# Matemàtica Aplicada

Curs 22-23

# Índex



# 1 Codis i Criptografia

## 1.1 L'algorisme d'Euclides

Curiosament, els mètodes de xifratge actuals requereixen, per tal de desxifrar, tècniques basada en un algorisme que té més de 2300 anys, l'algorisme d'Euclides. Com veurem, aquest algorisme, llegit al revés, permet trobar l'invers multiplicatiu d'un nombre mòdul $p$.

L'algorisme d'Euclides permet trobar el màxim comú divisor sense factoritzar els nombres. Donats dos nombres enters, $a$ i $b$, el màxim comú divisor, que denotarem per $(a, b)$, és el nombre enter més "gran" (màxim) que divideix tant $a$ com $b$. L'algorimse consisteix en anar provant "candidats" a ser el màxim comú divisor de més gran a més petit, i comença preguntant-se, quin és el nombre més gran possible que divideixi tant $a$ com $b$? Doncs la resposta és, òbviament, el més petit de tots dos. Suposem que $b < a$, aleshores no hi pot haver com nombre enter més gran que $b$ que divideixi $b$ ($a$ potser sí). Per tant, el primer candidat a ser el màxim comú divisor de $a$ i $b$ és el més petit dels dos, $b$.

Per comprovar si $b = (a, b)$ només caldrà veure si el residu resultant de dividir $a$ entre $b$ és 0 o no. Dividim doncs $a$ entre $b$ i obtenim un quocient $q$ i un residu $r$, i per tant podem escriure:

$$a = b \cdot q + r \tag{1}$$

Si $r = 0$ aleshores $b = (a, b)$. En canvi, si $r \neq 0$ aleshores caldrà trobar un nou candidat més petit que $b$.
El nou candidat ve de fer la següent reflexió: si el nombre que busquem ha de dividir tant $a$ com $b$, aleshores aquest nombre també haurà de dividir $r$. Això ve de fer el següent raonament: suposem que $n|a$ i $n|b$ (és a dir, $n$ divideix $a$ i $b$), aleshores

$$\frac{a}{n} \text{ i } \frac{b}{n} \text{ són nombres enters i les fraccions se simplifiquen}$$

D'altra banda, fent servir l'expressió (1), tindrem que

$$\underbrace{\frac{a}{n}}_{\text{nombre enter}} = \frac{b \cdot q + r}{n} = \underbrace{\frac{b}{n}}_{\text{nombre enter}} + \frac{r}{n}$$

Podem concloure que $n$ també haurà de dividir $r$ per tal que el resultat de fer $\frac{b}{n} + \frac{r}{n}$ sigui un nombre enter.
Com estem buscant el nombre més gran possible que divideixi $b$ i $r$, i $r$ és el més petit perquè és el residu, provem amb el propi $r$. Com $r$ es divideix a si mateix, només caldrà provar si $r$ divideix $b$. Fent la divisió obtenim un nou quocient i un nou residu:

$$b = r \cdot q_2 + r_2 \tag{2}$$

Ara, si $r_2 = 0$ aleshores ja estem, $r$ serà l'enter més gran que es divideix a si mateix i a $b$, i per tant també divideix $a$ i serà el màxim comú divisor de $a$ i $b$. Ara bé, si $r_2 \neq 0$ aleshores haurem de trobar un nou candidat més petit que $r$.
Recordem que buscàvem el nombre més gran que dividís tant $b$ com $r$ (automàticament dividirà $a$ per la igualtat (1)). Repetint el mateix argument que abans amb l'equació (2), si el nou candidat ha de dividir $b$ i $r$ també haurà de dividir $r_2$. Busquem doncs el nombre més gran possible que divideixi $r$ i $r_2$: automàticament dividirà $b$ i també dividirà $a$. Com $r_2 < r$ (perquè és el darrer residu), el més gran possible serà el propi $r_2$. Mirem doncs si $r_2$ divideix $r$ obtenint un nou quocient i un nou residu:

$$r = r_2 \cdot q_3 + r_3$$

Ara, si $r_3 = 0$ ja hem acabat, perquè $r_2$ serà l'enter més gran que es divideix a si mateix i a $r$, per l'equació (2) també dividirà $b$ i per l'equació (1) també dividirà $a$ i,

per tant, $r_2$ serà el màxim comú divisor de $a$ i $b$. Ara bé, si $r_3 \neq 0$ aleshores haurem de trobar un nou candidat més petit que $r_2$. L'argument es torna a repetir obtenint un nou residu resultat d'intentar $r_2$ entre $r_3$:

$$r_2 = r_3 \cdot q_4 + r_4$$

S'entra així en un procés iteratiu fins que finalment es troba un residu 0 resultant de dividir el residu $r_n$ entre el residu $r_{n+1}$:

$$r_{n-1} = r_n \cdot q_{n+1} + 0$$

En aquest moment haurem trobat el nombre més gran, $r_n$, que divideix $r_{n-1}$ i $r_{n-2}$. Anant enrere desfent l'argument, aquest nombre $r_n$ també dividirà $r$ i $b$, i finalment dividirà $b$ i $a$. De manera esquemàtica tenim:

