4. Congruències

NOMBRES CONGRUENTS

Una de les classificacions més habituals en el conjunt $\mathbb{Z}$ dels nombres enters consisteix a considerar nombres parells i nombres senars. Aquesta partició està relacionada amb els possibles residus de la divisió entera entre 2: els nombres parells corresponen a residu 0 i els senars a residu 1. A continuació anem a generalitzar aquest tipus de particions utilitzant un divisor positiu qualsevol.

► Suposem un nombre enter $m \geq 1$. L'enter a és *congruent* amb l'enter b *mòdul* m si ambdós nombres obtenen el mateix residu de la seva divisió entera entre m. Ho denotem $a \equiv b \,(mod\, m)$.

Per exemple, $17 \equiv 22 \,(mod\, 5)$; ambdós obtenen residu 2 en la divisió per 5.

No obstant, $17 \not\equiv 22 \,(mod\, 7)$, ja que $17 = 7 \cdot 2 + 3$ i $22 = 7 \cdot 3 + 1$.

► El següent enunciat és una definició alternativa de nombres enters congruents mòdul m.

Dos nombres a, $b \in \mathbb{Z}$ són congruents mòdul m $(m \geq 1)$ si la seva diferència és múltiple de m:

$$\boxed{a \equiv b \,(mod\, m) \quad \Leftrightarrow \quad m|(a-b)}$$

Ambdues definicions són equivalents. Si els nombres a i b obtenen el mateix residu de la seva divisió per m:

$$\left.\begin{array}{l} a = m\,q_1 + r \\ b = m\,q_2 + r \end{array}\right\} \quad \Rightarrow \quad a - b = m\,(q_1 - q_2) \quad \Rightarrow \quad m|(a-b).$$

Recíprocament, si $m|(a-b)$ llavors $a - b = m\,k$ per a un determinat $k \in \mathbb{Z}$. Els nombres a i b difereixen en un múltiple de m de manera que

$$b = m\,q + r \;(0 \leq r < m) \quad \Rightarrow \quad a = b + m\,k = m\,(q+k) + r \;(0 \leq r < m)$$

i el residu de la divisió d'a i b entre m és el mateix.

Exemples

$17 \equiv 22\ (mod\, 5)$	ja que	$5\vert(-5)$	$42 \equiv 20\ (mod\, 11)$	ja que	$11\vert 22$
$17 \not\equiv 22\ (mod\, 7)$	ja que	$7 \not\vert (-5)$	$79 \not\equiv 52\ (mod\, 11)$	ja que	$11 \not\vert 27$

Propietat Per a cada enter $m \geq 1$, la relació de congruència és una relació d'equivalència definida en el conjunt $\mathbb{Z}$ dels nombres enters.

Cada nombre és congruent amb ell mateix (propietat reflexiva). Si un nombre és congruent amb un altre, aquest ho és amb el primer (propietat simètrica). Si un primer nombre és congruent amb un segon i aquest amb un tercer, el primer ho és amb el tercer (propietat transitiva). Aquestes tres propietats són les que caracteritzen una relació d'equivalència.

► Tota relació d'equivalència estableix una partició en classes sobre el conjunt en el qual està definida. A la relació d'equivalència *congruent mòdul* m trobem m classes, tantes com possibles residus de la divisió entera per m:

$$0,\ 1,\ 2,\ \ldots\ , m-1.$$

Triem com a *representant canònic* de cada classe el residu comú de la divisió per m. Denotem cada classe mitjançant $\overline{r}$ $(0 \leq r \leq m-1)$.

Exemple Classes d'equivalència en $\mathbb{Z}$ segons la congruència mòdul 2.

$$\overline{0} = \{\ldots,\ -4,\ -2,\ 0,\ 2,\ 4,\ 6,\ \ldots\}$$
$$\overline{1} = \{\ldots,\ -3,\ -1,\ 1,\ 3,\ 5,\ 7,\ \ldots\}$$

La classe de 0 està formada per tots els enters que en la divisió per 2 obtenen residu 0: són els nombres parells. La classe de 1 està formada pels de residu 1: són els senars.

Exemple Classes d'equivalència en $\mathbb{Z}$ segons la congruència mòdul 5.

$$\overline{0} = \{\ldots, -10,\ -5,\ 0,\ 5,\ 10,\ 15,\ \ldots\}$$
$$\overline{1} = \{\ldots,\ -9,\ -4,\ 1,\ 6,\ 11,\ 16,\ \ldots\}$$
$$\overline{2} = \{\ldots,\ -8,\ -3,\ 2,\ 7,\ 12,\ 17,\ \ldots\}$$
$$\overline{3} = \{\ldots,\ -7,\ -2,\ 3,\ 8,\ 13,\ 18,\ \ldots\}$$
$$\overline{4} = \{\ldots,\ -6,\ -1,\ 4,\ 9,\ 14,\ 19,\ \ldots\}$$

La classe de 0 està formada per tots els enters la divisió dels quals entre 5 és exacta: són els múltiples de 5. Les restants classes són múltiples de 5 més 1, més 2, més 3 o més 4. És a dir:

$$\overline{0} = \{5\,t,\ \forall\, t \in \mathbb{Z}\},\ \overline{1} = \{5\,t+1,\ \forall\, t \in \mathbb{Z}\},\ \ldots\ ,\overline{4} = \{5\,t+4,\ \forall\, t \in \mathbb{Z}\}.$$

► Com a tota relació d'equivalència podem considerar el conjunt de les classes segons les diferents congruències mòdul m, per a cada $m \geq 1$. Designem mitjançant $\mathbb{Z}/m$ cadascun d'aquests conjunts.

$$\mathbb{Z}/2 = \{\,\overline{0},\,\overline{1}\,\},\quad \mathbb{Z}/3 = \{\,\overline{0},\,\overline{1},\,\overline{2}\,\},\quad \mathbb{Z}/4 = \{\,\overline{0},\,\overline{1},\,\overline{2},\,\overline{3}\,\},$$

$$\mathbb{Z}/5 = \{\,\overline{0},\,\overline{1},\,\overline{2},\,\overline{3},\,\overline{4}\,\},\quad \mathbb{Z}/6 = \{\,\overline{0},\,\overline{1},\,\overline{2},\,\overline{3},\,\overline{4},\,\overline{5}\,\},\ \ldots$$

La següent propietat permet definir una suma i un producte a cada conjunt $\mathbb{Z}/m$. Operant un element qualsevol d'una classe amb un altre element qualsevol d'una altra classe s'obté com a resultat nombres que estan en una mateixa classe, tant per a la suma com per al producte.

