1.3. LA FUNCIÓ D'EULER. POTÈNCIES i CONGRUÈNCIES

Inicialment, la funció d'Euler ens permet contestar a la següent pregunta:

- Donat $n \in \mathbb{N}$, quants enters positius menors o iguals a n són coprimers amb n?

En altres paraules, quants enters positius x menors que n verifiquen $\text{mcd}(x,n)=1$?

La resposta ens la dóna la funció d'Euler.

DEFINICIÓ:

La funció d'Euler és la funció

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}$$
$$n \longrightarrow \varphi(n) := \#\{x \mid 0 \le x \le n \text{ t.q. } \text{mcd}(x,n)=1\}$$
$$= \#\{\text{invertibles a } \mathbb{Z}/(n)\}.$$

EXEMPLE:

(a) $\varphi(4) = 2$ (els invertibles a $\mathbb{Z}/(n)$ són $\bar{1}$ i $\bar{3}$)

(b) Si p és primer $\varphi(p) = p-1$ perquè totes les classes llevat del $\bar{0}$ són invertibles a $\mathbb{Z}/p$.

L.

Si n és gran, necessitem propietats que ens permetin calcular $\varphi(n)$.

PROPOSICIÓ:

(a) Si $\text{mcd}(x,y)=1$, aleshores $\varphi(x\cdot y) = \varphi(x)\cdot\varphi(y)$

(b) Si p és primer, $\varphi(p^k) = p^{k-1}\cdot(p-1) = p^k - p^{k-1}$.

(c) Si $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ és la factorització de n en nombres primers, aleshores

$$\varphi(n) = p_1^{a_1-1}\cdot(p_1-1)\cdot p_2^{a_2-1}\cdot(p_2-1)\cdot\cdots\cdot p_k^{a_k-1}\cdot(p_k-1).$$

En altres paraules,

$$\varphi(n) = \prod_{i=1}^{k} \left(p_i^{a_i} - p_i^{a_i-1}\right)$$

OBS:

Fixeu-vos que si sabem la factorització de n en primers, calcular $\varphi(n)$ és fàcil però ja hem dit que conèixer la factorització de n en primers si $n \gg 0$ és MOLT DIFÍCIL. Veurem que en aquesta dificultat es basa l'èxit del RSA per codificar informació. En relació a això (a la codificació RSA) el següent resultat és molt important.

TEOREMA (DE EULER)

Suposem que $\text{mcd}(y, m) = 1$ ($\bar{y}$ és invertible a $\mathbb{Z}/m$). Aleshores,

$$y^{\varphi(m)} \equiv 1 \text{ a } \mathbb{Z}/(m)$$

└.

COROLARI (Petit Teorema de Fermat)

(a) Si $p \nmid y$, p primer, aleshores

$$y^{p-1} \equiv 1 \text{ a } \mathbb{Z}/(p).$$

(b) Si $\text{mcd}(y, m) = 1$ i $a \equiv x \bmod (\varphi(u))$ aleshores,

$$y^a \equiv y^x \text{ a } \mathbb{Z}/(u)$$

└

DEMO: (a) és una aplicació directa del Teorema de Euler.

(b) si $a \equiv x \bmod \varphi(u) \Rightarrow a - x = k \cdot \varphi(u)$ per cert $k \in \mathbb{Z}_{>0}$. $\Rightarrow a = k \cdot \varphi(u) + x$

$$\Rightarrow y^a = y^{k\cdot\varphi(u)+x} = y^{k\cdot\varphi(u)} \cdot y^x \equiv \left(y^{\varphi(u)}\right)^k \cdot y^x \equiv 1 \cdot y^x$$

(Teo Euler)

$$\Rightarrow y^a \equiv y^x \text{ a } \mathbb{Z}/(u)$$

└

Aquest corolari ens dóna una forma molt útil per calcular potències grans a $\mathbb{Z}/(u)$ si estem en les hipòtesi del Teorema.

EXEMPLE:

Volem calcular 5^{4371} a $\mathbb{Z}/144$

Com a $\text{mcd}(5, 144) = 1$, simplificarem la potència calculant $\varphi(144)$

$144 = 2^4 \cdot 3^2 \Rightarrow \varphi(144) = (2^4 - 2^3)(3^2 - 3) = 48$

Calculem ara $\overline{4371}$ a $\mathbb{Z}/48$. Observem que $4371 = 48 \cdot 91 + 3$ per tant

$$4371 \equiv 3 \text{ a } \mathbb{Z}/48.$$

Per tant

$$5^{4371} \equiv 5^3 \text{ a } \mathbb{Z}/144$$
$$\equiv 125$$

■

1.4. INTRODUCCIÓ A LA CRIPTOGRAFIA.

La paraula CRIPTOGRAFIA prové de la unió de dues paraules gregues:

κρυπτω kripto (ocult) : γραφως graphos (escriure)

i la seva definició és escriptura oculta.

