Índex

Aritmètica entera bàsica

Enters com a anell

Els *enters* $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ amb $+$ i $\cdot$ forma un *anell*:

- $(\mathbb{Z}, +)$ és un *grup abelià*:
  - $\forall a, b, c$: $a + (b + c) = (a + b) + c$ (associativa)
  - $\exists 0$ t.q. $\forall a$: $a + 0 = 0 + a = a$ (el. neutre)
  - $\forall a, \exists -a$: $a + (-a) = (-a) + a = 0$ (el. oposat)
  - $\forall a, b$: $a + b = b + a$ (commutativa)
- $(\mathbb{Z}, \cdot)$ compleix:
  - $\forall a, b, c$: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativa)
  - $\exists 1$ t.q. $\forall a$: $a \cdot 1 = 1 \cdot a = a$ (el. neutre)
  - $\forall a, b$: $a \cdot b = b \cdot a$ (commutativa)
- $(\mathbb{Z}, +, \cdot)$ compleix:
  - $\forall a, b, c$: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (distributiva)

Enters com a conjunt ordenat

Enters amb $\leq$ habitual és conjunt *totalment ordenat*:

- $\forall a$: $a \leq a$
- $\forall a, b, c$: $a \leq b$ i $b \leq c \implies a \leq c$
- $\forall a, b$: $a \leq b$ i $b \leq a \implies a = b$
- $\forall a, b$: o bé $a < b$, o bé $a > b$, o bé $a = b$

A més:

- Tot subconjunt $S \subset \mathbb{Z}$ fitat inferiorment té mínim:
  Si $\exists f$ t.q. $\forall a \in S, f \leq a$, aleshores $\exists b \in S$ t.q. $\forall a \in S, b \leq a$

A més, es comporta bé respecte operacions:

- Si $a \leq b$, aleshores $a + c \leq b + c$ $(\forall c \in \mathbb{Z})$
- Si $a \leq b$, aleshores $a \cdot c \leq b \cdot c$ $(\forall c \in \mathbb{N})$

Teorema: Divisió euclidiana

Donats $a, b \in \mathbb{Z}$, $(b \neq 0)$, existeixen únics q (*quocient*) i r (*resta* o *residu*), t.q.

$$a = b \cdot q + r, \qquad 0 \leq r < b$$

Demostració

Suposem $b > 0$. Sigui $R = \{a - bx \mid x \in \mathbb{Z}\} \cap \mathbb{Z}_{\geq 0}$.

- R fitat inf. per 0
- R no buid (si $a \geq 0$, $a \in S$; altrament $a - ba = a(1-b) \in R$)
- Sigui r mínim de R. $r \geq 0$ per definició. Si $r \geq b$, $r - b \in R$ i r no mínim. A més, $r = a - bq$ per a cert q. (existència)
- Suposem no únics ((q, r) i (q', r')). Si $q = q'$, $r = r'$ i hem acabat. Si $q' < q$,

$$r' = a - |b|q' = (a - |b|q) + |b|(q - q') \geq (a - |b|q) + |b| = r + |b| \geq |b|,$$

contradicció. □

Divisibilitat

- "$a \bmod b$" indica residu de divisió euclidiana de a entre b
- Si residu 0 ($a = q \cdot b$):
  - a és *múltiple* de b
  - b *divideix* a, $b|a$
- Relació amb operacions:
  - Si $a|b$ i $c \in \mathbb{Z}$ qualsevol: $a|b \cdot c$
  - Si $a|b$ i $a|c$: $a|b + c$

Algoritme d'Euclides

Màxim comú divisor

Donats $a, b \in Z$:

- $\mathrm{CD}(a, b)$ divisors comuns positius de a i b
- $\mathrm{mcd}(a, b)$ major divisor comú positiu de a i b
- Definició alternativa:

$$x \,|\, a, \quad x \,|\, b \implies x \,|\, \mathrm{mcd}(a, b).$$

- a i b són *relativament primers* (o *coprimers*) si $\mathrm{mcd}(a, b) = 1$.

