Fonaments Matemàtics (segona part)

José Luis Ruiz

Juliol 2017

Departament de Matemàtiques
Facultat d'Informàtica de Barcelona
Universitat Politècnica de Catalunya

L’anell dels nombres enters

L'anell dels enters

Nombres naturals i nombres enters

Nombre naturals: $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Nombres enters: $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$.

Operacions amb enters

La suma i el producte de dos enters és un altre enter; és a dir, són *operacions binàries internes* en el conjunt $\mathbb{Z}$:

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \qquad \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}.$$

Propietats de les operacions

Propietats de la suma

- **Associativa:** si $a, b, c \in \mathbb{Z}$, llavors $a + (b + c) = (a + b) + c$.
- **Commutativa:** si $a, b \in \mathbb{Z}$, llavors $a + b = b + a$.
- **Existència d'element neutre:** si $a \in \mathbb{Z}$, llavors $0 + a = a$.
- **Existència d'element invers:** si $a \in \mathbb{Z}$, llavors $a + (-a) = 0$.

Propietats de les operacions

Propietats del producte

- **Associativa:** si $a, b, c \in \mathbb{Z}$, llavors $a(bc) = (ab)c$.
- **Commutativa:** si $a, b \in \mathbb{Z}$, llavors $ab = ba$.
- **Existència d'element neutre:** si $a \in \mathbb{Z}$, llavors $1 \cdot a = a$.

Propietat distributiva

Si $a, b, c \in \mathbb{Z}$, llavors $a(b + c) = ab + ac$.

$\mathbb{Z}$ és un anell

Definició d'anell

Un **anell** és un conjunt amb dues operacions que satisfan totes les propietats anteriors.

Exemple: $\mathbb{Z}$ és un anell amb la *suma* i el *producte* usuals.

Definició de cos

Un **cos** és un conjunt amb dues operacions que satisfan totes les propietats anteriors i, a més, l'equació $ax = 1$ té solució per a tot $a \neq 0$.

Exemple: $\mathbb{Q}$ és un cos.

Observació

No sempre podem dividir un enter per un altre (és a dir, no sempre hi ha inversos): l'equació $ax = 1$ té solució a $\mathbb{Z}$ si, i només si, $a = 1$ o $a = -1$. Per tant, $\mathbb{Z}$ no és un *cos*.

Altres propietats de $\mathbb{Z}$

Llei de cancel·lació

Per a tot $a, b, c \in \mathbb{Z}$, si $a \cdot c = b \cdot c$ i $c \neq 0$, aleshores $a = b$.

Relació d'ordre

Si $a, b \in \mathbb{Z}$, aleshores:

$$a < b \iff b - a \in \mathbb{N} - \{0\}.$$

Relació d'ordre i operacions

- Si $a \in \mathbb{Z}$, llavors $a < 0$, $a = 0$ o $a > 0$.
- Si $a, b, c \in \mathbb{Z}$ i $a < b$, llavors $a + c < b + c$.
- Si $a, b, c \in \mathbb{Z}$, $a < b$ i $c > 0$, llavors $ac < bc$.
- Si $a, b, c \in \mathbb{Z}$, $a < b$ i $c < 0$, llavors $ac > bc$.

Divisibilitat

La relació de divisibilitat

Siguin $a, b \in \mathbb{Z}$.

Definició

a divideix b si existeix un enter $x \in \mathbb{Z}$ tal que $ax = b$. És a dir, si $ax = b$ té solució entera en x.

- També diem: a és un *divisor* de b; b és un *múltiple* d'a; b és *divisible* per a.
- Notació: $a \mid b$. Si a no divideix b, escrivim $a \nmid b$.

Observació

0 no divideix cap enter diferent de 0.

Propietats de la relació de divisibilitat

Propietats bàsiques

1. Per a tot $a \in \mathbb{Z}$, $1 \mid a$.
2. Per a tot $a \in \mathbb{Z}$, $a \mid 0$.
3. Per a tot $a, b, c \in \mathbb{Z}$, si $a \mid b$, llavors $a \mid bc$.
4. Reflexiva: per a tot $a \in \mathbb{Z}$, $a \mid a$.
5. Transitiva: per a tot $a, b, c \in \mathbb{Z}$, si $a \mid b$ i $b \mid c$, llavors $a \mid c$.
6. Linealitat: per a tot $a, b, c \in \mathbb{Z}$, si $a \mid b$ i $a \mid c$, llavors per a tot $x, y \in \mathbb{Z}$, $a \mid bx + cy$.