Propietat Suposem un enter qualsevol $m \geq 1$.

$$\left.\begin{array}{l} a \equiv b\ (mod\, m) \\ c \equiv d\ (mod\, m) \end{array}\right\} \quad \Rightarrow \quad \left\{\begin{array}{lll} \text{(i)} & a+c \equiv b+d & (mod\, m) \\ \text{(ii)} & a\,c \equiv b\,d & (mod\, m) \end{array}\right.$$

Demostració. Segons la definició, les condicions de l'enunciat equivalen a $m|(a-b)$ i $m|(c-d)$, és a dir, $a-b = m\,s$ i $c-d = m\,t$, per a determinats $s,\ t \in \mathbb{Z}$.

(i) $(a+c)-(b+d) = a-b+c-d = m\,(s+t) \ \Rightarrow\ a+c \equiv b+d\ (mod\, m)$.

(ii) Per a provar $a\,c \equiv b\,d\ (mod\, m)$, la seva diferència ha de ser múltiple de m:

$$a\,c - b\,d = a\,c - b\,c + b\,c - b\,d = (a-b)\,c + b\,(c-d) = m\,(s\,c + b\,t).$$

Exemple Comprovem la propietat anterior en $\mathbb{Z}/5$ prenent dues parelles de nombres congruents entre sí.

$$\left.\begin{array}{l} 17 \equiv 2\ (mod\, 5) \\ 29 \equiv 4\ (mod\, 5) \end{array}\right\} \quad \Rightarrow \quad \left\{\begin{array}{ll} \text{Suma:} & 46 \equiv 6 \equiv 1\ (mod\, 5) \\ \text{Producte:} & 493 \equiv 8 \equiv 3\ (mod\, 5) \end{array}\right.$$

OPERACIONS EN $\mathbb{Z}/\mathbf{m}$

▶ Podem definir una suma i un producte entre les classes segons cada relació de congruència mòdul m. El resultat no depèn del representant triat. Per aquest motiu convé prendre els representants més senzills, és a dir, els canònics.

▶ Fixat un enter $m \geq 1$, per comoditat, denotem els elements de $\mathbb{Z}/m$ sense la barra de la classe. No obstant, cadascun dels seus elements representa a la totalitat de la classe.

$$\mathbb{Z}/m = \{\, 0,\, 1,\, 2,\, \ldots\, , m-1 \,\}.$$

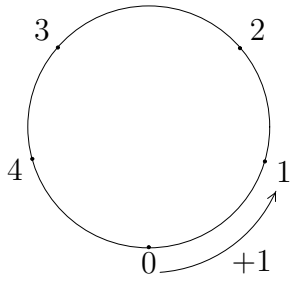
Taules de les operacions suma i producte en $\mathbb{Z}/5$

Utilitzem els cinc representants de les classes mòdul 5 per tal de completar la taula de les operacions suma i producte. S'operen els representants i es busca la classe del resultat.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}/5$



La suma compleix les mateixes propietats que la suma en $\mathbb{Z}$: associativa, commutativa, element neutre (classe 0) i element oposat. L'oposat de 1 és 4 ($1 + 4 = 0$ en $\mathbb{Z}/5$), l'oposat de 2 és 3 ($2 + 3 = 0$ en $\mathbb{Z}/5$), ...

El producte compleix propietats com el producte en $\mathbb{Z}$: associativa, commutativa, element neutre (classe 1) i distributiva respecte la suma.

► Una altra propietat que pot complir el producte definit en un determinat conjunt A és l'existència d'*element invers*. Si 1 representa el neutre del producte en A,

$$\boxed{a \in A \text{ té invers } \Leftrightarrow \exists\, a^{-1} \in A \,/\, a\, a^{-1} = 1}$$

El producte en $\mathbb{Z}$ no compleix, en general, la propietat de l'element invers. Només són invertibles en $\mathbb{Z}$ els nombres 1 i -1.

En $\mathbb{Z}/5$ cadascun dels seus elements, excepte el neutre de la suma 0, posseeix element invers:

$$\forall\, n \in (\mathbb{Z}/5)^* \;\exists\, n^{-1} \in (\mathbb{Z}/5)^* \,/\, n\, n^{-1} = 1.$$

En particular:

$$1^{-1} = 1 \;\; (1 \cdot 1 = 1); \quad 2^{-1} = 3,\, 3^{-1} = 2 \;\; (2 \cdot 3 = 1); \quad 4^{-1} = 4 \;\; (4 \cdot 4 = 1).$$

Taules de les operacions suma i producte en $\mathbb{Z}/6$

Com en el cas anterior, utilitzem els sis representants de les classes mòdul 6 per tal de formar les dues taules.

$+$	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

La taula de la suma en $\mathbb{Z}/6$ no presenta diferències essencials amb la taula de la suma en $\mathbb{Z}/5$. L'element neutre de la suma en $\mathbb{Z}/6$ és la classe de 0.

La simetria de les taules respecte la diagonal principal equival a la commutativitat de les operacions.