- Els orígens de la criptografia es remunten al principi de la història. Desde "sempre" les persones han utilitzat diverses mètodes amb l'objectiu de que un missatge no arribés a mans d'una persona no autoritzada a llegir-lo.
- El primer mètode de criptografia conegut és del segle V a.C : tenia el nom de "ESCÍTALA", un sistema utilitzat pels espartans per enviar missatges secrets.
- L'objectiu clàssic de la criptografia és l'intercanvi de missatges a través d'un canal segur. Tradicionalment aquest objectiu s'assolia posant-se d'acord, a priori, emisor i receptor en una certa informació secreta : LA CLAU. (clau que permet xifrar i desxifrar els missatges).
- Els sistemes clàssics, anomenats de CLAU PRIVADA, són actualment insuficients o inadequats per les noves necessitats. Per això van aparèixer els sistemes criptogràfics de CLAU PÚBLICA. Aquest són els que necessiten d'un substrat matemàtic més potent i són els més estudiats.
- Els criptosistemes de clau pública estan basats en la Teoria de la Complexitat Computacional i es cuiden de que desxifrar un missatge secret resulti impossible a la pràctica, a menys de tenir certa informació suplementària que només té el receptor legal.
- La criptografia avui en dia cobreix :
  - Protocols d'autenticació
  - Protocols per compartir secrets.
  - Transaccions electròniques segures
  - Eleccions electròniques
  - etc.....

DEFINICIÓ:

Un CRIPTOSISTEMA és una terna $(\mathcal{M}, \mathcal{C}, \mathcal{K})$ on:

$\mathcal{M}$ = Conjunt de missatges originals

$\mathcal{C}$ = Conjunt de missatges xifrats

$\mathcal{K}$ = Conjunt finit de claus

juntament amb dues funcions

$$c: \mathcal{M} \times \mathcal{K} \longrightarrow \mathcal{C} \qquad \text{(xifrat)}$$

$$d: \mathcal{C} \times \mathcal{K} \longrightarrow \mathcal{M} \qquad \text{(desxifrat)}$$

tals que $d(c(M,k)) = M$ per a tot $(M,k) \in \mathcal{M} \times \mathcal{K}$.

Un element M de $\mathcal{M}$ s'anomena missatge i és una successió finita de sígues o lletres d'un cert alfabet $\mathcal{A}$. El resultat d'aplicar a M la funció c de xifrat dóna lloc a un missatge xifrat C, que és una col·lecció de sígues d'un alfabet B. La funció c depèn d'una clau $k \in \mathcal{K}$. El missatge original M es recupera a partir de C mitjançant d.

A continuació veurem un exemple de criptosistema de clau privada (El xifrat Afí) i un exemple de criptosistema de clau Pública (RSA)

EL XIFRAT AFÍ

Considerem l'alfabet llatí de 26 caràcters

$$\underset{0}{A}, \underset{1}{B}, \underset{2}{C}, \ldots \ldots \underset{25}{Z} \qquad (*)$$

Enumerem cadascun dels caràcters del 0 al 25.

Per fer el xifrat determinem enters a i b amb $\text{mcd}(a, 26) = 1$.

El mètode consisteix en substituir del missatge M, cada lletra pel seu valor numèric x (segons (*)) i canviar x per y on

$$y \equiv ax + b \quad a \ \mathbb{Z}_{/26}$$

i finalment canviar y per la lletra que li correspon segons (*).

Com $\text{mcd}(a,26) = 1$, podem desxifrar (canviar x a partir de y) donat que

$$x \equiv a^{-1} \cdot (y - b) \quad a \ \mathbb{Z}_{/26}$$

EXEMPLE

Fixem $a = 15$; $b = 22$ i volem xifrar la paraula HOLA.

H O L A
↓ ↓ ↓ ↳ 0
7 14 11

$H \rightsquigarrow 7$: $y \equiv 15 \cdot 7 + 22 \equiv 23$ a $\mathbb{Z}/(26)$ pq $15 \cdot 7 + 22 = 127 \equiv 23 \mod 26$ → X

$O \rightsquigarrow 14$: $y \equiv 15 \cdot 14 + 22 \equiv 232 \equiv 24$ a $\mathbb{Z}/26$ → Y

$L \rightsquigarrow 11$ $y \equiv 15 \cdot 11 + 22 \equiv 187 \equiv 5$ a $\mathbb{Z}/26$ → F

$A \rightsquigarrow 0$ $y \equiv 15 \cdot 0 + 22 \equiv 22$ a $\mathbb{Z}/26$. → W.