Propietats de la relació de divisibilitat

Propietats addicionals

1. Si $a, b \in \mathbb{Z}$, llavors: $a \mid b \iff \pm a \mid \pm b$.
2. Si $a, b, c \in \mathbb{Z}$ i $a \mid b$, llavors $ac \mid bc$.
3. Si $a, b, c \in \mathbb{Z}$ i $ac \mid bc$ i $c \neq 0$, llavors $a \mid b$.
4. Si $a, b \in \mathbb{Z}$ i $a \mid b$ i $b \neq 0$, llavors $|a| \leq |b|$.
5. Si $a, b \in \mathbb{Z}$ i $a \mid b$ i $b \mid a$, llavors $|a| = |b|$.
6. Si $a, b \in \mathbb{Z}$ i $a \mid b$ i $a \neq 0$, llavors $\frac{b}{a} \mid b$.

Divisió euclidiana

Teorema de la divisió euclidiana

Si $a \in \mathbb{Z}$ i $b \in \mathbb{Z} - \{0\}$, aleshores existeixen enters únics q i r que satisfan:

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

Quocient i residu

Els enters q i r s'anomenen, respectivament, *el quocient* i *el residu* de la divisió entera de a per b.

Observació

No confondre el teorema de la divisió amb l'algorisme usual de la divisió!

Nombres primers i factorització d'enters

Nombres primers

Definició

- Un enter $p > 1$ és *primer* si, i només si, els únics divisors positius de p són 1 i p.
- Un nombre enter $n > 1$ és *compost* si no és primer.

Exemples

- Els primers més petits que 50 són:

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

- El primer conegut més gran (gener de 2016) és: $2^{74207281} - 1$, que té 22338618 dígits decimals.

Propietats dels nombres primers

Teorema de factorització d'enters (existència)

Tot enter $n > 1$ és un nombre primer o un producte de nombres primers.

Teorema d'Euclides

Hi ha infinits nombres primers.

Proposició

Tot enter compost N té un factor primer $p \leq \sqrt{N}$.

Test de primalitat

Sigui $N > 1$ un enter. Si per a tot primer $q \leq \sqrt{N}$ se satisfà $q \nmid N$, llavors N és primer.

Garbell d'Eratòstenes

Sigui $N > 3$ enter.

Problema

Trobar tots els primers $p \leq N$.

Garbell d'Eratòstenes

L: llista dels enters *senars* entre 3 i N.
$x \in L$ pot estar en 3 estats: marcat com a primer, està eliminat, cap dels anteriors.

1. $p =$ primer element de L no marcat com a primer ni eliminat.
2. Marquem p com a primer. Si $p > \sqrt{N}$, acabem i marquem com a primers els $x \in L$ encara no eliminats.
3. Si $p \leq \sqrt{N}$, eliminem els $x \in L$ múltiples de p. Tornem al pas 1.

Exemple

Primers < 100

Apliquem el garbell d'Eratòstenes a $N = 100$.

3	5	7	~~9~~	11	13	~~15~~	17	19	~~21~~
23	~~25~~	~~27~~	29	31	~~33~~	~~35~~	37	~~39~~	41
43	~~45~~	47	~~49~~	~~51~~	53	~~55~~	~~57~~	59	~~61~~
~~63~~	~~65~~	67	~~69~~	71	73	~~75~~	~~77~~	79	~~81~~
83	~~85~~	~~87~~	89	~~91~~	~~93~~	~~95~~	97	~~99~~	

Obtenim els primers:

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	67	71	73	79	83	89	97

El màxim comú divisor

El màxim comú divisor

Màxim comú divisor

Per definició: $\mathrm{mcd}(0, \ldots, 0) = 0$.
$d \in \mathbb{Z}$ és *el màxim comú divisor* de $a_1, \ldots, a_n \in \mathbb{Z}$ (no tots nuls) si, i només si, d satisfà:

1. d és un divisor comú dels enters $a_1, \ldots, a_n$;
2. si d' és un divisor comú de $a_1, \ldots, a_n$, aleshores $d' \leq d$.