La taula del producte en $\mathbb{Z}/6$ és radicalment diferent a la del producte en $\mathbb{Z}/5$. A les línies de la taula del producte en $\mathbb{Z}/6$ observem elements repetits, a la vegada que alguns nombres no apareixen com a resultats.

A les files o columnes corresponents a 2, 3 i 4 no apareix com a resultat 1, que és el neutre del producte. Això suposa que 2, 3 i 4 no tenen invers per a aquesta operació. Només tenen invers el propi neutre 1 i el 5:

$$1 \cdot 1 = 1, \quad 5 \cdot 5 = 1.$$

Analitzant la taula del producte, els nombres 2, 3, $4 \neq 0$ presenten 0 a les seves files o columnes, encara que l'altre factor no sigui 0. En concret:

$$2 \cdot 3 = 3 \cdot 2 = 0, \qquad 3 \cdot 4 = 4 \cdot 3 = 0.$$

► En un conjunt numèric dotat de suma i producte on 0 representa el neutre de la suma, es diu que dos nombres a i b són *divisors de zero* si

$$\boxed{a\,b = 0 \quad \text{però} \quad a,\, b \neq 0}$$

La situació dels elements pel producte és diferent en els conjunts $\mathbb{Z}/m$ que hem considerat.

- En $(\mathbb{Z}/5)^*$ tots els seus elements són invertibles i no hi ha divisors de zero.

- En $(\mathbb{Z}/6)^*$: 1, 5 són invertibles i 2, 3, 4 són divisors de zero.

Les següents propietats mostren quan succeeix una cosa o una altra.

Propietat Suposem un enter $m \geq 2$.

$$a \in (\mathbb{Z}/m)^* \text{ es invertible} \quad \Leftrightarrow \quad mcd(a,\, m) = 1$$

($\Rightarrow$) Si $a \neq 0$ és invertible en $\mathbb{Z}/m$ existeix un element $a' \in \mathbb{Z}/m$ tal que $a\,a' = 1$, és a dir, $a\,a' \equiv 1\ (mod\, m)$:

$$a\,a' - 1 = m\,k \text{ per a determinat } k \in \mathbb{Z} \quad \Rightarrow \quad a\,a' + m\,(-k) = 1.$$

Com que 1 és combinació lineal entera d'a i m, podem afirmar, per la identitat de Bezout, que $mcd(a,\, m) = 1$.

($\Leftarrow$) Per la identitat de Bezout, si a i m són primers entre sí existeixen dos nombres enters x i y tals que: $a\,x + m\,y = 1$.

Prenent classes mòdul m: $\overline{a}\,\overline{x} + \overline{m}\,\overline{y} = \overline{1}$.

Però $\overline{m} = \overline{0}$, d'on, $\overline{a}\,\overline{x} = \overline{1}$: a és invertible en $\mathbb{Z}/m$) i $a^{-1} = x$.

Propietat Suposem un enter $m \geq 2$.

Si $a \in (\mathbb{Z}/m)^*$ i $mcd(a,\, m) = d \neq 1$, llavors a és divisor de zero en $\mathbb{Z}/m$.

Suposem ara que a i m no són primers entre sí: $mcd(a,\, m) = d \neq 1$. Existeixen dos nombres enters no nuls q_1 i q_2 tals que $a = d\,q_1$ i $m = d\,q_2$.

Multiplicant la segona igualtat per q_1 i substituint amb a:

$$m\,q_1 = d\,q_2\,q_1 = a\,q_2$$

Prenent classes mòdul m, $\overline{0} = \overline{a}\,\overline{q}_2$, la qual cosa equival a $a\,q_2 = 0$ en $\mathbb{Z}/m$ i a és divisor de zero.

Exemple En $\mathbb{Z}/8$: 1, 3, 5, 7 són invertibles; 2, 4, 6 són divisors de zero.

$$1^{-1} = 1; \quad 3^{-1} = 3\ (3\cdot 3 = 1); \quad 5^{-1} = 5\ (5\cdot 5 = 1); \quad 7^{-1} = 7\ (7\cdot 7 = 1);$$

$$2\cdot 4 = 4\cdot 2 = 0; \qquad 4\cdot 6 = 6\cdot 4 = 0.$$

► Si p és primer, tots els elements de $(\mathbb{Z}/p)^*$ són invertibles.

Un conjunt amb dues operacions es diu que té estructura de *cos* si, a més a més de complir les set propietats com la suma i el producte en $\mathbb{Z}$, tot element diferent del neutre de la suma té invers per al producte.

$$\boxed{\mathbb{Z}/p \text{ és cos } \forall\, p \text{ primer}}$$

► Si m és compost, $\mathbb{Z}/m$ no és cos ja que té divisors de zero i aquests no són invertibles. Els elements 1 i $m-1$ són invertibles en $\mathbb{Z}/m$ per a qualsevol $m \geq 1$ ja que 1 i $m-1$ són sempre primers amb m.

RESOLUCIÓ DE CONGRUÈNCIES

Resoldre congruències consisteix a resoldre equacions on les incògnites són elements pertanyents a algun conjunt $\mathbb{Z}/m$ $(m \geq 1)$.

Considerem la congruència multiplicativa

$$\boxed{a\,x \equiv b\ (mod\, m)}$$

Propietat Si anomenem $d = mcd(a,\, m)$.

(i) La congruència $a\,x \equiv b\ (mod\, m)$ té solució si i només si $d|b$.

(ii) Si té solució, el nombre de solucions de $a\,x \equiv b\ (mod\, m)$ és d.