Mínim comú múltiple

- $\mathrm{mcm}(a, b)$ menor múltiple comú positiu de a i b
- Definició alternativa:

$$a \,|\, x, \quad b \,|\, x \implies \mathrm{mcm}(a, b) \,|\, x,$$

Lema

Siguin $a, b \in \mathbb{Z}_{>0}$, i $r = a \bmod b$. Aleshores $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$.

Demostració

Sigui $a = b \cdot q + r$ la divisió euclidiana. Vegem que $\mathrm{CD}(a, b) = \mathrm{CD}(b, r)$:

- Sigui $d \in \mathrm{CD}(a, b)$. Com $r = a - bq$, d és divisor de r i de b: $d \in \mathrm{CD}(b, r)$.
- Sigui $d \in \mathrm{CD}(b, r)$. Com $a = bq + r$, d és divisor de a i de b: $d \in \mathrm{CD}(a, b)$.

Per tant, $\mathrm{CD}(a, b) = \mathrm{CD}(b, r)$ i $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$. $\square$

Teorema (algorisme d'Euclides)

Donats enters positius $a, b \in \mathbb{Z}_{>0}$, posem $r_0 = a$, $r_1 = b$ i considerem la successió de divisions euclidianes:

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 && (0 \le r_2 < r_1)\\
r_1 &= r_2 q_3 + r_3 && (0 \le r_3 < r_2)\\
r_2 &= r_3 q_4 + r_4 && (0 \le r_4 < r_3)\\
&\vdots\\
r_{i-1} &= r_i q_{i+1} + r_{i+1} && (0 \le r_{i+1} < r_i)\\
&\vdots\\
r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1} && (0 \le r_{k-1} < r_{k-2})\\
r_{k-2} &= r_{k-1} q_k + r_k && (r_k = 0)
\end{aligned}$$

Aleshores r_{k-1} (l'últim residu no nul) és igual a $\mathrm{mcd}(a, b)$.

Demostració

- L'algorisme acaba: Els residus són enters positius i formen successió estrictament decreixent.
- Al principi: $\mathrm{mcd}(a, b) = \mathrm{mcd}(r_0, r_1)$
- A cada pas, pel lema: $\mathrm{mcd}(r_{i-1}, r_i) = \mathrm{mcd}(r_i, r_{i+1})$
- Al final: $\mathrm{mcd}(r_{k-2}, r_{k-1}) = r_{k-1}$

Per tant, $\mathrm{mcd}(a, b) = r_{k-1}$

Exemple

Calculem $\operatorname{mcd}(4864, 3458)$ donant la seqüència de divisions euclidianes que s'obtenen:

i	r	q
0	4864	–
1	3458	–
2	1406	1
3	646	2
4	114	2
5	76	5
6	38	1
7	0	2

Per tant, $\operatorname{mcd}(4864, 3458) = 38$.

Identitat de Bezout

Donats enters positius $a, b \in \mathbb{Z}_{>0}$, posem

$$\begin{aligned} r_0 &= a, & x_0 &= 1, & y_0 &= 0, \\ r_1 &= b, & x_1 &= 0, & y_1 &= 1 \end{aligned}$$

i considerem la successió de divisions euclidianes:

$$\begin{aligned} r_0 &= r_1 q_2 + r_2 & x_2 &= x_0 - q_2 x_1, & y_2 &= y_0 - q_2 y_1, \\ r_1 &= r_2 q_3 + r_3 & x_3 &= x_1 - q_3 x_2, & y_3 &= y_1 - q_3 y_2, \\ r_2 &= r_3 q_4 + r_4 & x_4 &= x_2 - q_4 x_3, & y_4 &= y_2 - q_4 y_3, \\ &\vdots \\ r_{i-1} &= r_i q_{i+1} + r_{i+1} & x_{i+1} &= x_{i-1} - q_{i+1} x_i, & y_{i+1} &= y_{i-1} - q_{i+1} y_i, \\ &\vdots \\ r_{k-2} &= r_{k-1} q_k + r_k & x_k &= x_{k-2} - q_k x_{k-1}, & y_k &= y_{k-2} - q_k y_{k-1}, \end{aligned}$$

Aleshores $x = x_{k-1}$ i $y = y_{k-1}$ compleixen que $\operatorname{mcd}(a, b) = x \cdot a + y \cdot b$.

