z}/10$, $\mathbb{Z}/17$ y $\mathbb{Z}/24$.

14. Demostrar que un número es divisible por tres si y sólo si la suma de sus dígitos en base decimal es múltiplo de 3.

15. Sea n un número natural y sea $(x_k x_{k-1} \dots x_0)_{10}$ su representación en base 10. Sea $\theta(n) = x_0 + x_1 + \cdots + x_k$. Demostrar que

$$n \equiv \theta(n) \mod 9.$$

16. La conocida "prueba del 9" se basa en la propiedad $\theta(xy) \equiv xy \equiv \theta(x)\theta(y)$, consecuencia del problema anterior. Usar este hecho para demostrar que dos de los siguientes productos son erroneos. ¿Qué se puede decir del otro producto?

1. $5783 \times 40162 = 233256846$
2. $9787 \times 1258 = 12342046$
3. $8901 \times 5743 = 52018443$.

17. Calcular módulo 47 las potencias de 2 siguientes: 2^{32}, 2^{47}, 2^{200}.

18. Resolver las siguientes ecuaciones

$$\begin{array}{rcll} 2x & \equiv & 5 & (\text{mod } 7), \\ 3x & \equiv & 6 & (\text{mod } 9), \\ 19x & \equiv & 30 & (\text{mod } 40), \\ 9x & \equiv & 5 & (\text{mod } 25), \end{array} \qquad \begin{array}{rcll} 103x & \equiv & 444 & (\text{mod } 999), \\ 980x & \equiv & 1500 & (\text{mod } 1600), \\ 128x & \equiv & 833 & (\text{mod } 1001), \\ 987x & \equiv & 610 & (\text{mod } 1597). \end{array}$$

19. Encontrar una solución del sistema de ecuaciones

$$\begin{cases} x + 2y = 4 \\ 4x + 3y = 4 \end{cases}$$

en $\mathbb{Z}/7$. ¿Existe alguna solución en $\mathbb{Z}/5$?

20. Resolver la ecuación $x^2 - 3x - 3 = 0$ en $\mathbb{Z}/7$.

21. Buscar un número entero C no divisible por 11 y tal que la sucesión de números $a_n = C^n$ satisfaga la ecuación

$$a_n \equiv a_{n-1} + a_{n-2} \quad \text{mód } 11.$$

22. Buscar el último dígito de la expresión decimal de 7^{1000}.

23. Calcular 11^{289} mód 360 y 7^{418} mód 120

24. Resolver

$$\begin{array}{rcll} 5x & \equiv & 12 & (\text{mod } 13), \\ 7x & \equiv & 3 & (\text{mod } 11), \\ 5x & \equiv & 3 & (\text{mod } 14), \end{array} \qquad \begin{array}{rcll} 4x & \equiv & 7 & (\text{mod } 15), \\ 3x & \equiv & 5 & (\text{mod } 16), \end{array}$$

25. Calcular $\varphi(2000)$, $\varphi(2001)$, $\varphi(2002)$, $\varphi(2003)$ y $\varphi(2004)$.

26. Buscar una solución del sistema

$$\begin{cases} 10x \equiv 2 & \text{mód } 4 \\ 3x \equiv 1 & \text{mód } 5 \\ x \equiv 2 & \text{mód } 3 \end{cases}$$

27. Para hacer el recuento de las tropas después de una batalla, los generales chinos distribuían sus soldados en filas de diferente longitud y contaban la cantidad de soldados restantes en cada distribución. A partir de estos residuos calculaban el total. Un general tenía 1200 soldados al comenzar una batalla. Una vez terminada, le sobraban 3 soldados si formaban en filas de 5, sobraban 3 si las filas eran de 6, sólo sobraba uno si las filas eran de 7 y ninguno si las filas eran de 11. ¿Cuántos soldados sobrevivieron a la batalla?

28. Un pastor tiene un cierto número de ovejas. Nos ha dicho que si las cuenta de 2 en 2 sobra una, si las cuenta de 3 en 3 sobran 2, si las cuenta de 4 en 4 sobran 3, si las cuenta de 5 en 5 sobran 4, si las cuenta de 6 en 6 sobran 5 y si las cuenta de 7 en 7 sobran 6, pero no tiene más de 500 ovejas. ¿Cuántas ovejas tiene el pastor?