Demostració. Provem que resoldre la congruència $a\,x \equiv b\ (mod\, m)$ equival a resoldre l'equació diofàntica lineal

$$a\,x + m\,y = b \qquad (*)$$

Si x_0 és solució de la congruència, $a\,x_0 \equiv b\ (mod\, m)$,

$$a\,x_0 - b = m\,k,\ \text{ per a cert } k \in \mathbb{Z} \ \Rightarrow\ a\,x_0 + m\,(-k) = b.$$

Queda provat que $(x_0,\, -k)$ és solució de l'equació diofàntica $(*)$.

Recíprocament, si $(x_0,\, y_0)$ és solució de l'equació $(*)$:

$$a\,x_0 + m\,y_0 = b.$$

Aleshores, $a\,x_0 - b = m\,(-y_0)$, d'on, $a\,x_0 \equiv b\ (mod\, m)$.

(i) Havíem provat que la condició necessària i suficient per tal que l'equació diofàntica lineal $(*)$ tingui solució és que $d|b$, sent $d = mcd(a,\, m)$. L'equivalència entre la resolució de l'equació diofàntica i la congruència prova que el criteri de resolució és el mateix.

(ii) Si $(x_0,\, y_0)$ és una solució particular de $(*)$, la seva solució general és

$$(x,\, y) = (\, x_0 + m\,t/d,\, y_0 - a\,t/d\,) \quad \forall\, t \in \mathbb{Z}.$$

Per a cada t amb $0 \le t < d$ provem que s'obté una solució diferent de la congruència $a\,x \equiv b\ (mod\, m)$.

Si dos nombres t_1 i t_2 amb $0 \le t_1 < t_2 < d$ donessin lloc a solucions iguals en $\mathbb{Z}/m$:

$$(\, x_0 + m\,t_1/d\,) - (\, x_0 + m\,t_2/d\,) = m\,k.$$

Llavors $m\,(t_1 - t_2) = d\,m\,k$ ens porta a $t_1 - t_2 = d\,k$, és a dir, $d|(t_1 - t_2)$, la qual cosa és impossible. Això garanteix d solucions diferents.

Veiem que no hi ha més solucions. Considerem un nombre t tal que $t \ge d$ ó $t < 0$. Per l'algorisme de la divisió entera $t = d\,q + r$ amb $0 \le r < d$. La solució corresponent

$$x_0 + m\,t/d = x_0 + m\,(d\,q + r)/d = x_0 + m\,r/d + m\,q$$

es diferencia de la solució per a $t = r$ en un múltiple de m: pertany a la mateixa classe en $\mathbb{Z}/m$, llavors és la mateixa solució.

Exemple Resoldre la congruència $3\,x - 2 \equiv 4\ (mod\, 5)$.

En primer lloc sumem 2 a ambdós membres per transformar-la en una congruència multiplicativa.

$$3\,x - 2 + 2 \equiv 4 + 2\ (mod\, 5) \quad \Rightarrow \quad 3\,x \equiv 1\ (mod\, 5).$$

Com que $mcd(3,\,5) = 1$ i $1|1$, segons la propietat anterior, la congruència té una única solució. Per a aïllar x multipliquem ambdós membres per l'invers de 3 en $\mathbb{Z}/5$: $3^{-1} = 2$:

$$2 \cdot 3\,x \equiv 2 \cdot 1\ (mod\,5) \quad \Rightarrow \quad x \equiv 2\ (mod\,5).$$

La solució és $x \equiv 2\ (mod\,5)$ o equivalentment: $x = 2 + 5\,t,\ \forall\, t \in \mathbb{Z}$.

► Les congruències mòdul qualsevol primer p sempre tenen solució única, ja que $mcd(a,\,p) = 1$ per a $0 < a < p$. Per resoldre-les no s'acostuma a passar a l'equació diofàntica associada sinó que es determina l'invers del coeficient a en $\mathbb{Z}/p$.

Exemple Resoldre la congruència $3\,x + 1 \equiv 4\ (mod\,6)$.

La transformem en congruència multiplicativa:

$$3\,x + 1 - 1 \equiv 4 - 1\ (mod\,6) \quad \Rightarrow \quad 3\,x \equiv 3\ (mod\,6)$$

En aquest cas $mcd(3,\,6) = 3$ i $3|3$. La congruència té tres solucions. El nombre 3 no té invers en $\mathbb{Z}/6$. Si mirem la fila del 3 a la taula de multiplicar en $\mathbb{Z}/6$ podem obtenir les solucions:

$$x \equiv 1\ (mod\,6), \quad x \equiv 3\ (mod\,6), \quad x \equiv 5\ (mod\,6).$$

Les tres solucions poden expressar-se com a $x = 1 + 2\,t,\ \forall\, t \in \mathbb{Z}$.

Exemple Resoldre la congruència $3\,x + 5 \equiv 1\ (mod\,6)$.

Operant, $3\,x + 5 - 5 \equiv 1 - 5\ (mod\,6)$ dóna lloc a $3\,x \equiv 2\ (mod\,6)$.

En aquest cas $mcd(3,\,6) = 3$, però $3 \not| 2$. La congruència no té solució.

Exemple Resoldre la congruència $x^2 - x \equiv 0\ (mod\,7)$.

Estem buscant solucions en $\mathbb{Z}/7$ on no hi ha divisors de 0 ja que 7 és un nombre primer. En aquest cas:
$x^2 - x \equiv 0\ (mod\,7);\ x\,(x-1) \equiv 0\ (mod\,7)\ \Rightarrow\ x \equiv 0\ (mod\,7)$ ó $x \equiv 1\ (mod\,7)$.

Exemple Resoldre la congruència $x^2 - x \equiv 0\ (mod\,6)$.

La situació en aquest cas és diferent al cas anterior. En $\mathbb{Z}/6$ existeixen divisors de 0, ja que 6 no és primer. Un producte igualat a 0 no implica que cap dels seus factors sigui nul.