Notació: $d = \mathrm{mcd}(a_1, \ldots, a_n)$. Observem que $d > 0$.

Enters primers entre ells

$a, b \in \mathbb{Z}$ són *primers entre ells* si, i només si, els únics divisors comuns d'a i de b són ± 1. És a dir, si $\mathrm{mcd}(a, b) = 1$.

Propietats del màxim comú divisor

Propietats

1. El màxim comú divisor d'un conjunt finit d'enters existeix i és únic.
2. El màxim comú divisor no depèn del signe:

$$\mathrm{mcd}(a,b) = \mathrm{mcd}(-a,b) = \mathrm{mcd}(a,-b) = \mathrm{mcd}(-a,-b).$$

3. $\mathrm{mcd}(a,0) = |a|$.
4. Si $a, b \in \mathbb{Z}$, $b \neq 0$ i $b \mid a$, aleshores $\mathrm{mcd}(a,b) = |b|$.
5. Si $a, b \neq 0$ i $d = \mathrm{mcd}(a,b)$, llavors $a/d, b/d$ són enters primers entre ells; és a dir: $\mathrm{mcd}(a/d, b/d) = 1$.

Teorema d'Euclides

Teorema d'Euclides

Si $a, b \in \mathbb{Z}$, aleshores $\text{mcd}(a, b) = \text{mcd}(a - b, b)$.

Conseqüència

Si $a \geq 0$ i $b > 0$ són enters i $a = bq + r$, amb $0 \leq r < b$, llavors:

$$\text{mcd}(a, b) = \text{mcd}(a - bq, b) = \text{mcd}(r, b).$$

La identitat de Bézout

Identitat de Bézout

Teorema

Si $a, b \in \mathbb{Z}$ i $d = \text{mcd}(a, b)$, aleshores existeixen enters x i y tals que:

$$d = ax + by.$$

És a dir, el màxim comú divisor de dos nombres enters és una combinació lineal, amb coeficients enters, d'aquests nombres.

Observació

Els coeficients x i y de la identitat de Bézout no són únics. Per exemple, si x i y satisfan $ax + by = d$, llavors:

$$\forall t \in \mathbb{Z} \;\; a(x - bt) + b(y + at) = d$$

Conseqüències de la identitat de Bézout

Proposició

Siguin $a, b \in \mathbb{Z}$, $d = \mathrm{mcd}(a, b)$. Si d' és un divisor comú de a i b, llavors $d'|d$.

Definició alternativa del mcd

Siguin $a, b \in \mathbb{Z}$ no nuls. Llavors $d \in \mathbb{Z}$ és el màxim comú divisor de a i b si, i només si:

1. $d|a$ i $d|b$;
2. si $d'|a$ i $d'|b$, llavors $d'|d$;
3. $d > 0$.

Associativitat del mcd

$\mathrm{mcd}(\mathrm{mcd}(a, b), c) = \mathrm{mcd}(a, \mathrm{mcd}(b, c)) = \mathrm{mcd}(a, b, c)$.

Conseqüències de la identitat de Bézout

Proposició

Siguin $a, b \in \mathbb{Z}$. Llavors: a i b són primers entre ells si, i només si, existeixen $x, y \in \mathbb{Z}$ tals que $ax + by = 1$.

Lema de Gauss

Si $a, b, c \in \mathbb{Z}$, $a \mid bc$ i $\mathrm{mcd}(a, b) = 1$, aleshores $a \mid c$.

Lema d'Euclides

Si p és un primer i a i b són enters tals que $p \mid ab$, aleshores $p \mid a$ o $p \mid b$.