Per tant HOLA es xifra com XYFW

Per $a = 15$, $b = 22$ per desxifrar necessitem invertir 15 a $\mathbb{Z}/26$

$26 = 1 \cdot 15 + 11$
$15 = 1 \cdot 11 + 4$
$11 = 2 \cdot 4 + 3$
$4 = 1 \cdot 3 + 1$
$3 = 3 \cdot 1$

→ $1 = 4 - 1 \cdot 3 = 4 - 1 \cdot (11 - 2 \cdot 4) = 3 \cdot 4 - 1 \cdot 11 = 3(15 - 11) - 1 \cdot 11$
$= 3 \cdot 15 - 4 \cdot 11 = 3 \cdot 15 - 4(26 - 1 \cdot 15) = 7 \cdot 15 - 4 \cdot 26$

$\Rightarrow \overline{15}^{-1} = \overline{7}$ a $\mathbb{Z}/26$.

$\Rightarrow x = 7(y - 22)$

Si volem desxifrar VMFW ja sabem que F → L i W → A. Si calculem el resta podem comprovar que

$V = 21 \rightsquigarrow 19$ (= T) ja que $7(21 - 22) = -7 \equiv 19 \mod 26$.

: que VMFW → TILA.

Un cas molt conegut del xifrat afí és el xifrat de CESAR, en el que prenem $a = 1$. En aquest cas de fet el que fem és desplaçar les lletres.

EL XIFRAT RSA

Em 1977 Ronald Rivest, Adi Shamir i Leonard Adleman, 3 estudiants a al MIT van crear el anomenat sistema RSA. Aquest criptosistema de clau pública és el més famós i més utilitzat avui en dia, sobretot en internet.

Els tres joves, l'any 1982 van fundar una companyia RSA Data Security que el 2006 va ser comprada per 2100 milions de dòlars.

- El sistema RSA es basa en la dificultat de factoritzar nombres grans en producte de primers. En altres paraules en la impossibilitat de calcular $\varphi(n)$ per $n \gg 0$.

- Els passos del RSA són els següents:

1. Alice escull 2 nombres primers p i q. Anomenem $n = p \cdot q$ i tenim

$$\varphi(n) = (p-1)\cdot(q-1)$$

2. Alice escull $e \in \mathbb{N}$, $1 < e < \varphi(n)$ tal que $\text{mcd}(e, n) = 1$.

Després calcula $d \in \mathbb{N}$ tal que

$$d \equiv e^{-1} \mod \varphi(n)$$

3. Alice envia a Bob els nombres n i e (e s'anomena l'exponent de la clau pública) però manté en secret d (exponent de la clau privada)

4. Bob transforma un missatge M en un enter m $\quad 0 \leq m < n$

Aleshores calcula $C = m^e \mod n$ i envia c a Alice.

5. Alice calcula m amb la fórmula

$$m = c^d \mod (n).$$

OBS: En efecte això és correcte.

Si $\text{mcd}(m, n) = 1$, aleshores

$$c^d = (m^e)^d = m^{ed} \overset{d \equiv e^{-1} \mod \varphi(n) \Rightarrow ed = 1 + \alpha\varphi(n)}{=} m^{1+\alpha\varphi(n)} = m \cdot (m^{\varphi(n)})^{\alpha} \overset{\text{Teo Euler}}{=} m \cdot 1 = m \mod (n)$$

Si $\text{mcd}(m, n) \neq 1$ com $n = p \cdot q \Rightarrow \text{mcd}(m, n) = p$ o $\text{mcd}(m, n) = q$.

Els dos casos s'estudien aprox com els anteriors.

Fets clau:
- Alice fa pública la seva clau (n i e)
- Tothom que vol enviar un missatge a alice o pot fer convertir n i e
- Ningú pot desxifrar el missatge, llevat Alice pq es necessita d i per calcular d cal saber $\varphi(n)$ i només coneixent n és "impossible".

COMENTARIS: - Hi ha una base de dades pública de Claus públiques.

- Per factoritzar un nº de 768 dígits es van utilitzar 80 processadors per seleccionar certs polinomis necessaris per fer la factorització. Van trigar mig any en trobar els polinomis.
. Per la factorització es van utilitzar varis cents d'ordenadors i la factorització va trigar quasi 2 anys addicionals als 1/2 any que portàvem. S'estima que si es fes servir un ordenador a 2.2 GHz amb 2 GB de RAM caldrien 1500 anys per la factorització.

- Elecció de p i q:

Tenim el que s'anomena el Test de primalitat que és un algorisme polinòmic.
És un test probabilístic que no demostra en sentit matemàtic que un nombre és primer, però ho garantitza amb una probabilitat més gran que volguem.
Per escollir p i q escollim 2 nombres grans a i b imparells i els passem al test probabilístic. Si ho són s'agafen. Si a no és primer es substitueix per a+2, a+4, etc... fins obtenir els primers (donada el pt de vista probabilístic).

- FUTUR:

- Si existeixen computadors quàntics es petaria el RSA donat que aquests estan preparats per factoritzar nombres ~~grans~~ en primers, en temps "real".
Això destruiria tots els sistemes d'encriptació que es basen en la impossibilitat de factoritzar.
- Actualment hi ha projectes de recerca engegats investigant criptosistemes no destructibles amb computació quàntica. S'hi està invertint molt donat que és la majoria de processos es basen en RSA.