Si $x^2 - x \equiv 0 \ (mod\, 6)$, és a dir, $x\,(x-1) \equiv 0 \ (mod\, 6)$ pot passar:

(i) $\mathbf{x \equiv 0 \ (mod\, 6)}$

(ii) $x - 1 \equiv 0 \ (mod\, 6) \qquad \mathbf{x \equiv 1 \ (mod\, 6)}$

(iii) $\left\{ \begin{array}{l} x \equiv 2 \ (mod\, 6) \\ x - 1 \equiv 3 \ (mod\, 6) \end{array} \right. \qquad \left\{ \begin{array}{l} x \equiv 2 \ (mod\, 6) \\ x \equiv 4 \ (mod\, 6) \end{array} \right.$ no hi ha solució

(iv) $\left\{ \begin{array}{l} x \equiv 3 \ (mod\, 6) \\ x - 1 \equiv 2 \ (mod\, 6) \end{array} \right. \qquad \mathbf{x \equiv 3 \ (mod\, 6)}$

(v) $\left\{ \begin{array}{l} x \equiv 3 \ (mod\, 6) \\ x - 1 \equiv 4 \ (mod\, 6) \end{array} \right. \qquad \left\{ \begin{array}{l} x \equiv 3 \ (mod\, 6) \\ x \equiv 5 \ (mod\, 6) \end{array} \right.$ no hi ha solució

(vi) $\left\{ \begin{array}{l} x \equiv 4 \ (mod\, 6) \\ x - 1 \equiv 3 \ (mod\, 6) \end{array} \right. \qquad \mathbf{x \equiv 4 \ (mod\, 6)}$

Exemple Resoldre el sistema de congruències lineals

$$\left. \begin{array}{l} 2\,x + 3\,y \equiv 5 \ (mod\, 7) \\ 3\,x - 5\,y \equiv 2 \ (mod\, 7) \end{array} \right\}$$

Es pot eliminar tots els negatius utilitzant nombres entre 1 i 6. El sistema queda:

$$\left. \begin{array}{l} 2\,x + 3\,y \equiv 5 \ (mod\, 7) \\ 3\,x + 2\,y \equiv 2 \ (mod\, 7) \end{array} \right\}$$

► S'utilitza reducció per a resoldre sistemes de congruències lineals.

Multipliquem la primera congruència per 3 i la segona per 2 per tal d'eliminar la incògnita x restant.

$$\left. \begin{array}{l} 3 \cdot (2\,x + 3\,y) \equiv 3 \cdot 5 \ (mod\, 7) \\ 2 \cdot (3\,x + 2\,y) \equiv 2 \cdot 2 \ (mod\, 7) \end{array} \right\} \quad \Rightarrow \quad \left. \begin{array}{l} 6\,x + 2\,y \equiv 1 \ (mod\, 7) \\ 6\,x + 4\,y \equiv 4 \ (mod\, 7) \end{array} \right\}$$

Aleshores, $2\,y \equiv 3 \ (mod\, 7)$. Com l'invers de 2 en $\mathbb{Z}/7$ és 4:

$$4 \cdot 2\,y \equiv 4 \cdot 3 \ (mod\, 7) \quad \Rightarrow \quad y \equiv 5 \ (mod\, 7)$$

Una vegada obtinguda la incògnita y substituïm el seu valor en una de les equacions per tal de determinar la incògnita x:

$$2\,x + 3 \cdot 5 \equiv 5 \ (mod\, 7) \ \Rightarrow \ 2\,x + 1 \equiv 5 \ (mod\, 7) \ \Rightarrow \ 2\,x \equiv 4 \ (mod\, 7).$$

Multiplicant novament per $2^{-1} = 4$ en $\mathbb{Z}/7$:

$$x \equiv 2 \ (mod\, 7).$$

La solució del sistema és $x \equiv 2 \ (mod\, 7)$, $y \equiv 5 \ (mod\, 7)$. Aquesta solució també pot expressar-se mitjançant tots els nombres solució en $\mathbb{Z}$:

$$(x,\, y) = (\, 2 + 7\, t,\, 5 + 7\, t'\,) \quad \forall\, t,\ t' \in \mathbb{Z}.$$

Exemple Resoldre el sistema de congruències lineals

$$\left.\begin{array}{l} 5\, x - 4\, y \equiv \ \ 7 \ (mod\, 11) \\ 3\, x + 9\, y \equiv -1 \ (mod\, 11) \end{array}\right\}$$

Posem tots els nombres en positiu i reduïm per tal d'eliminar x.

$$\left.\begin{array}{l} 5\, x + 7\, y \equiv \ \ 7 \ (mod\, 11) \\ 3\, x + 9\, y \equiv 10 \ (mod\, 11) \end{array}\right\} \quad \Rightarrow \quad \left.\begin{array}{l} 4\, x + 10\, y \equiv 10 \ (mod\, 11) \\ 4\, x + \quad y \equiv \ \ 6 \ (mod\, 11) \end{array}\right\}$$

Restant, $9\, y \equiv 4 \ (mod\, 11)$. En $\mathbb{Z}/11$, $9^{-1} = 5$, aleshores $y \equiv 9 \ (mod\, 11)$.

Substituint a la primera congruència:

$$5\, x + 8 \equiv 7 \ (mod\, 11) \ \ \Rightarrow \ \ 5\, x \equiv 10 \ (mod\, 11) \ \ \Rightarrow \ \ x \equiv 9 \cdot 10 \equiv 2 \ (mod\, 11).$$

La solució del sistema és: $x \equiv 2 \ (mod\, 11)$, $y \equiv 9 \ (mod\, 11)$.

► Un problema clàssic de congruències consisteix a determinar el residu de la divisió entera quan el nombre és una potència.

Exemple tipus Determinar el residu de la divisió de 23^{84292} entre 7.