L’algorisme d’Euclides

Algorisme d'Euclides

Algorisme

Siguin $a \geq 0$ i $b > 0$ enters. Aplicant el teorema de la divisió entera successives vegades, obtenim:

$$\begin{aligned}
a &= bq_1 + r_1, & q_1 &\geq 0, & 0 &\leq r_1 < b \\
b &= r_1 q_2 + r_2, & q_2 &\geq 0, & 0 &\leq r_2 < r_1 \\
&\vdots & &\vdots & &\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, & q_n &\geq 0, & 0 &\leq r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1}
\end{aligned}$$

Aleshores:

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r_1) = \mathrm{mcd}(r_1, r_2) = \cdots = \mathrm{mcd}(r_{n-1}, r_n) = r_n.$$

Algorisme d'Euclides

Organització dels càlculs

X	$x_{-1}=1$	$x_0=0$	x_1	x_2	$\dots$	x_{n-2}	x_{n-1}	$\boxed{x_n}$
Y	$y_{-1}=0$	$y_0=1$	y_1	y_2	$\dots$	y_{n-2}	y_{n-1}	$\boxed{y_n}$
Q	$-$	q_1	q_2	q_3	$\dots$	q_{n-1}	q_n	q_{n+1}
R	a	b	r_1	r_2	$\dots$	r_{n-2}	r_{n-1}	$\boxed{r_n}$
	r_1	r_2	r_3	r_4	$\dots$	$\boxed{r_n}$	0	

$$x_{-1}=1, \quad x_0=0, \quad x_{k+1}=x_{k-1}-q_{k+1}x_k,$$
$$y_{-1}=0, \quad y_0=1, \quad y_{k+1}=y_{k-1}-q_{k+1}y_k.$$

Proposició

Per a tot $k \geq 0$, se satisfà: $r_k = ax_k + by_k$. En particular:

$$r_n = \mathrm{mcd}(a,b) = ax_n + by_n$$

Algorisme d'Euclides

Exemple

Càlcul de $\mathrm{mcd}(4999, 1109)$ i de la identitat de Bézout.

X	1	0	1	-1	2	-65	$\boxed{522}$
Y	0	1	-4	5	-9	293	$\boxed{-2353}$
Q	—	4	1	1	32	8	2
R	4999	1109	563	546	17	2	$\boxed{1}$
	563	546	17	36 2	$\boxed{1}$	0	

Per tant:

$$\mathrm{mcd}(4999, 1109) = 1, \qquad 4999 \cdot 522 + 1109 \cdot (-2353) = 1.$$

El mínim comú múltiple

El mínim comú múltiple

Mínim comú múltiple

Siguin $a_1, \ldots, a_n$ enters.
Si algun dels $a_j = 0$, el mínim comú múltiple és 0, per definició.
Si tots els enters $a_1, \ldots, a_n$ són no nuls, el mínim comú múltiple és l'enter m tal que:

1. per a tot j, $a_j \mid m$;
2. si $r > 0$ i per a tot j, $a_j \mid r$, llavors $m \leq r$;
3. $m > 0$.

Notació: $\operatorname{mcm}(a_1, \ldots, a_n)$.

Propietats del mínim comú múltiple

Propietats

1. El mínim comú múltiple d'un conjunt finit d'enters existeix i és únic.
2. El mínim comú múltiple no depèn del signe:

$$\operatorname{mcm}(a,b) = \operatorname{mcm}(-a,b) = \operatorname{mcm}(a,-b) = \operatorname{mcm}(-a,-b).$$

3. Si $a, b \in \mathbb{Z}$, $b \neq 0$ i $b \mid a$, aleshores $\operatorname{mcm}(a,b) = |a|$.
4. Si $m = \operatorname{mcm}(a,b)$ i r és un múltiple comú d'a i de b, llavors $m \mid r$.
5. Associativitat:
   $\operatorname{mcm}(a,b,c) = \operatorname{mcm}(\operatorname{mcm}(a,b),c) = \operatorname{mcm}(a,\operatorname{mcm}(b,c))$.
6. Càlcul: $\operatorname{mcm}(a,b) \cdot \operatorname{mcd}(a,b) = |ab|$.

Teorema fonamental de l'aritmètica

Teorema fonamental de l'aritmètica

Teorema

Tot enter $n \geq 2$ factoritza de manera única com a producte de primers (llevat de l'ordre en què escrivim els primers.)