$$\begin{array}{lll}
r_{n-1} = r_n \cdot q_{n+1} + 0 & \Longrightarrow & r_n | r_{n-1} \\
r_{n-2} = r_{n-1} \cdot q_n + r_n & \Longrightarrow & r_n | r_{n-2} \\
r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1} & \Longrightarrow & r_n | r_{n-3} \\
 & \vdots & \\
r_2 = r_3 \cdot q_4 + r_4 & \Longrightarrow & r_n | r_2 \\
r = r_2 \cdot q_3 + r_2 \Longrightarrow & r_n | r & \\
b = r \cdot q_2 + r_2 & \Longrightarrow & r_n | b \\
a = b \cdot q + r & \Longrightarrow & r_n | a
\end{array}$$

Per tant, si $r_n$ és el primer residu en ser 0, aleshores $r_n = (a, b)$.

**Observació 1.** *Fixem-nos que a cada divisió el residu disminueix en almenys una unitat i en algun moment serà 0. Per tant, l'algorisme convergeix i sempre es troba una solució.*

Vegem un exemple.

**Exemple 1.** *Trobem* $(210, 45)$. *Com* $45 < 210$ $45$ *serà el primer candidat més gran a dividir-los tots dos. Provem:*

$$\begin{array}{lll}
210 = 4 \cdot 45 + 30 & \Longrightarrow & 45 \not| 210 \\
45 = 1 \cdot 30 + 15 & \Longrightarrow & 30 \not| 45 \\
30 = 2 \cdot 15 + 0 & \Longrightarrow & 15 | 30
\end{array}$$

*Com 15 divideix 30, també dividrà 45 i per tant també dividirà 210. Així,* $15 = (210, 45)$.

## 1.2 L'algorisme d'Euclides estès

Com veurem, l'algorisme d'Euclides permet calcular l'invers d'un nombre a $\mathbb{Z}_p$, la qual cosa és clau a l'hora de desencriptar en els mètodes moderns. Això ve de la següent resultat:

**Proposició 1.** *Si $a$ i $b$ són dos enters i $d$ és el seu màxim comú divisor, aleshores existeixen dos enters $n$ i $m$ de manera que $d$ es pot escriure com*

$$d = n \cdot a + m \cdot b$$

L'algorisme d'Euclides permet calcular $n$ i $m$ simplement aïllant el residu a cada divisió i fent substitució del residu anterior:

$$210 = 4 \cdot 45 + 30 \Longrightarrow 30 = 210 - 4 \cdot 45$$
$$45 = 1 \cdot 30 + 15 \Longrightarrow 15 = 45 - 1 \cdot 30 = 45 - 210 + 4 \cdot 45 = 3 \cdot 45 - 210$$

Per tant, obtenim

$$15 = 3 \cdot 45 + (-1) \cdot 210$$

## 1.3 Invers mòdul $p$

Suposem ara que tenim dos nombres enters, $a$ i $p$, que són coprimers; és a dir, que el seu màxim comú divisor és 1 perquè no tenen cap factor en comú (coprimers): $1 = (a, p)$. Per tant tindrem que existeixen dos enters de manera que

$$1 = n \cdot a + m \cdot p$$

Ara fixem-nos que si aquesta igualtat la llegim mòdul $p$ obtenim:

$$1 = n \cdot a + m \cdot p \equiv n \cdot a \bmod p$$

De la igualtat

$$1 = n \cdot a \bmod p$$

en traiem que $n = a^{-1} \bmod p$. Com hem vist abans, l'algorisme d'Euclides invers permet calcular $n$ i $m$ i, per tant, l'invers d'$a$ mòdul $p$.

**Exemple 2.** *Calculem l'invers de* 258 *mòdul* 571. *Apliquem l'algorisme d'Euclides per trobar el màxim comú divisor de* 258 *i* 571. *Com* 571 *és primer aquest hauria de*

*ser 1:*

$$\begin{array}{ll} 571 = 2 \cdot 258 + 55 \Longrightarrow & 55 = 571 - 2 \cdot 258 \\ 258 = 4 \cdot 55 + 38 \Longrightarrow & 38 = 258 - 4 \cdot 55 = 9 \cdot 258 - 4 \cdot 571 \\ 55 = 1 \cdot 38 + 17 \Longrightarrow & 17 = 55 - 1 \cdot 38 = 571 - 2 \cdot 258 - (9 \cdot 258 - 4 \cdot 571) \\ & 17 = 5 \cdot 571 - 11 \cdot 258 \\ 38 = 2 \cdot 17 + 4 \Longrightarrow & 4 = 38 - 2 \cdot 17 = 9 \cdot 258 - 4 \cdot 571 - 2 \cdot (5 \cdot 571 - 11 \cdot 258) \\ & 4 = 31 \cdot 258 - 14 \cdot 571 \\ 17 = 4 \cdot 4 + 1 \Longrightarrow & 1 = 17 - 4 \cdot 4 = 5 \cdot 571 - 11 \cdot 258 - 4 \cdot (31 \cdot 258 - 14 \cdot 571) \\ & 1 = 61 \cdot 571 - 135 \cdot 258 \\ 4 = 4 \cdot 1 + 0 & \end{array}$$

