Introducció a la Criptografia

Grup de Recerca en Criptografia i Grafs

Campus de Igualada
Universitat de Lleida

Index

Divisibilitat

La teoria de la divisibilitat en l'anell d'enters es basa en:

Divisió entera

Si a i b són dos enters on $b \neq 0$, aleshores existeixen dos únics enters q i r (**quocient** i **residu**) tals que

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

- **Divisors i múltiples**. Diem que b és un *divisor* de a, i escrivim $b \mid a$, si existeix un enter c tal que $a = b \cdot c$. També es diu que
  - a és un *múltiple* de b, i escrivim $a = \dot{b}$
  - a és *divisible* per b.

Màxim comú divisor

Donats dos enters a i b, es diu que $d \in \mathbb{Z}$ és el **màxim comú divisor** de a i b,
i ho denotem

$$d = \gcd(a, b)$$

si d satisfà:

1) $d \mid a$ i $d \mid b$ (d és divisor de a i b).
2) Si $d' \mid a$ i $d' \mid b$ aleshores $d' \leq d$ (d ès el més gran dels divisors).

Maneres de calcular-lo

- Factoritzant a i b
- Usant algoritme d'Euclides

Propietats del màxim comú divisor

- **Aditiva**. Si $a \neq b$, aleshores

$$\begin{aligned} \gcd(a,b) &= \gcd(a, b-a) \quad \text{si } a < b \\ \gcd(a,b) &= \gcd(a-b, b) \quad \text{si } b < a \end{aligned}$$

- **Multiplicativa**. Si $b \neq 0$, aleshores

$$\gcd(a,b) = \gcd(b,r),$$

on r és el residu de la divisió de a per b.

Algoritme d'Euclides

Donats dos enters a i b, repetim la divisió fins que el residu sigui zero:

$$\left.\begin{array}{rcll} a & = & b \cdot q_1 + r_1, & r_1 < |b| \\ b & = & r_1 \cdot q_2 + r_2, & r_2 < r_1 \\ \vdots & & \vdots & \\ r_{n-2} & = & r_{n-1} \cdot q_n + r_n, & r_n < r_{n-1} \\ r_{n-1} & = & r_n \cdot q_{n+1} + r_{n+1}, & r_{n+1} = 0 \end{array}\right\} \Rightarrow \gcd(a,b) = r_n.$$

Podem usar una taula per seguir l'algoritme:

	q_1	q_2	q_3	$\dots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\dots$	r_{n-2}	r_{n-1}	r_n
r_1	r_2	r_3	r_4	$\dots$	r_n	0	

$\Rightarrow \quad \gcd(a,b) = r_n.$

Identitat de Bezout

Identitat de Bezout

Si $d = \gcd(a, b)$ aleshores existeixen enters r i s tals que

$$d = a \cdot r + b \cdot s,$$

és a dir, d es pot expressar com una *combinació lineal* de a i b.

Aquests enters r i s es poden determinar pel anomenat **algoritme d'Euclides estés**.

Nombres primers

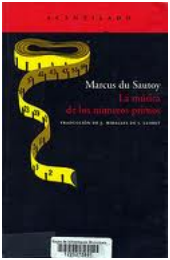
- Juguen el paper dels *àtoms* de la Química

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \ldots$$

- Euclides va provar que hi ha **infinits primers**
- En el film **Contact**, dirigit al 1997 per R. Zemeckis, l'astrònoma Ellie Arroway (Jodie Foster) aconsegueix captar senyals intel.ligents de l'univers

A la cerca de primers

- Quina regla hi ha per trobar el **següent primer?**
  $\ldots 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, \ldots$
- El seu comportament és un misteri
  - Hi ha primers consecutius que la seva diferència és 2: primers bessons
  - Entre 10000000 i 10000100 només hi ha 2 primers: 10000019 and 10000079



És fàcil trobar primers grans?

Avui en dia, per garantir la confidencialitat de la informació que circula per internet, s'utilitzen mètodes per **xifrar** la informació que necessiten primers grans.

Tests de primalitat

- Hi ha algoritmes (**test de primalitat**) per determinar si un nombre és primer
- Usant ordinadors amb gran capacitat de còmput es troben primers:
    - $2^{20.996.011} - 1$ (més de 6 milions de xifres), trobat per una xarxa distribuida, 2005
    - $2^{30.402.457} - 1$ (més de 9 milions de xifres), trobat per C. Cooper i S. Boone, 2006
    - $2^{43.112.609} - 1$ (més de 12 milions de xifres), trobat per una xarxa distribuida, 2008

L'anell d'enters mòdul m

- Donat un enter $m \neq 0$, es diu que un enter a és **congruent** a un enter b mòdul m si $a - b$ és un múltiple de m. Ho denotem

$$a \equiv b \pmod{m}.$$

- El conjunt de les **classes de residus** de $\mathbb{Z}$ mòdul m és

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}, \text{ on } \overline{a} = \{a + k \cdot m \mid k \in \mathbb{Z}\}.$$

- A $\mathbb{Z}_m$ hi ha definides dos **operacions internes**:

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{and} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Càlcul d'inversos a $(\mathbb{Z}_m, +, \cdot)$

Invertibles de $(\mathbb{Z}_m, +, \cdot)$

- Si $a \in \mathbb{Z}$ és un múltiple de m aleshores $\overline{a} = \overline{0} \in \mathbb{Z}_m$.
- Si $a \in \mathbb{Z}$ és un enter tal que $\gcd(a, m) = 1$ aleshores $\overline{a}$ és un **element invertible** de $\mathbb{Z}_m$.
- Si $a \in \mathbb{Z}$ és un enter tal que $\gcd(a, m) \neq 1$ aleshores $\overline{a}$ és un **divisor de zero** de $\mathbb{Z}_m$.