Demostració

A cada pas: $r_i = x_i a + y_i b$.

- $i = 0, 1$: es compleix trivialment a partir de la definició.
- $i - 1, i \implies i + 1$:

$$\begin{aligned} x_{i+1} \cdot a + y_{i+1} \cdot b &= (x_{i-1} - q_{i+1} x_i) \cdot a + (y_{i-1} - q_{i+1} y_i) \cdot b \\ &= (x_{i-1} \cdot a + y_{i-1} \cdot b) - q_{i+1}(x_i \cdot a + y_i \cdot b) \\ &= r_{i-1} - q_{i+1} r_i \\ &= r_{i+1}. \end{aligned}$$

Al pas $k - 1$: $\operatorname{mcd}(a, b) = r_{k-1} = x_{i-1} a + y_{i-1} b = x \cdot a + y \cdot b$. $\square$

Exemple

Calculem $\text{mcd}(4864, 3458)$ i els coeficients que compleixen la identitat de Bezout.

i	r	q	x	y
0	4864	–	1	0
1	3458	–	0	1
2	1406	1	1	−1
3	646	2	−2	3
4	114	2	5	−7
5	76	5	−27	38
6	38	1	32	−45
7	0	2	−91	128

Per tant, $\text{mcd}(4864, 3458) = 38 = 32 \cdot 4864 + (-45) \cdot 3458$.

Proposició

Fixats enters positius $a, b \in \mathbb{Z}_{>0}$, i un enter arbitrari k, existeixen enters $x, y \in \mathbb{Z}$ tals que $x \cdot a + y \cdot b = k$ ssi k és un múltiple de $\text{mcd}(a, b)$.

Demostració

- Si k és múltiple de $\text{mcd}(a, b)$, diguem $k = k' \cdot \text{mcd}(a, b)$, per la identitat de bezout tenim que existeixen enters x', y' amb $\text{mcd}(a, b) = x'a + y'b$, d'on $k = k'(x'a + y'b) = (k'x')a + (k'y')b$.
- Recíprocament, si k és de la forma $x \cdot a + y \cdot b$, donat d un divisor comú de a i b, es té que d és un divisor de $x \cdot a + y \cdot b$, d'on k és múltiple de d. En particular, k és múltiple de $\text{mcd}(a, b)$. □

Nombres primers

Primers i irreductibles

- Un nombre p (positiu) és *primer* si:

$$p | x \cdot y \implies p | x \text{ ó } p | y.$$

- Un nombre p (positiu) és *irreductible* si:

$$p = x \cdot y \ (x, y > 0) \implies x = p \text{ ó } y = p.$$

Proposició

Donat p enter positiu, són equivalents que sigui primer i que sigui irreductible.

Demostració

- (primer $\implies$ irreductible): Suposem p primer i sigui $p = xy$ factorització. Com $p|xy$ tenim $p|x$ (o $p|y$); aleshores $x = pq$ (per a cert q) i $p = xy = pqy$ d'on $qy = 1$. Així $y = 1$ i $x = p$.
- (irreductible $\implies$ primer): Suposem p irreductible i suposem $p|xy$. Si $p|x$, hem acabat. Si $p\nmid x$ tenim $\mathrm{mcd}(p, x) = 1$, d'on

$$1 = pr + xs \implies y = pry + xsy \implies pry = y - xsy$$

i per tant:

$$p|y - sxy \implies p|y$$

□

Proposició

Tot nombre major que 1 es divideix per algun nombre primer.