29. Codificar el mensaje

NO ENTREGUEIS ESTE SOBRE

usando el cifrado afín $C \equiv 7P + 10 \pmod{26}$

30. Decodificar el mensaje siguiente

KT VTULVTUDPT ADJPYLUT JDYQL CTYT PRADWDPTY VLGJTOLJ

que ha estado codificado usando el cifrado afín $C \equiv 11P + 19 \pmod{26}$.

31. Julio César solía usar congruencias para encriptar sus mensajes. Primero ordenaba alfabéticamente las 23 letras del alfabeto (latino romano) y asociaba a cada letra α su posición $p(\alpha)$, de 0 hasta 22. Así la letra A quedaba asociada al 0, la B al 1, la C al 2,.... Luego, sumaba 3 módulo 23 a las posiciones de las letras. Al final, cada letra α quedaba asociada al entero $p(\alpha) + 3 \pmod{23}$.
Vamos a usar como alfabeto el conjunto ordenado de sólo 7 letras (B,C,E,H,I,N,O). Para aplicar el método de César tendremos que trabajar módulo 7. ¿Cuál sería, en este caso, el sentido del mensaje 3051 65462?.

32. Se intercepta el texto cifrado:

FIUBVMUBZXBIUWCZH

que fue cifrado usando un código afín en el alfabeto de 27 letras (La A a Z de 0 a 25, y el espacio en blanco 26). Se sabe que la primera letra es L, y la segunda es O. Determinar la clave del cifrado y leer el mensaje.

Matemática Discreta

Quatrimestre de Primavera 2014

Lista 2 - Combinatoria

1. Sean σ y τ las permutaciones de S_7 siguientes:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 2 & 4 & 1 & 7 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 2 & 1 & 3 & 4 & 5 \end{pmatrix}.$$

i) Calculad $\sigma \circ \tau$ y $\tau \circ \sigma$. ¿Son iguales?

ii) Escribid σ^{-1} y τ^{-1} en notación estándar.

iii) ¿Conmutan entre sí σ y τ^{-1}?

2. Sean σ y τ dos permutaciones de S_n y sea $\gamma = \sigma \circ \tau$. Demostrar que $\gamma^{-1} = \tau^{-1} \circ \sigma^{-1}$. Calcular γ y γ^{-1} en el caso $n = 4$, con

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \text{i} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

3. Sean σ y τ dos permutaciones de S_n y sea $\gamma = \sigma \circ \tau \circ \sigma^{-1}$. Demostrar que $\gamma^k = \sigma \circ \tau^k \circ \sigma^{-1}$, para todo entero k.

4. Dadas las permutaciones

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix},$$

buscar una permutación γ tal que $\gamma^{-1} \circ \alpha \circ \gamma = \beta$. Hacer lo mismo con

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 8 & 3 & 2 & 1 & 4 & 7 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 7 & 6 & 8 & 4 & 2 & 5 \end{pmatrix}.$$

5. Calcular la signatura de las permutaciones α, β, γ i σ del ejercicio anterior.

6. (Parcial 2011) Calcular $\tau \circ \sigma^{-1}$, donde

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 6 & 2 & 4 & 1 & 7 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 2 & 1 & 3 & 7 & 5 \end{pmatrix}.$$

7. (Parcial 2012) Dar un ejemplo de dos permutaciones de S_9, una par i la otra impar, que conmuten.

8. Demuestra que en un conjunto de 30 personas en el que todas conocen a alguien, siempre hay, como mínimo dos, que conocen al mismo número de personas.

9. Demuestra que en un conjunto de $n > 1$ enteros podemos encontrar un par de números cuya diferencia sea divisible por $n - 1$.

10. En la asignatura de Matemática Discreta se han matriculado 92 alumnos. Demuestra que algún mes se celebran al menos 8 cumpleaños y que, por el contrario, algun mes se celebran como mucho 7 cumpleaños.