Càlcul de l'invers: Per la identitat de Bezout

$$1 = a \cdot r + m \cdot s$$

obtenim $a^{-1} = r$ a $\mathbb{Z}_m$.

Funció phi d'Euler

$$\phi(n) = \mathrm{Card}\,\{m \in \mathbb{Z}^+ \mid 1 \leq m \leq n \text{ and } \gcd(m,n) = 1\}$$

Propietats de la funció ϕ d'Euler

1. Si p és primer, $\phi(p) = p - 1$
2. Si p és primer i $\alpha \in \mathbb{Z}^+$, aleshores $\phi(p^\alpha) = p^{\alpha-1} \cdot (p-1)$
3. Si m i n són coprimers, aleshores $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$
   Si $n = p \cdot q$, p, q primers, aleshores $\phi(n) = (p-1)(q-1)$
4. Si $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_r^{\alpha_r}$ és la factorització de n, aleshores

$$\phi(n) = p_1^{\alpha_1 - 1} \cdot (p_1 - 1) \cdot p_2^{\alpha_2 - 1} \cdot (p_2 - 1) \dots p_r^{\alpha_r - 1} \cdot (p_r - 1)$$

Exponenciació modular

- **Teorema petit de Fermat.** Si $p \in \mathbb{Z}^+$ és un primer i a és un enter no divisible per p, aleshores
$$a^{p-1} \equiv 1 \pmod{p}$$

- **Teorema d'Euler.** Si $n \in \mathbb{Z}^+$ i a és coprimer amb n, aleshores
$$a^{\phi(n)} \equiv 1 \pmod{n}$$

P. de Fermat (1601-1665) i L. Euler (1707-1783)

Algoritme per calcular exponenciacions modulars

a^n mòdul m: **algoritme square–and–multiply**

1) Expressar l'exponent n en base 2:

$$(b_k b_{k-1} \dots b_1 b_0)_2$$

2) Substituir:

   cada 0 per la lletra S
   cada 1 pel parell de lletres SX

   Eliminar el parell SX corresponent a $b_k = 1$

3) Aplicar a l'enter a les regles de càlcul determinades per la seqüència de S's i X's:

   S : elevar al quadrat i reduir mòdul m
   X : multiplicar per a i reduir mòdul m

Exemple

Càlcul de 3^{2026} mòdul 100

Tenim $\phi(100) = 40$ i $2026 = 40 \cdot 50 + 26$. Pel Teorema d'Euler

$$3^{2026} \equiv 3^{26} \pmod{100}$$

Per a calcular $3^{26} \pmod{100}$ seguim l'algoritme:

- $26 = (11010)_2$.
- $11010 \longrightarrow SXSXSSXS \longrightarrow SXSSXS$
- $$3 \xrightarrow{S} 3^2 \xrightarrow{X} 3^3 \xrightarrow{S} 3^6 \xrightarrow{S} 3^{12} \xrightarrow{X} 3^{13} \xrightarrow{S} 3^{26}$$

Exemple (2)

Amb els càlculs i reduccions mòdul 100, obtenim

$$
\begin{array}{ccccccc}
 & S & & X & & S & \\
3 & \rightarrow & 3^2 = 9 & \rightarrow & 3 \cdot 9 = 27 & \rightarrow & 27^2 \equiv 29 \\
 & S & & X & & S & \\
 & \rightarrow & 29^2 \equiv 41 & \rightarrow & 3 \cdot 41 \equiv 23 & \rightarrow & 23^2 \equiv 29
\end{array}
$$

Per tant,

$$3^{26} \equiv 29 \pmod{100}$$

i, consequentment,

$$3^{2026} \equiv 29 \pmod{100}$$

Criptografia

- Des de l'antiguetat s'han xifrat missatges per aconseguir que fossin **secrets**
- Juli Cèsar enviava missatges als seus generals usant un codi per xifrar
- A principis del segle XX, amb la invenció de màquines electromecàniques, com la **màquina Enigma**, apareixen sistemes més complexos

- Fins als anys 70, la criptografia estava limitada a cercles militars i diplomàtics, però avui, amb Internet, són molts els escenaris on hi és present

Objectius de la criptografia

La criptografia és la ciència de l'escriptura secreta.
Els seus principals objectius són:

- Preservar la confidencialitat (secret) de la informació transmesa entre dos parts (emisor i receptor);
- Detectar si la informació ha estat modificada per una tercera part no autoritzada (integritat);
- Confirmar la identitat de l'emisor (autenticació).