Demostració.

Suposem que no. Sigui n més petit positiu que no es divideix per cap primer.

- n no és primer (altrament es divideix per ell mateix, un primer)
- Sigui $n = ab$ factorització ($1 < a, b < n$). Ara a sí es divideix per nombre primer (n és el més petit que no ho fa). Per tant, n també. Contradicció.

□

Teorema

Hi ha infinits nombres primers.

Demostració.

Suposem que no, i sigui n una fita superior per als nombres primers. Considerem $m = n! + 1$; aquest nombre no és divisible per cap enter $k \leq n$, ja que $m \bmod k = 1 \neq 0$. Per tant, no és divisible per cap nombre primer, cosa que és una contradicció. □

Teorema fonamental de l'aritmètica

Els nombres enters tenen factorització única. És a dir, donat un enter no nul, aquest es descomposa de forma única (llevat de signe i permutacions) en producte de primers.

Demostració

Existència: Vist a lògica.
Unicitat: Si $n = \pm 1 p_1 \cdots p_k = \pm 1 q_1 \cdots q_l$ són factoritzacions:

- signe ± 1: determinat pel fet que n sigui positiu o negatiu; és igual en totes dues descomposicions
- $p_1 \,|\, q_1 \cdots q_l$, d'on $p_1 \,|\, q_i$ (per algun i); per tant, $p_1 = q_i$.
- Iterem amb $n/p_1 = n/q_i$. □

p-components

- Donat p primer i n enter:

$$\mathrm{ord}_p(n) = \text{major } k \text{ t.q. } p^k | n$$

- En termes de descomposició:

$$n = \pm 1 \cdot p_1^{\mathrm{ord}_{p_1}(n)} p_2^{\mathrm{ord}_{p_2}(n)} \cdots p_k^{\mathrm{ord}_{p_k}(n)}$$

  amb p_i primers diferents 2 a 2.
- Aplicació a mcd i mcm:

$$\mathrm{mcd}(a,b) = \prod_p p^{\min(\mathrm{ord}_p(a), \mathrm{ord}_p(b))}$$

$$\mathrm{mcm}(a,b) = \prod_p p^{\max(\mathrm{ord}_p(a), \mathrm{ord}_p(b))}$$

- En particular: $ab = \mathrm{mcd}(a,b)\,\mathrm{mcm}(a,b)$

Exemple

Tenim $4864 = 2^8 \cdot 19$ d'on:

$$\mathrm{ord}_p(4864) = \begin{cases} 8 & \text{si } p = 2 \\ 1 & \text{si } p = 19 \\ 0 & \text{altrament} \end{cases}$$

Tenim $3458 = 2 \cdot 7 \cdot 13 \cdot 19$ d'on

$$\mathrm{ord}_p(3458) = \begin{cases} 1 & \text{si } p = 2, 7, 13, 19 \\ 0 & \text{altrament} \end{cases}$$

Per tant:

$$\mathrm{mcd}(4864, 3458) = 2 \cdot 19$$

$$\mathrm{mcm}(4864, 3458) = 2^8 \cdot 7 \cdot 13 \cdot 19$$

Aritmètica modular

Congruències

Fixem enter $N > 1$:

- $a, b \in \mathbb{Z}$ *congruent mòdul* N si $N | a - b$
- Notació: $a \equiv b \pmod{N}$
- Equivalent: $a \bmod N = b \bmod N$