11. Sea A un subconjunto del conjunto de los primeros $2n$ números naturales.

$$A \subseteq \{1, \ldots, 2n\}.$$

Supongamos que en A hay más de n elementos. Demuestra que podemos encontrar una terna $x, y, z \in A$ tal que $x + y = z$. Encuentra un subconjunto $A \subseteq \{1, \ldots, 2n\}$ de n elementos que no cumpla esta propiedad.

12. ¿Cuántos números enteros entre 1 y 1000 (incluyendo el 1 y el 1000) no son divisibles ni por 3, ni por 7 ni por 11?

13. En una clase hay 67 estudiantes, de los cuales hay 41 que saben inglés, 20 que saben francés y 10 que conocen ambas lenguas. ¿Cuántos estudiantes no conocen ninguna de las dos? Si además hay 12 estudiantes que hablan ruso, de los cuales 7 hablan también inglés, 5 hablan también francés y 3 las tres lenguas, ¿cuántos estudiantes no hablan ninguna de las tres lenguas?

14. ¿De cuántas formas distintas podemos elegir un conjunto de 5 cartas de una baraja de 52 cartas de tal forma que haya al menos una carta de cada palo?

15. Una llave se fabrica haciendo varias incisiones de profundidad variable. Si cada incisión tiene ocho profundidades posibles, ¿cuántas incisiones necesitamos para poder fabricar un millón de llaves distintas?

16. En un grupo de 20 personas hay que elegir tres cargos: presidente, tesorero y secretario. ¿De cuántas formas se puede hacer esta elección?

17. Calcula el número de cadenas de ceros y unos de longitud n que se pueden hacer con exactamente k ceros.

18. De cuántas maneras se pueden sentar 8 personas en una mesa redonda suponiendo que:

i) Todas las sillas son diferentes.

ii) La sillas son indistinguibles entre sí, pero nos importa quién está a la derecha y a la izquierda de cada uno.

19. De cuántas maneras podemos alinear n bolas blancas iguales y m bolas negras iguales de tal forma que todas las bolas negras estén juntas. Si las bolas están numeradas, ¿cuántas maneras distintas hay?

20. ¿Cuál es la probabilidad de ganar la Lotto 6/49?

21. ¿De cuántas maneras se pueden colocar 17 chicos y 13 chicas en una fila sin que haya dos chicas juntas?

22. ¿Cuántos resultados distintos podemos obtener al tirar de una sola vez 11 dados?

23. Dado un entero $n > 0$ ¿cuántas soluciones enteras tiene la ecuación

$$x_1 + x_2 + \cdots + x_k = n$$

tales que $x_1, \ldots x_k, \geq 1$? ¿Y tales que $x_1, \ldots, x_k \geq r$?

24. ¿De cuantas maneras podemos repartir 6 bolas numeradas en 10 cajas? ¿Y si en cada caja podemos poner como máximo una bola? En ambos casos, ¿De cuantas maneras podriamos repartir las bolas si fueran indistinguibles?

25. ¿De cuánta maneras podemos elegir un conjunto ordenado de k enteros no consecutivos entre 1 y n?

26. Cuántas palabras de 14 letras pueden hacer con las letras

AAAABUTTIOPRRS

De todas ellas calcular:

i) Cuántas no tienen dos T consecutivas.

ii) Cuántas tienen todas las vocales juntas.

iii) Cuántas tienen todas las vocales en orden alfabético.

iv) Cuántas tienen todas las vocales juntas y en orden alfabético.

27. Busca el coeficiente de x^2yz^4 en el desarrollo de $(x+y+z)^7$.

28. Una *progresión aritmética de diferencia d* es una sucesión $a_1, a_2, \ldots, a_n, \ldots$ tal que, para cada $n \in \mathbb{N}$, se cumple $a_{n+1} = a_n + d$.

i) Busca el término general de la sucesión.

ii) Queremos demostrar la fórmula

$$\sum_{i=1}^{n} a_i = \frac{(a_1 + a_n)n}{2},$$

para la suma de los n primeros términos de una sucesión artimética. Si llamamos f a la función del lado derecho y g a la función del lado izquierdo, demuestra que ambas funciones cumplen la misma recurrencia y que tienen los mismos valores iniciales.

iii) Calcula la suma de los 1000 primeros números naturales.