El valor exacte del nombre 23^{84292} és difícil de calcular i el residu de la divisió entera entre 7 seria difícil de determinar. Utilitzant propietats de les congruències, el residu es calcula amb uns quants passos d'operació.

L'enunciat equival a resoldre $23^{84292} \equiv x \ (mod\, 7)$.

Els nombres congruents compleixen:

$$\left.\begin{array}{l} a \equiv b \ (mod\, m) \\ c \equiv d \ (mod\, m) \end{array}\right\} \quad \Rightarrow \quad a\, c \equiv b\, d \ (mod\, m)$$

En particular, $a \equiv b \ (mod\, m) \Rightarrow a^2 \equiv b^2 \ (mod\, m) \Rightarrow a^3 \equiv b^3 \ (mod\, m)$, ...

Utilitzem aquest resultat buscant nombres congruents a les successives potències de la base 23 fins a obtenir un resultat senzill: 1 ó -1.

$$23 \equiv 2 \ (mod\, 7); \quad 23^2 \equiv 2^2 \equiv 4 \ (mod\, 7); \quad 23^3 \equiv 2^3 \equiv 1 \ (mod\, 7).$$

Cada producte de tres nombres 23 és congruent amb 1 mòdul 7. Agrupem de tres en tres l'exponent 84292 utilitzant la divisió entera:

$$84292 = 3 \cdot 28097 + 1$$

Llavors, $23^{84292} = 23^{3 \cdot 28097+1} = (23^3)^{28097}\, 23^1 \equiv 1^{28097}\, 2 \equiv 2 \ (mod\, 7)$.

El residu de la divisió entera de 23^{84292} entre 7 és 2.

Exemple Determinar el residu de la divisió de 17^{29318} entre 23.

Sense calcular les potències de 17, determinem amb quins nombres són congruents fins obtenir un 1 o un -1.

$$\begin{aligned}
&17^1 \equiv 17 \equiv -6 && (mod\, 23)\\
&17^2 \equiv (-6) \cdot (-6) \equiv 13 && (mod\, 23)\\
&17^3 \equiv 17 \cdot 13 \equiv 14 \equiv -9 && (mod\, 23)\\
&17^4 \equiv 13 \cdot 13 \equiv 8 && (mod\, 23)\\
&17^5 \equiv 17 \cdot 8 \equiv 21 \equiv -2 && (mod\, 23)\\
&17^6 \equiv (-9) \cdot (-9) \equiv 12 && (mod\, 23)\\
&\ldots\\
&17^{11} \equiv (-2) \cdot 12 \equiv -1 && (mod\, 23)
\end{aligned}$$

Dividim l'exponent 29318 entre 11: $29318 = 11 \cdot 2665 + 3$.

$$17^{29318} = 17^{11 \cdot 2665+3} = (17^{11})^{2665}\, 17^3 \equiv (-1) \cdot 14 \equiv 9 \ (mod\, 23).$$

El residu de la divisió entera de 17^{29318} entre 23 és 9.

▶ La determinació d'un nombre congruent amb les successives potències i que sigui menor que el mòdul pot ser laboriosa. D'entrada, es desconeix el nombre de potències necessàries fins a obtenir un 1 o un -1 en aquest desenvolupament. A la següent secció s'obtenen resultats que sistematitzen el procés.

LA FUNCIÓ D'EULER

La *funció d'Euler* és una aplicació $\phi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ que a cada natural $n \geq 1$ li fa correspondre el nombre d'enters x, $1 \leq x \leq n$, tals que x i n són primers entre sí.

$$\boxed{\phi(n) = card\{\ x\ /\ 1 \leq x \leq n\ \wedge\ mcd(x,n) = 1\}}$$

► Si p és un nombre primer, llavors $\phi(p) = p - 1$. Per definició, $\phi(1) = 1$.

► Valors de $\phi(n)$ per a n petit:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

► El valor de la funció $\phi(n)$ és igual al nombre d'invertibles en $\mathbb{Z}/n$.

Per exemple, $\phi(9) = 6$ i en $\mathbb{Z}/9$ els invertibles són: 1, 2, 4, 5, 7, 8.

Propietat Per a qualsevol natural $n \geq 1$ es verifica:

$$\sum_{d|n} \phi(d) = n.$$

Exemple Els divisors del nombre $12 = 2^2 \cdot 3$ són: 1, 2, 3, 4, 6, 12.

$$\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$$

Propietat Si p és primer, llavors $\phi(p^m) = p^m - p^{m-1}$.

Demostració. Contem els nombres que no són primers amb p^m:

$$p,\ 2\,p,\ 3\,p,\ \ldots\ ,\ p\,p,\ (p+1)\,p,\ \ldots\ ,\ p^2\,p,\ (p^2+1)\,p,\ \ldots\ldots\ldots,\ p^{m-1}\,p.$$

Llavors, els nombres primers amb p^m són $p^m - p^{m-1}$ i $\phi(p^m) = p^m - p^{m-1}$.

Per al cas general d'un nombre enter n ($n \geq 2$), sabem que existeix una factorització única en producte de primers. A partir d'aquesta propietat es pot oferir una expressió per al càlcul de la funció d'Euler d'un nombre qualsevol tal i com s'estableix en el següent resultat.

Teorema Suposem un nombre natural $n \geq 2$ que factoritza en la forma $n = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ amb $p_1 < p_2 < \cdots < p_t$ nombres primers. Aleshores:

$$\boxed{\phi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_t}\right)}$$

Exemple Càlcul de la funció d'Euler per al nombre 720. La descomposició en factors primers és $720 = 2^4 \cdot 3^2 \cdot 5$. Aplicant el teorema:

$$\phi(720) = 720 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 720 \frac{1}{2} \frac{2}{3} \frac{4}{5} = 192\,.$$

Exemple Valor de la funció d'Euler d'un nombre p^m amb p primer.