Corol·lari

Tot enter $n \neq 0, \pm 1$ es pot escriure de manera única com:

$$n = \epsilon \cdot p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

on $\epsilon = \pm 1$, $r \geq 1$, $a_i > 0$ i els p_i són primers diferents.

Aplicacions

Siguin $n, m \in \mathbb{Z}$, $n, m > 0$.

- Escrivim la factorització com: $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, on p_i són primers diferents i els $e_i > 0$.
- Si $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, amb $e_i > 0$, llavors els divisors positius de n són de la forma $p_1^{f_1} p_2^{f_2} \cdots p_t^{f_t}$, amb $0 \leq f_i \leq e_i$.
- El nombre de divisors positius de n és $\prod_{i=1}^{t} (e_i + 1)$.
- Si $n = p_1^{e_1} \cdots p_r^{e_r}$ i $m = p_1^{f_1} \cdots p_r^{f_r}$, on els exponents $e_i \geq 0$ i els $f_i \geq 0$, aleshores:

$$\operatorname{mcd}(n, m) = p_1^{\min(e_1, f_1)} \cdots p_r^{\min(e_r, f_r)},$$
$$\operatorname{mcm}(n, m) = p_1^{\max(e_1, f_1)} \cdots p_r^{\max(e_r, f_r)}.$$

Equacions diofàntiques

Equacions diofàntiques: l'equació $ax + by = c$

Siguin $a, b, c \in \mathbb{Z}$, $d = \text{mcd}(a, b)$.

Teorema

1. L'equació $ax + by = c$ té solució entera en x, y si, i només si, $d \mid c$.
2. Si (x_0, y_0) és una solució, llavors totes les solucions són de la forma:

$$x = x_0 - \frac{b}{d} \cdot t$$
$$y = y_0 + \frac{a}{d} \cdot t$$

on $t \in \mathbb{Z}$ és arbitrari.

Exemple

Trobeu totes les solucions enteres de $212x + 400y = 20$.

- $\mathrm{mcd}(212, 400) = 4 \mid 20$. Per tant, l'equació té solucions enteres.
- Identitat de Bézout: $400 \cdot (-9) + 212 \cdot 17 = 4$.
- Solució particular: $400 \cdot (-45) + 212 \cdot 85 = 20$.
- Solució general:

$$x = 85 - \frac{400}{4}t = 85 - 100t$$
$$y = -45 + \frac{212}{4}t = -45 + 53t$$

$t \in \mathbb{Z}$.

La relació de congruència

La relació de congruència

Nombres congruents

$m \geq 1$ enter. $a, b \in \mathbb{Z}$ són *congruents mòdul* m si $m \mid b - a$.
Notació: $a \equiv b \pmod{m}$ o bé simplement $a \equiv b\ (m)$.

És a dir:

$$\begin{aligned} a \equiv b \pmod{m} &\iff m \mid b - a \\ &\iff \exists k \in \mathbb{Z} \colon b = a + km \\ &\iff \text{residu de } a \text{ per } m = \text{residu de } b \text{ per } m. \end{aligned}$$

Exemples

- $\forall a, b \in \mathbb{Z}\ \ a \equiv b \pmod{1}$.
- $n \in \mathbb{Z}$ és parell $\iff n \equiv 0 \pmod{2}$.
  $n \in \mathbb{Z}$ és senar $\iff n \equiv 1 \pmod{2}$.

Propietats bàsiques de les congruències

Proposició

$m \geq 1$ enter. La relació de congruència mòdul m és d'equivalència a $\mathbb{Z}$. És a dir, si $a, b, c \in \mathbb{Z}$:

1. Reflexiva: $a \equiv a \pmod{m}$.
2. Simètrica: si $a \equiv b \pmod{m}$, llavors $b \equiv a \pmod{m}$.
3. Transitiva: si $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$, llavors $a \equiv c \pmod{m}$.

Congruències i operacions

Proposició

Les congruències mòdul un enter positiu m es poden sumar i multiplicar terme a terme. Concretament, si $a \equiv b \pmod{m}$ i $a' \equiv b' \pmod{m}$, llavors:

$$a + a' \equiv b + b' \pmod{m}, \qquad aa' \equiv bb' \pmod{m}.$$

Observació

En general, no es pot simplificar un factor comú dels dos membres d'una congruència. És a dir:

$$ra \equiv rb \pmod{m} \quad \text{no implica que} \quad a \equiv b \pmod{m}.$$

Contraexemple: $5 \cdot 12 \equiv 5 \cdot 18 \pmod{10}$, però $12 \not\equiv 18 \pmod{10}$.