29. Una *progresión geométrica de razón r* es una sucesión $a_1, a_2, \ldots, a_n, \ldots$ tal que, para cada $n \in \mathbb{N}$, se cumple $a_{n+1} = ra_n$.

i) Busca el término general de la sucesión.

ii) Utiliza la técnica del problema anterior para demostrar la fórmula de la suma de los términos de una sucesión geométrica

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

iii) Cuenta la leyenda que, cuándo un rey pregunto al inventor del juego de ajedrez qué recompensa quería por su invención, éste pidió el trigo necesario para colocar un grano de trigo en la primera casilla del tablero, dos granos en la segunda, cuatro granos en la tercera, ocho granos en la cuarta, y así, hasta llenar las 64 casillas del tablero. El rey, sorprendido por lo modesto de la petición accedió enseguida. Si 1000 granos de trigo pesan 32 gramos, ¿cuántos kilogramos de trigo se necesitan para pagar al inventor del juego de ajedrez? Si la producción anual de trigo de dicho país es de un millón de toneladas anuales y aumenta un 1,5 % anual, ¿cuánto tiempo tardará el rey en poder pagar al inventor?

30. Consideramos la función recursiva f definida por: $f(1) = 1$, $f(2n) = 4f(n)$ y $f(2n+1) = 4f(n) + 4n + 1$, para todo $n \in \mathbb{N}$.

i) Calcula $f(n)$ para $n = 2, 4, 5, 7$.

ii) Demuestra que $f(n) = n^2$ para todo $n \geq 1$.

31. Comprueba que $a_n = n^2 + 2n + 3$ es solución de la ecuación recurrente

$$a_n + 2a_{n-1} + a_{n-2} = 4n^2 + 10.$$

Busca si hay una solución de la ecuación

$$a_n - 3a_{n-1} - 4a_{n-2} = 6n^2 - 28n + 18$$

de la forma $a_n = An^2 + Bn + C$.

32. Resuelve las recurrencias siguientes:

i) $a_n = 3a_{n-1} + 4a_{n-2}$; $a_0 = a_1 = 1$.

ii) $a_n = a_{n-2}$; $a_0 = a_1 = 1$.

iii) $a_n = 4a_{n-1} - 4a_{n-2}$; $a_0 = a_1 = 2$.

iv) $a_n = 4a_{n-1} - 5a_{n-2}$; $a_0 = 0$, $a_1 = 1$.

v) $a_n - 3a_{n-1} - 4a_{n-2} = 0$; $a_0 = 1$, $a_1 = 1$.

vi) $a_n - 5a_{n-1} + 6a_{n-2} = 0$; $a_0 = 0$, $a_1 = 1$.

vii) $a_n = 2a_{n-1} + 1$; $a_0 = 0$ (Indicación: resta la equación que resulta del cambio $n \to n-1$.)

33. Resuelve las recurrencias siguientes:

i) $a_n - 3a_{n-1} - 4a_{n-2} = 1$; $a_0 = 1, a_1 = 0$.

ii) $a_n + 2a_{n-1} + a_{n-2} = 4n^2 + 10$; $a_0 = a_1 = 1$.

iii) $a_n - 3a_{n-1} - 4a_{n-2} = 6n^2 - 28n + 18$; $a_0 = 0, a_1 = 0$.

iv) $a_n + 2a_{n-1} - 3a_{n-2} = 8n - 14$; $a_0 = 1, a_1 = 2$.