*Per tant, obtenim que* 1 *és el màxim comú divisor (258 i 517 són coprimers) i, a més l'algorisme d'Euclides extès ens dóna:*

$$1 = 61 \cdot 517 - 135 \cdot 258$$

*Per tant, mòdul 517 obtenim que*

$$1 \equiv -135 \cdot 258 \bmod 571 \Longrightarrow -135 \equiv 258^{-1} \bmod 571$$

*Ara només caldria escriure -135 com a enters positiu mòdul 517, simplement sumant 571 obtenim:*

$$-135 \equiv 436 \bmod 571$$

*i ja tenim que*

$$258^{-1} \equiv 436 \bmod 571$$

*Per comprovar-ho només caldria multiplicar* $436 \cdot 258$ *i veure que és 1 mòdul 517:*

$$436 \cdot 258 = 112488 = 197 \cdot 571 + 1 \equiv 1 \bmod 571$$

# 2 Xifratges asimètrics: de clau pública i clau privada

Tot el que circula per la xarxa ha d'anar xifrat per tal que, si algú està escoltant el tràfic (sniffers), no pugui "entendre" el que escolta. Tot mètode de xifratge passa per tenir una mena de "password", que el decideix qui rebrà el missatge. Ara bé, en principi, l'emissor també hauria de conèixer aquest "password" per tal d'utilitzar-lo d'alguna manera per xifrar el missatge que enviarà, i és aquí on apareixen els principals punts febles dels mètodes de xifratge: el moment en què el receptor envia el

"password" a l'emissor perquè l'utilitzi en els missatges que l'enviarà. Si algú captura aquest "missatge inicial" (handshake) aleshores podria conèixer el "password" i desxifrar per tant to el que circuli.

Els xifratges de clau pública i clau privada aconsegueixen que l'emissor xifri els missatge sense de fet conèixer la "el password". Això funciona principalment de la següent manera:

1. El receptor s'inventa un "password", que s'anomena *clau privada* i que només coneix ell.

2. El mateix receptor, a partir de la clau privada obté (d'una manera molt complicada) una altra clau, que s'anomena la *clau pública*, i que "amaga" la clau privada.

3. El mateix receptor fa pública la clau pública dient "Qui vulgui escriure'm que faci servir aquesta clau pública per xifrar el missatge".

4. Tots el missatges s'envien al receptor venen xifrats amb la clau pública. Ara bé, el mètode que es fa servir per xifrar-los fa que, per tal de desxifrar-los sigui necessari conèixer també la clau privada. Com aquesta última només la té el receptor, "ningú" podrà desxifrar els missatges que rebi el receptor a part d'ell mateix.

## 2.1 Xifratge RSA

El xifratge RSA és un dels més estesos, es fa servir actualment en aplicacions com ara

- Connexions segures amb ssh o vpn
- Connexions bluetooth
- Transaccions bancàries (pagaments amb targeta o transferències)
- Connexions web segures

És un tipus de xifratge asimètric (amb clau pública i clau privada). Com tots els mètodes de xifratge s'assumeix que el missatge es troba traduït a un nombre, que pot provenir d'un text (codi ASCII), una foto (jpeg), d'un vídeo (mp4) o d'un so (mp3). Consisteix en els següents passos:

1. El receptor decideix un password en forma de dos nombres primers, $p$ i $q$. Aquests formaran la clau privada que només el receptor coneix. Quant més grans siguin aquests menys vulnerable serà el xifratge.

2. El receptor els multiplica: $n = p \cdot q$.

3. El receptor calcula $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$

4. El receptor escull un nombre $e$ coprimer amb $\varphi(n)$.

5. El receptor calcula $d = e^{-1} \bmod \varphi(n)$. Fixeu-vos que, tot i que $\varphi(n)$ no sigui un nombre primer, el fet que $e$ sigui coprimer amb $\varphi(n)$ ($\text{m.c.d}\,(\varphi(n), e) = 1$) garanteix que $e$ es pot invertir mòdul $\varphi(n)$.

6. El receptor difon la clau pública que consisteix en els dos enters $(n, e)$.

7. L'emissor (i tothom que estigui escoltant) rep la clau pública, $(n, e)$.

8. L'emissor tradueix el seu missatge (text, imatge, vídeo, so, dades,...) a un nombre $m$. De fet, el missatge que es vol transmetre es fragmenta: per exemple, es xifren les lletres d'un text una a una, es xifren els píxels d'una imatge un a un, es xifren els frames d'un vídeo un a un, etc...

9. L'emissor xifra $m$ fent $c = m^e \bmod n$. Ara, el nombre $c$ serà la versió xifrada del nombre $m$ xifrat. El punt clau del mètode és que ara, sabent $c$, $e$ i $n$ aquesta operació no es pot desfer així com així.