Tema 2: Conjunts i relacions (bloc 3)

Divisibilitat

Definicions

- Es diu que un nombre enter a és divisible per un enter b diferent de zero si existeix un altre enter k tal que $a = bk$. També es diu que b és divisor de a, que b divideix a, o que a és un múltiple de b. Sol denotar-se per $b \mid a$.

  Exemple: 3 divideix 6 (o 6 és múltiple de 3) però 3 no divideix 5.
- Direm que un nombre natural $p > 1$ és primer si els seus dos únics divisors naturals són 1 i ell mateix. Els nombres primers més menuts són $2, 3, 5, 7, 11, 13 \ldots$

  Si un nombre natural més gran que 1 no és primer, direm que és compost.
- El màxim comú divisor dels enters $a_1, a_2, \ldots, a_n$ és l'enter positiu més gran que els divideix tots. El denotarem per $\mathrm{mcd}(a_1, a_2, \ldots, a_n)$. El mínim comú múltiple dels enters no nuls $a_1, a_2, \ldots, a_n$ és l'enter positiu més petit que és múltiple de tots. El denotarem per $\mathrm{mcm}(a_1, a_2, \ldots, a_n)$.
- És diu que $a, b \in \mathbb{Z}$ són primers entre ells si $\mathrm{mcd}(a, b) = 1$.

Propietat

Tot nombre natural $n > 1$ s'escriu de forma única (tret de l'ordre) com a producte de nombres primers.

Exemples: $24 = 2^3 \cdot 3$ i $126 = 2 \cdot 3^2 \cdot 7$.

Conseqüències:

Siguen a i b dos nombres enters no nuls. Considerem les descomposicions de $|a|$ i $|b|$ com a producte de factors primers. Aleshores:

1. $\mathrm{mcd}(a, b)$ és el producte de tots els factors primers comuns a a ambdues descomposicions, elevats a l'exponent més petit.

   Exemple: $\mathrm{mcd}(24, 126) = 2 \cdot 3 = 6$

2. $\mathrm{mcm}(a, b)$ és el producte de tots els factors primers que apareixen en les descomposicions (els comuns i els no comuns), cadascun d'ells elevat a l'exponent més gran.

   Exemple: $\mathrm{mcm}(24, 126) = 2^3 \cdot 3^2 \cdot 7 = 504$

3. $\mathrm{mcd}(a, b) \cdot \mathrm{mcm}(a, b) = |a \cdot b|$.

Divisió euclidiana

Propietat

Siguen $a, b \in \mathbb{Z}$, amb $b > 0$. Aleshores existeixen dos nombres enters únics q, r tals que $a = q \cdot b + r$ i $0 \leq r < b$.

Els nombres a, b, q i r solen anomenar-se *dividend, divisor, quocient* i *residu*, respectivament.

Exemples:

- Si $a = 7$ i $b = 5$, aleshores $7 = 1 \cdot 5 + 2$.
- Si $a = 5$ i $b = 7$, aleshores $5 = 0 \cdot 7 + 5$.
- Si $a = -7$ i $b = 5$, aleshores $-7 = -2 \cdot 5 + 3$.
- Si $a = -5$ y $b = 7$, aleshores $-5 = -1 \cdot 7 + 2$.

Algorisme d'Euclides

L'algorisme d'Euclides permet calcular el màxim comú divisor de dos nombres enters sense necessitat de trobar les seues descomposicions com a producte de nombres primers. Es basa en la següent propietat:

Propietat

Si $a, b \in \mathbb{Z}$, amb $b \neq 0$, aleshores $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$, on r és el residu de la divisió euclidiana de a entre b.

Observació: Aquesta propietat es demostra fàcilment comprovant que els divisors comuns de a i b són els mateixos que els divisors comuns de b i r.

L'algorisme d'Euclides consisteix en l'aplicació reiterada d'aquesta propietat, reduint la grandària dels enters sense alterar el seu màxim comú divisor.