Propietats addicionals de les congruències

Simplificació de congruències

$m > 1$ enter. Si $a, b, r \in \mathbb{Z}$ i $\text{mcd}(m, r) = 1$, aleshores:

$$ra \equiv rb \pmod{m} \iff a \equiv b \pmod{m}.$$

Per tant, només podem eliminar un factor comú en una congruència (i mantenir el mòdul) si el factor i el mòdul són primers entre ells.

Propietats addicionals de les congruències

Altres propietats

1. Si $k \geq 1$, $a \equiv b \pmod{m} \iff ak \equiv bk \pmod{mk}$.
2. Si $a \equiv b \pmod{m}$ i $d \mid m$, llavors $a \equiv b \pmod{d}$.
3. Si $a \equiv b \pmod{r}$ i $a \equiv b \pmod{s}$, aleshores $a \equiv b \pmod{m}$, on $m = \text{mcm}(r, s)$.
4. $ra \equiv rb \pmod{m} \iff a \equiv b \pmod{m/d}$, on $d = \text{mcd}(r, m)$.

Classes de congruència

Classes de congruències

Sigui $m \geq 1$ un enter.

Observacions

- La relació de congruència mòdul m és una relació d'equivalència a $\mathbb{Z}$.
- Per tant, els enters es classifiquen en classes d'equivalència, que reben el nom de *classes de congruència mòdul m*.
- Cada $a \in \mathbb{Z}$ determina una classe de congruència: $\overline{a}$.

$$\begin{aligned} \overline{a} &= \{x \in \mathbb{Z} \colon x \equiv a \pmod{m}\} \\ &= \{x \in \mathbb{Z} \colon \exists k \in \mathbb{Z},\, x = a + mk\}. \end{aligned}$$

- Tenim: $a \equiv b \pmod{m} \iff \overline{a} = \overline{b}$.

El enters modulars $\mathbb{Z}_m$

Conjunt quocient

Denotem per $\mathbb{Z}_m$ el conjunt quocient de $\mathbb{Z}$ per la relació de congruència mòdul m:

$$\mathbb{Z}_m = \{\overline{a} : a \in \mathbb{Z}\}.$$

Proposició

$\mathbb{Z}_m$ té m elements: $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$.

Exemple

$\mathbb{Z}_4$

Determinem les classes de congruència mòdul 4:

$$\overline{0} = \{x : x \equiv 0 \pmod 4\} = \{4k : k \in \mathbb{Z}\} = \{0, \pm 4, \pm 8, \ldots\}$$
$$\overline{1} = \{x : x \equiv 1 \pmod 4\} = \{4k+1 : k \in \mathbb{Z}\} = \{1, -3, 5, -7, \ldots\}$$
$$\overline{2} = \{x : x \equiv 2 \pmod 4\} = \{4k+2 : k \in \mathbb{Z}\} = \{2, -2, 6, -6, \ldots\}$$
$$\overline{3} = \{x : x \equiv 3 \pmod 4\} = \{4k+3 : k \in \mathbb{Z}\} = \{3, -1, 7, -5, \ldots\}$$

En total hi ha 4 classes de congruència mòdul 4, que es corresponen amb els possibles residus de dividir un enter per 4. És a dir:

$$\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}.$$

Operacions amb clases de congruència

Suma i producte de classes

Sigui $m \geq 2$ un enter.

Definició de suma i producte de classes

Definim la suma i el producte de classes mòdul m per les fórmules:

$$\overline{a} + \overline{b} := \overline{a + b},$$
$$\overline{a} \cdot \overline{b} := \overline{ab}.$$

Proposició

La suma i el producte de classes estan ben definides a $\mathbb{Z}_m$. És a dir, les fórmules de les definicions no depenen dels representants triats.

Propietats de les operacions de classes

Teorema

El conjunt $\mathbb{Z}_m$ és un anell amb la suma i el producte de classes.