v) $a_n - 4a_{n-1} + 4a_{n-2} = n$; $a_0 = a_1 = 0$

Matemática Discreta

Quatrimestre de Primavera 2014

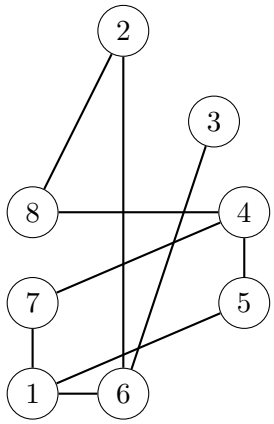
Lista 3 - Grafos

1. Demuestra que hay $2^{\frac{n(n-1)}{2}}$ grafos que tienen n vértices.

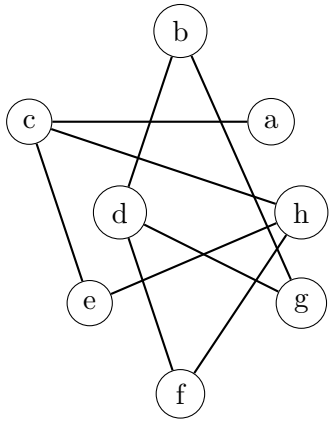
Indicación: Un conjunto con t elementos tiene 2^t subconjuntos.

2. Dados los grafos

G_1



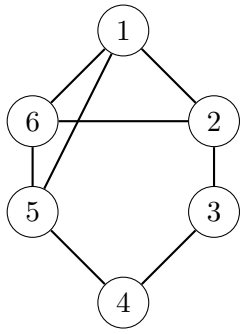
G_2



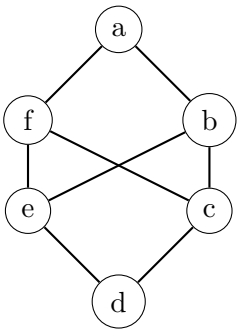
decide si son isomorfos o no. En caso de que lo sean, explicita un isomorfismo entre ellos. En caso que no lo sean, demuestra que no existe ningún isomorfismo.

3. Dados los grafos

G_1



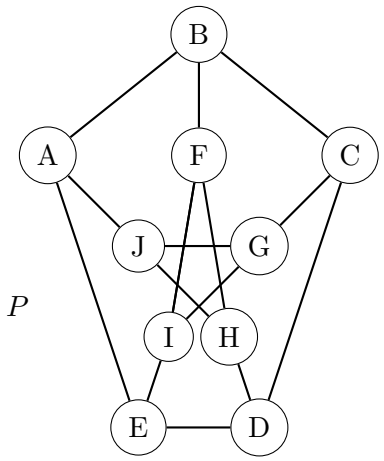
G_2



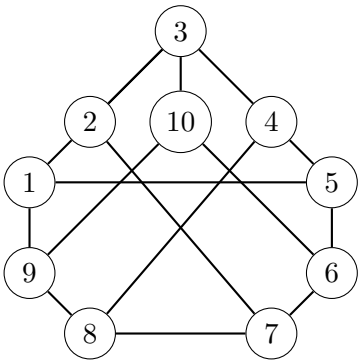
decide si son isomorfos o no. En caso de que lo sean, explicita un isomorfismo entre ellos. En caso que no lo sean, demuestra que no existe ningún isomorfismo.

4. Dos de los grafos P, Q y R són isomorfos.

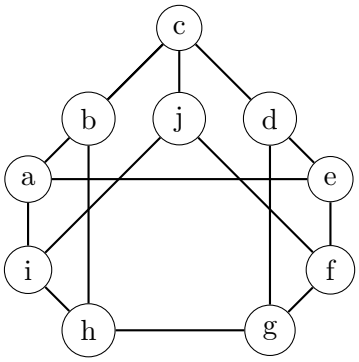
P



Q



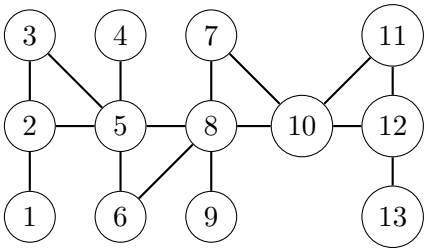
R



Determina el isomorfismo entre los dos grafos isomorfos y demuestra que el otro grafo no es isomorfo a ninguno de los restantes.