Algorisme d'Euclides:

Siguen a i b dos nombres enters amb $a \geq b > 0$ (com que $\text{mcd}(a, b) = \text{mcd}(|a|, |b|)$ podem suposar sense pèrdua de generalitat que a i b són positius). Considerem el següent procés recurrent:

- Fem la divisió euclidiana de a entre b $(a = q_1 \cdot b + r_1)$.
  $\hookrightarrow$ Si $r_1 = 0$, aleshores b divideix a i $\text{mcd}(a, b) = b$.
  $\hookrightarrow$ Si $r_1 \neq 0$,
  - Fem la divisió euclidiana de b entre r_1 $(b = q_2 \cdot r_1 + r_2)$.
    $\hookrightarrow$ Si $r_2 = 0$, aleshores r_1 divideix b i aplicant la propietat anterior,
    $$\text{mcd}(a, b) = \text{mcd}(b, r_1) = r_1.$$
    $\hookrightarrow$ Si $r_2 \neq 0$,
    - Fem de nou la divisió euclidiana del divisor de la divisió anterior entre el seu residu $(r_1 = q_3 \cdot r_2 + r_3)\ldots$

Com que $b > r_1 > r_2 > \cdots > r_n \geq 0$, arribarà un moment en què algun dels residus r_k serà nul i el procés acabarà. Aplicant la propietat anterior es dedueix que mcd(a, b) és el darrer residu no nul de l'algorisme d'Euclides.

Exemple

Calcula $\mathrm{mcd}(689, 234)$ fent servir l'algorisme d'Euclides.

1. Dividim $a = 689$ entre $b = 234$: $\begin{array}{l|l} 689 & 234 \\ \hline 221 & 2 \end{array}$

2. Dividim el divisor entre el residu: $\begin{array}{l|l} 234 & 221 \\ \hline 13 & 1 \end{array}$

3. Dividim el nou divisor entre el nou residu: $\begin{array}{l|l} 221 & 13 \\ \hline 0 & 17 \end{array}$

El darrer residu no nul és el 13. Per tant, $\mathrm{mcd}(689, 234) = 13$.

Observació:

Com que $\mathrm{mcd}(689, 234) \cdot \mathrm{mcm}(689, 234) = 689 \cdot 234$, podem calcular també el mínim comú múltiple de 689 i 234:

$$\mathrm{mcm}(689, 234) = 689 \cdot 234/13 = 12402.$$

Un altre exemple

Calcula $\mathrm{mcd}(54321, 50)$ fent servir l'algorisme d'Euclides.

$$\begin{array}{c|c} 54321 & \underline{50} \\ 21 & 1056 \end{array} \qquad \begin{array}{c|c} 50 & \underline{21} \\ 8 & 2 \end{array} \qquad \begin{array}{c|c} 21 & \underline{8} \\ 5 & 2 \end{array}$$

$$\begin{array}{c|c} 8 & \underline{5} \\ 3 & 1 \end{array} \qquad \begin{array}{c|c} 5 & \underline{3} \\ 2 & 1 \end{array} \qquad \begin{array}{c|c} 3 & \underline{2} \\ 1 & 1 \end{array} \qquad \begin{array}{c|c} 2 & \underline{1} \\ 0 & 2 \end{array}$$

Com que el darrer residu no nul és 1 es té que $\mathrm{mcd}(54321, 50) = 1$, per tant 54321 i 50 són primers entre ells.

A més a més, el seu mínim comú múltiple és:

$$\mathrm{mcm}(54321, 50) = 54321 \cdot 50/\mathrm{mcd}(54321, 50) = 2716050.$$

Conseqüències de l'Algorismeo d'Euclides

L'algorisme d'Euclides ens permet demostrar un teorema molt importante de la Teoria de Nombres, la *Identitat de Bézout*, que afirma que el màxim comú divisor de dos nombres enters pot expressar-se com a combinació lineal d'aquestos:

Identitat de Bézout

Per a qualsevol parell de nombres enters a, b, existeixen altres dos nombres enters x, y tals que $mcd(a, b) = x \cdot a + y \cdot b$.