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

► El següent teorema estableix la congruència amb 1 per a potències de nombres mitjançant la funció d'Euler del mòdul.

Teorema d'Euler Suposem a, $m \geq 1$.

$$\boxed{\text{Si} \quad mcd(a,\, m) = 1 \quad \text{aleshores} \quad a^{\phi(m)} \equiv 1 \; (mod\, m)}$$

Exemple Determinar el residu de la divisió de 77^{13262} entre 169.

Amb el Teorema d'Euler no necessitem provar potències fins a obtenir una congruència amb 1 mòdul 169. Només cal calcular la funció d'Euler de 169.

$$169 = 13^2 \quad \Rightarrow \quad \phi(169) = 13^2 - 13 = 156.$$

Com que és $mcd(77,\, 169) = 1$, pel Teorema d'Euler, $77^{156} \equiv 1 \; (mod\, 169)$.

Dividint l'exponent entre 156, $13262 = 156 \cdot 85 + 2$, obtenim:

$$77^{13262} = 77^{156 \cdot 85 + 2} \equiv 77^2 \equiv 14 \; (mod\, 169).$$

El residu de la divisió entera de 77^{13262} entre 169 és 14.

Petit Teorema de Fermat Suposem p primer.

$$\boxed{\text{Si} \quad mcd(a,\, p) = 1 \quad \text{aleshores} \quad a^{p-1} \equiv 1 \; (mod\, p)}$$

► Aquesta propietat és conseqüència del Teorema d'Euler quan el mòdul és un nombre primer p, en aquest cas $\phi(p) = p - 1$.

Exemple tipus Determinar el residu de la divisió de 23^{84292} entre 7.

Ara el mòdul és un primer, 7. Com que $mcd(23, 7) = 1$, el Petit Teorema de Fermat afirma que

$$23^6 \equiv 1 \ (mod\, 7).$$

Aquest exemple ens permet comprovar que el valor de l'exponent que ofereix el teorema no té perquè ser el menor. Sabem que $23^3 \equiv 1 \ (mod\, 7)$, però aquest resultat s'havia obtingut per càlcul de potències.

Ara, $84292 = 6 \cdot 14048 + 4$, d'on,

$$23^{84292} = 23^{6 \cdot 14048+4} = (23^6)^{14048}\, 23^4 \equiv 2^4 \equiv 2 \ (mod\, 7)$$

Exemple Determinar el residu de la divisió de 2^{290} entre 289.

El nombre 289 factoritza com a 17^2, així doncs $\phi(289) = 17^2 - 17 = 272$.

Com que $mcd(2, 289) = 1$, pel Teorema de Fermat, $2^{272} \equiv 1 \ (mod\, 289)$.

$$2^{290} = 2^{272+18} \equiv 2^{18} \ (mod\, 289)$$

D'entre les primeres potències de 2, la que pren un valor més pròxim al mòdul és $2^8 = 256 \equiv -33 \ (mod\, 289)$. Aleshores,

$$2^{18} = 2^{8 \cdot 2+2} \equiv (-33)^2 \cdot 4 \equiv 1089 \cdot 4 \equiv 21 \ (mod\, 289).$$

El residu de la divisió entera de 2^{290} entre 289 és 21.

CRITERIS DE DIVISIBILITAT

La determinació de criteris de divisibilitat en un sistema de numeració posicional és una conseqüència de les congruències de les potències de la base del sistema de numeració. El nostre sistema de numeració és decimal, això és, de base 10. Cada nombre s'escriu utilitzant les xifres o dígits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

Per a denotar un enter $n \geq 1$ mitjançant les seves xifres utilitzem la notació:

$$n = (x_k \cdots x_3 x_2 x_1 x_0)_{10} = x_0 + x_1\, 10^1 + x_2\, 10^2 + x_3\, 10^3 + \cdots + x_k\, 10^k$$

Per exemple, $(7459)_{10} = 9 + 5 \cdot 10^1 + 4 \cdot 10^2 + 7 \cdot 10^3$.

► Un enter $n \geq 1$ és divisible per m $(m \geq 1)$ si i només si $n \equiv 0 \ (mod\, m)$.

$$\boxed{m|n \ \Leftrightarrow \ n = x_0 + x_1\, 10^1 + x_2\, 10^2 + x_3\, 10^3 + \cdots + x_k\, 10^k \equiv 0 \ (mod\, m)}$$

Qualsevol nombre enter en el sistema decimal és una combinació lineal entera de potències de 10. Un criteri de divisibilitat entre m requereix conèixer les congruències de 10^i mòdul m $(i \geq 0)$.

• Criteri de divisibilitat entre 2

$$1 \equiv 1 \ (mod\, 2);\ 10^1 \equiv 0 \ (mod\, 2);\ 10^2 \equiv 0 \ (mod\, 2);\ \ldots$$

El nombre $n = (x_k \cdots x_3 x_2 x_1 x_0)_{10}$ és divisible entre 2 sii

$$x_0 \equiv 0 \ (mod\, 2) \ \Leftrightarrow \ x_0 \textit{ és parell.}$$

• Criteri de divisibilitat entre 3

$$1 \equiv 1 \ (mod\, 3);\ 10^1 \equiv 1 \ (mod\, 3);\ 10^2 \equiv 1 \ (mod\, 3);\ 10^3 \equiv 1 \ (mod\, 3);\ \ldots$$

El nombre $n = (x_k \cdots x_3 x_2 x_1 x_0)_{10}$ és divisible entre 3 sii

$x_0 + x_1 + \cdots + x_k \equiv 0 \ (mod\, 3) \ \Leftrightarrow$ *la suma de les seves xifres és múltiple de 3.*