Això vol dir que:

- la suma satisfà les propietats: associativa, commutativa, hi ha una classe neutra $\overline{0}$ i cada classe té una classe simètrica $\overline{a} + \overline{-a} = \overline{0}$;
- el producte és associatiu, commutatiu i té element neutre: $\overline{1}$;
- la suma i el producte satisfan la propietat distributiva.

En general, no podem dividir una classe per una altra; és a dir, no sempre existeix la classe inversa d'una classe respecte del producte.

Exemple

Operacions a $\mathbb{Z}_6$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Observem que $\overline{2}$ no té invers respecte del producte. És a dir, no hi ha cap classe $\overline{x} \in \mathbb{Z}_6$ tal que $\overline{2} \cdot \overline{x} = \overline{1}$. O, equivalentment, la congruència $2x \equiv 1 \pmod 6$ no té solució entera.

Per tant, $\mathbb{Z}_6$ no és un cos.

Classes invertibles

Definició

Diem que $\overline{a} \in \mathbb{Z}_m$ és *invertible* (respecte del producte) si té un invers; és a dir, si existeix $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$.

Notació

$\mathbb{Z}_m^* = \{\overline{x} \in \mathbb{Z}_m : \overline{x} \text{ és invertible}\}$.

Observació

Si una classe $\overline{a}$ és invertible, la seva classe inversa és única. La denotem per $\overline{a}^{-1}$.

Proposició

Una classe $\overline{a} \in \mathbb{Z}_m$ és invertible si, i només si, $\text{mcd}(a, m) = 1$.

Classes invertibles

Observació

Si $\overline{a} \in \mathbb{Z}_m^*$, llavors $\overline{a}^{-1}$ es pot calcular aplicant l'algorisme d'Euclides estès (identitat de Bézout) als enters a i m.

Càlcul de $\overline{6}^{-1}$ a $\mathbb{Z}_{13}$

- $\overline{6} \in \mathbb{Z}_{13}^*$, ja que $\mathrm{mcd}(6, 13) = 1$.
- Escrivim la identitat de Bézout de 6 i 13: $6 \cdot (-2) + 13 \cdot 1 = 1$.
- Per tant: $\overline{6} \cdot \overline{-2} + \overline{13} \cdot \overline{1} = \overline{1}$. És a dir: $\overline{6}^{-1} = \overline{-2} = \overline{11}$.

Quan és $\mathbb{Z}_m$ un cos?

Recordem que un cos és un anell on cada element no nul té invers respecte del producte.

Teorema

L'anell $\mathbb{Z}_m$ és un cos si, i només si, l'enter m és un nombre primer.

Observació

Si p és un nombre primer, aleshores el conjunt $\mathbb{Z}_p$ és un cos que té un nombre finit d'elements: és un *cos finit*. Per exemple: $\mathbb{Z}_2$, $\mathbb{Z}_3$ i $\mathbb{Z}_{13}$ són cossos finits. Però $\mathbb{Z}_4$, $\mathbb{Z}_6$ no són cossos (només anells).

Exponenciació modular

Teorema petit de Fermat

Teorema

Si p és primer i $p \nmid a$, llavors $a^{p-1} \equiv 1 \pmod{p}$.

O bé, en termes de classes: si $\overline{a} \in \mathbb{Z}_p$ i $\overline{a} \neq \overline{0}$, llavors $\overline{a}^{p-1} = \overline{1}$.

Demostració

- L'aplicació $f : \mathbb{Z}_p \setminus \{\overline{0}\} \to \mathbb{Z}_p \setminus \{\overline{0}\}, f(\overline{x}) = \overline{a} \cdot \overline{x}$ és bijectiva.
- Per tant, els conjunts $\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$ i $\{f(\overline{1}), f(\overline{2}), \ldots, f(\overline{p-1})\}$ són iguals.
- Fem el producte de tots els elements i ha de donar igual:

$$\overline{1} \cdot \overline{2} \cdots \overline{p-1} = \overline{a}^{p-1} \cdot \overline{1} \cdot \overline{2} \cdots \overline{p-1}$$

- D'on deduïm que $\overline{a}^{p-1} = \overline{1}$.