A més, tots els multiples de $mcd(a, b)$, i només aquestos, poden expressar-se com a combinació lineal de a i b:

Conseqüència

Si a, b i c són nombres enters, aleshores

$$\exists\, x, y \in \mathbb{Z} \text{ tals que } c = x \cdot a + y \cdot b \text{ si, i només si, } mcd(a, b) \mid c$$

La relació de congruència

En aquesta secció estudiarem amb més detall **la relació de congruència mòdul *m*** entre nombres enters i el seu conjunt quocient, **els enters mòdul** *m*. Recordem aquesta relació, introduïda en el bloc anterior del tema:

Definició

Si m és un nombre enter, $m > 1$, direm que dos nombres enters a i b són *congruents mòdul m* *si $a - b$ és un múltiple de m.*
Escriurem $a \equiv b \pmod{m}$.

És fàcil demostrar que

$a \equiv b \pmod{m}$ si i només si els residus de les divisions euclidianes de a i b entre m coincideixen.

Per exemple, $17 \equiv 53 \pmod{6}$ perquè $17 - 53 = -36$ és un múltiple 6 o perquè els residus de les divisions de 17 i 53 entre 6 coincideixen:

$$\begin{array}{r|l} 17 & \underline{6} \\ 5 & 2 \end{array} \qquad\qquad \begin{array}{r|l} 53 & \underline{6} \\ 5 & 8 \end{array}$$

Els enters mòdul *m*

Recordem que la relació de congruència mòdul m és una relació d'equivalència (és a dir, és reflexiva, simètrica i transitiva). Per tant, podem construir el conjunt quocient format per les classes d'equivalència originades per aquesta relació:

Notació

Considerem un nombre enter $m > 1$.

- Denotarem per $\mathbb{Z}_m$ el conjunt quocient $\mathbb{Z}$ respecte de la relació de congruència mòdul m.
- Els elements de $\mathbb{Z}_m$, les classes d'equivalència, s'anomenen *classes residuals mòdul m* (o simplement *enters mòdul m*) i els denotarem per $\overline{a}$, amb $a \in \mathbb{Z}$.

Per a tot $a \in \mathbb{Z}$ es té que $\overline{a} = \overline{r}$ en $\mathbb{Z}_m$, on r és el residu de la divisió euclidiana de a entre m. Per tant, $\mathbb{Z}_m$ té exactament m elements:

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$$

Els enters mòdul m

1. Si $m = 2$, aleshores $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, on

   $$\overline{0} = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod{2}\} = \{\dots, -4, -2, 0, 2, 4, \dots\} = \{2n \mid n \in \mathbb{Z}\}$$

   $$\overline{1} = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod{2}\} = \{\dots, -3, -1, 1, 3, 5, \dots\} = \{1 + 2n \mid n \in \mathbb{Z}\}$$

2. Si $m = 3$, aleshores $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$, on

   $$\overline{0} = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod{3}\} = \{\dots, -6, -3, 0, 3, 6, \dots\} = \{3n \mid n \in \mathbb{Z}\}$$

   $$\overline{1} = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod{3}\} = \{\dots, -5, -2, 1, 4, 7, \dots\} = \{1 + 3n \mid n \in \mathbb{Z}\}$$

   $$\overline{2} = \{a \in \mathbb{Z} \mid a \equiv 2 \pmod{3}\} = \{\dots, -4, -1, 2, 5, 8, \dots\} = \{2 + 3n \mid n \in \mathbb{Z}\}$$

3. En general, $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\}$, on

   $$\overline{0} = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod{m}\} = \{m \cdot n \mid n \in \mathbb{Z}\}$$

   $$\overline{1} = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod{m}\} = \{1 + m \cdot n \mid n \in \mathbb{Z}\}$$

   $$\overline{2} = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod{m}\} = \{2 + m \cdot n \mid n \in \mathbb{Z}\}$$

   $$\vdots$$

   $$\overline{m-1} = \{a \in \mathbb{Z} \mid a \equiv m-1 \pmod{m}\} = \{(m-1) + m \cdot n \mid n \in \mathbb{Z}\}$$

Operacions en $\mathbb{Z}_m$

Definició

Si $\overline{a}$ i $\overline{b}$ són dos elements de $\mathbb{Z}_m$, aleshores la *suma* i el *producte* de $\overline{a}$ i $\overline{b}$ es defineixen de la següent manera:

$$\overline{a}+\overline{b}=\overline{a+b}, \qquad \overline{a}\cdot\overline{b}=\overline{a\cdot b}$$

Observació: Pot demostrar-se que la definició d'aquestes operacions no depèn dels representants elegits per a cada classe residual.