Classes de congruències

- La relació "ser congruents mòdul N" és d'equivalència
- Classe d'equivalència de $a \in \mathbb{Z}$: $[a]_N$ ó $[a]$:

$$[a]_N = \{\ldots, a - 2N, a - N, a, a + N, a + 2N, \ldots\}.$$

- Conjunt de classes d'equivalència: $\mathbb{Z}_N$:

$$\mathbb{Z}_N = \{[0], [1], \ldots, [N-1]\}$$

Exemple

Prenem $N = 6$; aleshores $\mathbb{Z}_6$ té 6 elements:

$$\begin{aligned}
[0] &= \{\ldots, -6, 0, 6, 12, \ldots\} \\
[1] &= \{\ldots, -5, 1, 7, 13, \ldots\} \\
[2] &= \{\ldots, -4, 2, 8, 14, \ldots\} \\
[3] &= \{\ldots, -3, 3, 9, 15, \ldots\} \\
[4] &= \{\ldots, -2, 4, 10, 16, \ldots\} \\
[5] &= \{\ldots, -1, 5, 11, 17, \ldots\}
\end{aligned}$$

Operacions amb classes de congruència

Sobre $\mathbb{Z}_N$: operacions de suma i de producte:

$$\begin{aligned}
[a] + [b] &= [a + b] \\
[a] \cdot [b] &= [a \cdot b]
\end{aligned}$$

Lema

L'operació està ben definida:

$$\left.\begin{aligned} a \equiv a' \pmod{N} \\ b \equiv b' \pmod{N} \end{aligned}\right\} \implies \left\{\begin{aligned} a + b \equiv a' + b' \pmod{N} \\ a \cdot b \equiv a' \cdot b' \pmod{N} \end{aligned}\right.$$

Demostració

Sigui k, l t.q $kN = a - a'$ i $lN = b - b'$. Ara:

- $(k + l)N = (a + b) - (a' + b') \implies N \,|\, (a + b) - (a' + b')$
  $\implies a + b \equiv a' + b' \pmod{N} \implies [a + b] = [a' + b']$
- $ab = a'b' + N(la' + kb' + klN) \implies N \,|\, ab - a'b'$
  $\implies ab \equiv a'b' \pmod{N} \implies [ab] = [a'b']$ □

Exemple

La taula de la suma i el producte a $\mathbb{Z}_6$ és:

$+$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

$\mathbb{Z}_N$ com a anell

$(\mathbb{Z}_N, +, \cdot)$ és anell:

- $(\mathbb{Z}_N, +)$ grup abelià; element neutre: $[0]$; el. oposat de $[a]$: $[-a]$.
- $(\mathbb{Z}_N, \cdot)$ propietat associativa; element neutre, $[1]$.
- $(\mathbb{Z}_N, +, \cdot)$ propietat distributiva del producte respecte de la suma

Invertibles

- $[a] \in \mathbb{Z}_N$ *invertible* (o a invertible mòdul N) si $\exists [b] \in \mathbb{Z}_N : [a] \cdot [b] = [1]$
- Elements invertibles: $\mathbb{Z}_N^*$ (grup amb el producte)

Proposició

$[a] \in \mathbb{Z}_N$ invertible $\iff \operatorname{mcd}(a, N) = 1$.

Demostració

- Si $[a]$ invertible, sigui $[b]$ amb $[a] \cdot [b] = [ab] = [1]$
  $\implies N \,|\, 1 - ab \implies \exists k : 1 = kN + ab \implies \operatorname{mcd}(a, N) = 1$ (Bezout)
- Si $\operatorname{mcd}(a, N) = 1 \implies \exists r, s \in \mathbb{Z}$: $1 = ra + sN \implies 1 \equiv ra \pmod{N}$
  $\implies [1] = [r] \cdot [a]$.

Exemple

$$\mathbb{Z}_6^* = \{[1], [5]\}$$

Corol·lari

Si p és primer, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{[0]\}$

Càlcul d'inversos

Si $[a]$ invertible, es pot trobar l'invers $[a]^{-1}$ amb algorisme d'Euclides estès:

$$\mathrm{mcd}(a, N) = 1 \implies \exists r, s: \ ra + sN = 1 \implies [r][a] = 1 \implies [a]^{-1} = [r]$$

Exemple

Invers de 35 mòdul 2452

$$\mathrm{mcd}(2452, 35) = 1, \qquad 1 = (-17) \cdot 2452 + 1191 \cdot 35,$$

$$[35]_{2452}^{-1} = [1191]_{2452}.$$

Nombre d'invertibles

- $\phi(N) := |\mathbb{Z}_N^*|$ (ϕ d'Euler)
- Equiv.: $\phi(N) = |\{k \mid 1 \leq N < k, \mathrm{mcd}(k, N) = 1\}|$

Teorema d'Euler

Si $y \in \mathbb{Z}$ té $\gcd(y, N) = 1$, aleshores $y^{\phi(N)} \equiv 1 \pmod N$.