• Criteri de divisibilitat entre 4

$$1 \equiv 1 \ (mod\, 4);\ 10^1 \equiv 2 \ (mod\, 4);\ 10^2 \equiv 0 \ (mod\, 4);\ 10^4 \equiv 0 \ (mod\, 4);\ \ldots$$

El nombre $n = (x_k \cdots x_3 x_2 x_1 x_0)_{10}$ és divisible entre 4 sii

$$x_0 + 2\, x_1 \equiv 0 \ (mod\, 4) \ \Leftrightarrow \ x_0 + 10\, x_1 \equiv 0 \ (mod\, 4) \ \Leftrightarrow \ (x_1 x_0)_{10} \equiv 0 \ (mod\, 4)$$

$$\Leftrightarrow \textit{ el nombre } (x_1 x_0)_{10} \textit{ es múltiple de 4.}$$

• Criteri de divisibilitat entre 5

$$1 \equiv 1 \ (mod\, 5);\ 10^1 \equiv 0 \ (mod\, 5);\ 10^2 \equiv 0 \ (mod\, 5);\ \ldots$$

El nombre $n = (x_k \cdots x_3 x_2 x_1 x_0)_{10}$ és divisible entre 5 sii

$$x_0 \equiv 0 \ (mod\, 5) \ \Leftrightarrow \ x_0 \textit{ és 0 ó 5.}$$

• Criteri de divisibilitat entre 9

$$1 \equiv 1 \ (mod\, 9);\ 10^1 \equiv 1 \ (mod\, 9);\ 10^2 \equiv 1 \ (mod\, 9);\ 10^3 \equiv 1 \ (mod\, 9);\ \ldots$$

El nombre $n = (x_k \cdots x_3 x_2 x_1 x_0)_{10}$ és divisible entre 9 sii

$x_0 + x_1 + \cdots + x_k \equiv 0 \ (mod\, 9) \ \Leftrightarrow$ *la suma de les seves xifres és múltiple de 9.*

• Criteri de divisibilitat entre 11

$1 \equiv 1 \ (mod\, 11);\ 10^1 \equiv -1 \ (mod\, 11);\ 10^2 \equiv 1 \ (mod\, 11);\ 10^3 \equiv -1 \ (mod\, 11);$

$10^4 \equiv 1 \ (mod\, 11);\ 10^5 \equiv -1 \ (mod\, 11);\ \ldots$

El nombre $n = (x_k \cdots x_3 x_2 x_1 x_0)_{10}$ és divisible entre 11 sii

$$x_0 - x_1 + x_2 - x_3 + x_4 - x_5 + \cdots + (-1)^k x_k \equiv 0 \ (mod\, 11) \ \Leftrightarrow$$

$$(x_0 + x_2 + x_4 + \cdots) - (x_1 + x_3 + x_5 + \cdots) \equiv 0 \ (mod\, 11) \ \Leftrightarrow$$

la diferència entre la suma de xifres de lloc senar i la suma de xifres de lloc parell és múltiple de 11 (0, 11 o múltiple de 11).

Exemple Determinar un criteri de divisibilitat entre 7.

Calculem les congruències de les potències de 10 mòdul 7.

$$1 \equiv 1 \ (mod\, 7);\ 10^1 \equiv 3 \ (mod\, 7);\ 10^2 \equiv 2 \ (mod\, 7);\ 10^3 \equiv -1 \ (mod\, 7);$$

$$10^4 \equiv -3 \ (mod\, 7);\ 10^5 \equiv -2 \ (mod\, 7);\ 10^6 \equiv 1 \ (mod\, 7);\ 10^7 \equiv 3 \ (mod\, 7);\ \ldots$$

A partir de $10^6 \equiv 1 \ (mod\, 7)$ el resultat de les congruències es repeteix. Per tant, el nombre $n = (x_k \cdots x_3 x_2 x_1 x_0)_{10}$ és divisible entre 7 sii

$$(x_0 + 3\,x_1 + 2\,x_2 - x_3 - 3\,x_4 - 2\,x_5) + (\cdots) + \cdots \equiv 0 \ (mod\, 7).$$

Per exemple, el nombre 3218096 és divisible entre 7, ja que:

$$6 + 3 \cdot 9 + 2 \cdot 0 - 8 - 3 \cdot 1 - 2 \cdot 2 + 3 = 36 - 15 = 21 \equiv 0 \ (mod\, 7).$$

Exemple Comprovar si és correcta la divisió $4792835 = 719 \cdot 6567 + 432$.

Si la igualtat numèrica anterior és certa també ho serà per a les seves classes mòdul 9. Cadascun d'aquests nombres és congruent mòdul 9 amb la suma de les seves xifres, però cada vegada que s'obté un 9 aquest és congruent amb 0 $(mod\, 9)$ i pot ser simplificat. A partir de l'enunciat:

$$2 \equiv 8 \cdot 6 + 0 \ (mod\, 9); \quad \text{però} \quad 2 \not\equiv 3 \ (mod\, 9).$$

Per tant, la divisió anterior no és correcta.

Aquest procediment es coneix com la "prova del nou". Si la prova del nou falla podem assegurar que l'operació és incorrecta. No obstant, un resultat favorable de la prova del nou no garanteix la correcció del càlcul inicial.

Exercicis

1. Resoldre les congruències

$$\text{(i) } 5\,x + 4 \equiv 3 \ (mod\, 7) \qquad \text{(ii) } 2\,x - 5 \equiv 7 \ (mod\, 8)$$

2. Resoldre el sistema de congruències

$$\left.\begin{array}{l} -3\,x + \ \ y \equiv 4 \ (mod\, 7) \\ -2\,x - 3\,y \equiv 1 \ (mod\, 7) \end{array}\right\}$$

3. Calcular el residu de la divisió de 17^{4027} entre 24.

4. Determinar un criteri de divisibilitat entre 13.