Criptosistemes

- Un criptosistema és un algoritme que transforma un missatge intel.ligible (plaintext) en un de no intel.ligible (ciphertext) i viceversa.
- Els processos de xifrat i dexifrat estàn controlats per un o més paràmetres (claus).

Model matemàtic

Un criptosistema està format per tres conjunts finits:

- Conjunt de missatges en clar M,
- Conjunt de missatges xifrats C i
- l'espai de claus K i dos families de funcions, de xifrat $\{E_k\}_{k\in K}$ i de desxifrat $\{D_k\}_{k\in K}$, tals que $\forall k \in K$

$$\begin{aligned} E_k : M &\longrightarrow C \\ D_k : C &\longrightarrow M \end{aligned}$$

$$D_k(E_k(m)) = m, \quad \forall m \in M.$$

Criptosistema de Cèsar

Aquest xifrat substitueix cada lletra de l'alfabet per la lletra que es troba deplaçada tres (k) posicions a la dreta:

plain	a	b	c	d	e	...	v	w	x	y	z
cipher	d	e	f	g	h	...	y	z	a	b	c

Funció de xifrat:

$$\begin{array}{rcl} E_k : \mathbb{Z}_{26} & \longrightarrow & \mathbb{Z}_{26} \\ m & \longrightarrow & m+k \end{array}$$

Funció de desxifrat :

$$\begin{array}{rcl} D_k : \mathbb{Z}_{26} & \longrightarrow & \mathbb{Z}_{26} \\ c & \longrightarrow & c-k \end{array}$$

Criptoanàlisi: atac per força bruta.

Rivest, Shamir, Adleman (1977)

- Rivest, Shamir and Adleman van crear al 1977 un criptosistema de clau pública
  - Les operacions de xifrat i desxifrat es calculen mòdul $n = p \cdot q$, producte de dos **primers grans**
  - La seguretat es basa en el **problema de la factorització d'enters**

- El nostre DNI porta un chip RSA amb claus de 2048 bits
- La majoria de transaccions online usen RSA per iniciar la clau de sessió

El criptosistema RSA

- **Setup del criptosistema**

  Generar dos primers grans p i q
  Calcular $n = p \cdot q$
  La *i*nformació trampa és $\phi(n) = (p-1)(q-1)$
- **Clau pública**

  Un enter e tal que $\gcd(e, \phi(n)) = 1$.
- **Clau privada**

  L'enter d tal que $e \cdot d \equiv 1 \pmod{\phi(n)}$

Encriptació RSA

Algoritme (Encriptació RSA)

INPUT: El paràmetre n, la clau pública e i el missatge en clar m

OUTPUT: El missatge xifrat c

- Representar el missatge m com un enter $\pmod{n}$
- Calcular $c = m^e \pmod{n}$
- Retornar c

Desencriptació RSA

Algoritme (Desencriptació RSA)

INPUT: El paràmetre n, la clau privada d i el missatge xifrat c

OUTPUT: El missatge en clar m

- Calcular $m = c^d \pmod{n}$
- Retornar m

En efecte, usant el Teorema d'Euler:

$$c^d \equiv (m^e)^d \equiv m^{1+r\cdot\Phi(n)} \equiv m \cdot \left(m^{\Phi(n)}\right)^r \equiv m \pmod{n}.$$

Seguretat del RSA

- La seva seguretat es basa en la intractabilitat del **problema de la factorització d'enters**
- El tamany recomanat de n és, d'almenys, 2048 bits.
- Per garantir la seguretat long–term, es recomana usar n de 3072 bits.

Requeriments primers RSA

Es recomana prendre p i q tals que:

- p i q amb **mateixa bitlength**, però tals que $p - q$ no sigui massa petit
- $p - 1$ i $q - 1$ no haurien de ser **smooth**
- $\gcd(p - 1, q - 1)$ petit

Una possibilitat: $p = 2p' + 1$ i $q = 2q' + 1$, amb p' i q' primers (p i q s'anomenen **primers segurs**)

Reptes RSA

Reptes RSA Laboratories

Challenge	Prize	Satatus	Date
RSA-576	$ 10,000	Factored	2003
RSA-640	$ 20,000	Factored	2005
RSA-768	$ 50,000	Factored	2009
RSA-896	$ 75,000	Not Factored	
RSA-1024	$ 100,000	Not Factored	
RSA-1536	$ 150,000	Not Factored	
RSA-2048	$ 200,000	Not Factored	

Alguns reptes RSA

- **RSA-576**

  Decimal Digits: 174 Digit Sum: 785

  1881988129206079638386972394616504398071635633794173827007633564229888597152346654853190606065047430453173880113033967161996923212057340318795506569962213051687593076502570 59

- **RSA-1024**

  Decimal Digits: 309 Decimal Digit Sum: 1369

  135066410865995223349603216278805969938881475605667027524485143851526510604859533833940287150571909441798207282164471551373680419703964191743046496589274256239341020864383202110372958725762358509643110564073501508187510676594629205563685529475213500852879416377328533906109750544334999811150056977236890927563