Lema

Si $\mathbb{Z}_N^* = \{[x_1], \dots, [x_k]\}$ i $[y] \in \mathbb{Z}_N^*$ quals., $\{[y][x_1], \dots, [y][x_k]\} = \mathbb{Z}_N^*$.

Demostració (Lema)

Per a cada $[x_i]$, $[y][x_i] = [x_{\sigma(i)}]$ (certa permutació $\sigma \in \mathfrak{S}_k$):

- $[y][x_i]$ té invers $[x_i]^{-1}[y]^{-1} \implies [y][x_i] = [x_{\sigma(i)}]$
- $\sigma(i) = \sigma(j) \implies [y][x_i] = [y][x_j] \implies [x_i] = [x_j]$

Teorema d'Euler

Si $y \in \mathbb{Z}$ té $\gcd(y, N) = 1$, aleshores $y^{\phi(N)} \equiv 1 \pmod N$.

Demostració

S'ha de provar: $[y] \in \mathbb{Z}_N^* \implies [y]^{\phi(N)} = [1]$:

- Sigui $\mathbb{Z}_N = \{[x_1], \dots, [x_k]\}$ ($k = \phi(N)$)
- Sigui $u = [x_1] \dots [x_k] \in \mathbb{Z}_N^*$
- Lema anterior: $u = [x_1] \cdots [x_k] = ([y][x_1]) \cdots ([y][x_k]) = [y]^k u$
- Per tant: $[y]^k = [1]$. □

Corol·lari: Teorema petit de Fermat

Si p és primer, $n^p \equiv n \pmod p$ per a tot enter n.

Teorema xinès dels residus

Equacions lineals amb congruències

Equació $x \equiv a \pmod{M}$ (x: variable; a, M: dades)
Solucions: $x = \dots, a - 2M, a - M, a, a + M, a + 2M, \dots$

Teorema xinès dels residus

El sistema

$$\begin{aligned} x &\equiv a \pmod{M} \\ x &\equiv b \pmod{N} \end{aligned}$$

té solució si, i només si,

$$\operatorname{mcd}(M, N) \mid b - a.$$

En tal cas, i donada una solució x_0, totes les solucions del sistema són les de la congruència

$$x \equiv x_0 \pmod{\operatorname{mcm}(M, N)}.$$

Demostració

- Si hi ha solució, siguin y, z amb $x = a + My = b + Nz$
  $\iff My - Nz = b - a \implies$ (Bezout) $\operatorname{mcd}(M, N) \mid b - a$
- Si $\operatorname{mcd}(M, N) \mid b - a$, sigui y, z amb $My - Nz = b - a$.
  Ara $x = a + My = b + Nz$ és solució
- Si x_0, x_1 són solucions, $x_1 - x_0$ és solució de

$$\begin{aligned} x &\equiv 0 \pmod{M} \\ x &\equiv 0 \pmod{N} \end{aligned}$$

  equivalent a: $x \equiv 0 \pmod{\operatorname{mcm}(M, N)}$ □

Demostració

Considerem el sistema:

$$\begin{aligned} x &\equiv 11 \pmod{74} \\ x &\equiv 13 \pmod{63} \end{aligned}$$

Les solucions compleixen que existeixen y, z amb

$$x = 11 + 74y = 13 + 63z,$$

d'on tenim que

$$74y - 63z = 2.$$

Fent servir l'algorisme estès d'Euclides obtenim la solució

$$74 \cdot (-17) + 63 \cdot 20 = 2$$

i, per tant, podem prendre $y = -17$ i $z = -20$. Aleshores

$$x = 13 - 63 \cdot 20 = -1247$$

és una solució.