Exponenciació modular

Problema

Donats enters $a, n, m \geq 1$, calcular $a^n \pmod{m}$.

- Expressem l'exponent en binari: $n = n_k n_{k-1} \dots n_1 n_{0(2)}$.
- Calculem, mòdul m, els termes de la successió:

$$b_0 = a, b_1 = b_0^2 = a^2, b_2 = b_1^2 = a^{2^2}, \dots, b_k = b_{k-1}^2 = a^{2^k}.$$

- Multipliquem, mòdul m, els termes b_i tals que $n_i = 1$.

En efecte:

$$a^n = a^{\sum_{i=0}^{k} n_i 2^i} = \prod_{i=0}^{k} \left(a^{2^i}\right)^{n_i} = \prod_{i=0}^{k} b_i^{n_i}.$$

Exponenciació modular

Exemple

Calcular $23^{1690} \pmod{350}$.

- $1690 = 11010011010_{(2)}$.
- Calculem els b_i, $i = 0, \ldots, 10$, mòdul 350:

$$b_0 = 23 \qquad b_1 = 23^2 \equiv 179 \qquad b_2 \equiv 179^2 \equiv 191$$
$$b_3 \equiv 191^2 \equiv 81 \qquad b_4 \equiv 81^2 \equiv 261 \qquad b_5 \equiv 261^2 \equiv 221$$
$$b_6 \equiv 221^2 \equiv 191 \qquad b_7 \equiv 81 \qquad b_8 \equiv 261$$
$$b_9 \equiv 221 \qquad b_{10} \equiv 191$$

- Finalment:

$$\begin{aligned} 23^{1690} &= b_1 b_3 b_4 b_7 b_9 b_{10} \equiv 179 \cdot 81 \cdot 261 \cdot 81 \cdot 221 \cdot 191 \\ &\equiv 179 \cdot 81 \equiv 149 \end{aligned}$$

Teorema xinès dels residus

Teorema xinès dels residus: motivació

Problema (Sun-Tsu, segle I)

Trobeu un nombre que al dividir per 3 dóna residu 2, al dividir per 5 dóna residu 3 i al dividir per 7 dóna residu 2.

És a dir, una solució del sistema de congruències lineals:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

Teorema xinès dels residus

Teorema

Siguin $a_1, \ldots, a_k$ enters arbitraris i $m_1, \ldots, m_k$ enters positius primers entre ells dos a dos. Llavors el sistema de congruències lineals:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\ldots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

té solució en x i és única mòdul $m = m_1 \cdots m_k$.

Teorema xinès dels residus

Demostració

- Siguin $M_i = (m_1 \cdots m_k)/m_i$, $i = 1, \ldots, k$.
- $\text{mcd}(m_i, M_i) = 1 \Rightarrow M_i y \equiv 1 \pmod{m_i}$ té solució.
- Sigui y_i una solució: $M_i \cdot y_i \equiv 1 \pmod{m_i}$.
- Llavors $x = a_1 M_1 y_1 + \cdots + a_k M_k y_k$ és una solució del sistema.

Finalment, donades dues solucions x, x' del sistema, tenim:

$$\forall i : \; x \equiv x' \pmod{m_i} \Rightarrow x \equiv x' \pmod{m}$$

on $m = \text{mcm}(m_1, \ldots, m_k) = m_1 \cdots m_k$.

Teorema xinès dels residus

Exemple

El sistema següent té solució (els mòduls són primers entre ells dos a dos):

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7.$$

Organitzem els càlculs:

$M_1 = 5 \cdot 7 = 35$	$35y_1 \equiv 1 \pmod 3$	$y_1 = 2$	$a_1 = 2$
$M_2 = 3 \cdot 7 = 21$	$21y_2 \equiv 1 \pmod 5$	$y_2 = 1$	$a_2 = 3$
$M_3 = 3 \cdot 5 = 15$	$15y_2 \equiv 1 \pmod 7$	$y_3 = 1$	$a_3 = 2$

La solució del sistema és:

$$\begin{aligned} x \equiv \textstyle\sum_i a_i M_i y_i &= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \\ &= 233 \equiv 23 \pmod{105} \end{aligned}$$