5. Demuestra que un grafo es bipartito si y solamente si no tiene ningún ciclo de longitud impar.

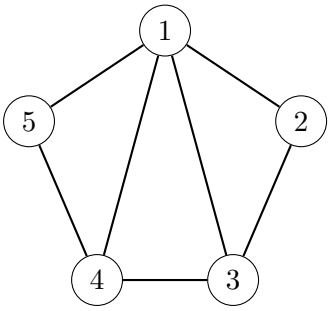
6. Calcula el diámetro, radio, centro y periféria del siguiente grafo:



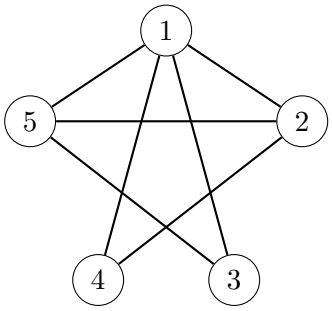
7. Sea A la matriz adyacente del grafo K_4. Sin calcular la matriz directamente, determina A^3.

8. Dados los grafos

G_1



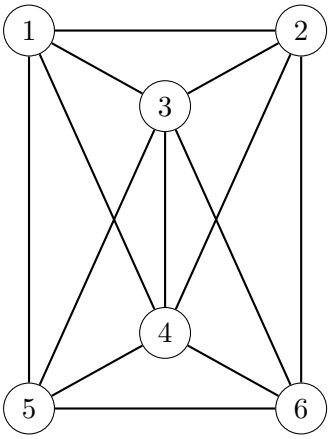
G_2



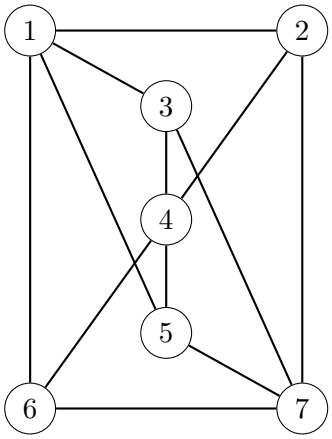
1. ¿Son isomorfos? Explicita un isomorfismo o demuestra que no existe ninguno.
2. ¿Son eulerianos? En caso afirmativo, encuentra un camino euleriano.
3. ¿Son hamiltonianos? En caso afirmativo, encuentra un ciclo hamiltoniano.

9. Dados los grafos

G_1

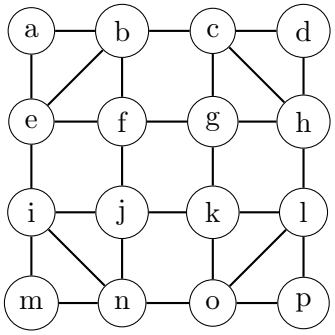


G_2



1. ¿Son isomorfos? Explicita un isomorfismo o demuestra que no existe ninguno.
2. ¿Son eulerianos? En caso afirmativo, encuentra un camino euleriano.
3. ¿Son hamiltonianos? En caso afirmativo, encuentra un ciclo hamiltoniano.

10. Utiliza el algoritmo de Hierholzer para determinar un circuito Euleriano en el siguiente grafo (Indicación: Utiliza $R_1 : a, b, c, g, f, j, i, e, a$ como circuito inicial).



11. Sea G un grafo conexo de orden 24 que es regular de orden 3. Cuantas regiones hay en una representación plana de G ?

12. Sea G un grafo plano de orden menor que 12. Demuestra que $\delta(G) \leq 4$.

13. Determina el número cromático de los grafos bipartidos.

14. Consideramos los siguientes 7 comites:

$$C_1 = \{\text{Alicia, Brian, Carlos}\}$$

$$C_2 = \{\text{Carlos, David, Eva}\}$$

$$C_3 = \{\text{David, Ferran}\}$$

$$C_4 = \{\text{Alicia, Gemma}\}$$

$$C_5 = \{\text{Eva, Helena}\}$$

$$C_6 = \{\text{Eva, Brian, Gemma}\}$$

$$C_7 = \{\text{Helena, Carlos, Ferran}\}$$

Determina el menor tiempo en el que los 7 comites pueden realizar una reunión de una hora.