Corol·lari: Forma clàssica de TXR

Siguin M, N nombres positius relativament primers. Aleshores el sistema de congruències

$$\begin{aligned} x &\equiv a \pmod{M} \\ x &\equiv b \pmod{N} \end{aligned}$$

té sempre solució.

Corol·lari: Forma general de TXR

Siguin $M_1, \ldots, M_k$ nombres positius relativament primers dos a dos. Aleshores el sistema de congruències

$$x \equiv a_i \pmod{M_i} \qquad (i = 1, \ldots, k)$$

té sempre solució.

Proposició: càlcul de $\phi(n)$

- Si $m, n > 0$ relativament primers:

$$\phi(m \cdot n) = \phi(m)\phi(n).$$

- Si p és primer i $r \geq 1$:

$$\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1) = p^r\left(1 - \frac{1}{p}\right).$$

- Si $n = \prod_{i=1}^{k} p_i^{r_i}$ (p_i primers diferents):

$$\phi(n) = \prod_{i=1}^{k} p_i^{r_i - 1}(p_i - 1) = n \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).$$

Demostració

1. Considerem

$$\begin{aligned} \mathbb{Z}_{mn} &\to \mathbb{Z}_m \times \mathbb{Z}_n \\ [a]_{mn} &\mapsto ([a]_m, [a]_n) \end{aligned}$$

   Per TXR: a invertible mòd. mn ssi inv. mòdul n i mòdul m.
   $\implies$ Aplicació és bijecció entre $\mathbb{Z}^*_{mn}$ i $\mathbb{Z}^*_m \times \mathbb{Z}^*_n$ $\implies \phi(mn) = \phi(m)\phi(n)$
2. Hi ha $p^r/p = p^{r-1}$ múltiples de p a $\{0, \ldots, p^r\}$
   $\implies$ hi ha $p^r - p^{r-1}$ **no** múltiples de p
   $\implies$ hi ha $p^r - p^{r-1}$ rel. primers amb p^r.
3. Immediat a partir dels anteriors □

Aplicacions a criptografia

Criptografia

Criptografia: Mètodes per a modificar missatges a enviar de manera que capturant el missatge modificat no es pugui recuperar el missatge original

Codificació

- *Codificació*: Mètodes per a transformar missatges en números, de manera que es puguin tractar matemàticament
- *Blocs i codis*: Els missatges es divideixen en blocs de longitud fixada, i cada bloc es codifica en un únic número.

Codificacions simples

- Alfabet llatí:

A	B	C	...	Y	Z
0	1	2	...	24	25

- Codificació `ASCII`:

NUL	SOH	...	0	1	...	9	...	A	...	Z	...	a	...	z	...	DEL
0	1	...	48	49	...	57	...	65	...	90	...	97	...	122	...	127

- Codificació `UNICODE`: estén `ASCII` amb caràcters extra (accents,...)

Codis per blocs

- Considerar blocs de k caràcters, codificats entre 0 i $N-1$.
- El bloc $(c_{k-1}, c_{k-2}, \dots, c_1, c_0)$ es codifica per:

$$C = c_{k-1} \cdot N^{k-1} + c_{k-2} N^{k-2} + \cdots + c_1 N + c_0$$

- El codi anterior es decodifica per:

$$\begin{aligned} c_0 &= C \bmod N \\ c_1 &= \frac{C - c_0}{N} \bmod N \\ c_i &= \frac{C - c_0 - \cdots - c_{i-1} N^{i-1}}{N^i} \bmod N \end{aligned}$$

Exemple

Missatge: `Criptografia`.
Blocs de longitud 4 i codifiquem els caracters pel seu codi ASCII.
Bloc: `Crip`. Codis ASCII: $(67, 114, 105, 112)$

$$C = 67 \cdot 128^3 + 114 \cdot 128^2 + 105 \cdot 128 + 112 = 142\,390\,512.$$

Seqüencia de codis:

$$142\,390\,512, \quad 245\,101\,554, \quad 205\,108\,449.$$

Criptografia

- Ara missatges són enters (entre 0 i $N-1$):

$$m \in \mathcal{M} = \{0, \ldots, N-1\} \simeq \mathbb{Z}_N$$

- Processos de xifrat i desxifrat:

$$E : \mathcal{M} \to \mathcal{C} \qquad D : \mathcal{C} \to \mathcal{M}$$

  $\mathcal{C}$ conjunt de *criptogrames*
- Condició:

$$D(E(m)) = m \quad \text{per a tot } m \in \mathcal{M}$$

- Processos sovint depenen de paràmetre k (clau): E_k i D_k

Xifrat de Cesar

- Missatges: $\mathcal{M} = \mathbb{Z}_{26}$ (blocs de 1 caracter llatí)
- Criptogrames: $\mathcal{C} = \mathbb{Z}_{26}$
- Funcions d'encriptació i desencriptació:

$$E(m) = m + 3 \bmod 26, \qquad D(c) = c - 3 \bmod 26$$

Exemple

ATAQUEU s'encripta en DWDTXHX

Generalització: xifrat afí

- Paràmetres: $a \in \mathbb{Z}_N^*$, $b \in \mathbb{Z}_N$
- Funcions d'encriptació i desencriptació:

$$E_{a,b}(x) = ax + b, \qquad D_{a,b}(x) = a^{-1}(x - b)$$

Xifrat de clau pública

- Idea: Tot usuari pot xifrar missatges per a qualsevol usuari. Únicament el destinatari el pot desxifrar.
- Procés de xifrat E_{k_p}: Depèn de k_p (clau pública del destinatari)
- Procés de desxifrat D_{k_s}: Depèn de k_s (clau privada del destinatari)
- Condició: Per a tot usuari (amb claus k_p, k_s) i tot missatge m:

$$D_{k_s}(E_{k_p}(m)) = m$$

- Condició de seguretat: Donat k_p és molt difícil trobar k_s

Xifrat RSA

- Primer i més emprat sistema de clau pública
- p, q primers "grans" (200 xifres)
- $n = p \cdot q$
- $\phi(n) = (p-1)(q-1)$
- e amb $1 < e < \phi(n)$ i $\mathrm{mcd}(e, \phi(n)) = 1$
- d invers de e mòdul $\phi(n)$
- $k_p = (n, e)$
- $k_s = (n, d)$
- $E_{k_p}(m) = m^e \bmod n$
- $D_{k_s}(c) = c^d \bmod n$

Exemple

Exemple de codificar CRIPTOGRAFIA. Missatges amb $4 \cdot 7 = 28$ bits.
Cal p i q amb $p \cdot q > 2^{28}$:

- Prenem $p = 16\,381$ i $q = 17\,011$.
- Calculem $n = pq = 278\,657\,191$.
- Calculem $\phi(n) = (p-1)(q-1) = 278\,623\,800$.
- Triem l'exponent $e = 155\,327$, que és relativament primer amb $\phi(n)$.
- Calculem l'invers de e mòdul $\phi(n)$, $d = 233\,323\,463$.
- Claus pública i privada:
  $k_p = (278\,657\,191, 155\,327)$, $\quad k_s = (278\,657\,191, 233\,323\,463)$.
- Xifrat de $m = 142\,390\,512$:
  $c = m^e \bmod n = (142\,390\,512)^{155\,327} \bmod 278\,657\,191 = 229\,531\,282$.
- Desxifrat del criptograma:
  $m = c^d \bmod n = (229\,531\,282)^{233\,323\,463} \bmod 278\,657\,191 = 142\,390\,512$.