Exemples: En $\mathbb{Z}_4$, $\overline{2}+\overline{3}=\overline{5}=\overline{1}$

En $\mathbb{Z}_7$, $\overline{3}\cdot\overline{6}=\overline{18}=\overline{4}$

Observació: Si m és petit, podem construir un quadre de doble entrada amb tots els resultats possibles de l'operació suma en $\mathbb{Z}_m$ (i el mateix amb l'operació producte). Aquest tipus de quadre es coneix com taula de Cayley de l'operació.

Exemple: Construïm les taules de Cayley de la suma i el producte en $\mathbb{Z}_6$.

Operacions en $\mathbb{Z}_m$

Observacions

- Les operacions suma i producte en $\mathbb{Z}_m$ són commutatives i associatives.
- El producte és distributiu respecte de la suma.
- $\overline{0}$ i $\overline{1}$ són neutres de la suma i del producte, respectivament.
- Tot element de $\mathbb{Z}_m$ té simètric respecte de la suma (també anomenat *oposat*). En concret, l'oposat de $\overline{a}$ és $\overline{-a}$, ja que $\overline{a} + \overline{-a} = \overline{0}$.

Tanmateix, **no** tots els elements de $\mathbb{Z}_m$ tenen simètric respecte del producte (també anomenat *invers*):

Exemples:

- $\overline{0}$ no té invers en cap $\mathbb{Z}_m$ perquè $\overline{0} \cdot \overline{a} = \overline{0} \neq \overline{1}$, $\forall\, \overline{a} \in \mathbb{Z}_m$.
- $\overline{3}$ no té invers en $\mathbb{Z}_6$ ja que no existeix cap element $\overline{a}$ de $\mathbb{Z}_6$ que satisfaça que $\overline{3} \cdot \overline{a} = \overline{1}$.

Propietat

$\overline{a} \neq \overline{0}$ té invers (respecte del producte) en $\mathbb{Z}_m$ si, i només si, $\mathrm{mcd}(a, m) = 1$.

Equacions en congruències lineals

El nostre objectiu ara és resoldre equacions lineals en $\mathbb{Z}_m$:

$$\overline{a} \cdot \overline{x} = \overline{b} \quad \text{on} \quad \overline{a}, \overline{b} \in \mathbb{Z}_m$$

o, equivalentment, congruències lineals amb una incògnita del tipus:

$$ax \equiv b \pmod{m}.$$

En particular, quan $\overline{b} = \overline{1}$, així podrem calcular l'invers d'un element $\overline{a} \in \mathbb{Z}_m$, quan existeixca.

Propietat

L'equació

$$\overline{a} \cdot \overline{x} = \overline{b}$$

en $\mathbb{Z}_m$ té solució si, i només si, $\text{mcd}(a, m)$ divideix b.

Aquesta propietat ens diu en quins casos té solució l'equació, però no ens diu quantes solucions té, ni com calcular-les. A continuació anem a abordar aquesta qüestió.

Resolució d'equacions en congruències

$$ax \equiv b \pmod{m} \qquad (\overline{a} \cdot \overline{x} = \overline{b} \quad \text{en } \mathbb{Z}_m)$$

Existència de solució

- **Cas 1**: a és primer amb m.

  En aquest cas, la congruència té solució única en $\mathbb{Z}_m$.

- **Cas 2**: $d = \text{mcd}(a, m) \neq 1$ però d divideix b.

  En aquest cas, l'equació té d solucions en $\mathbb{Z}_m$.
  Com que d divideix a, m i b podem construir l'equació:

  $$a'x \equiv b' (\text{mod } m')$$

  on $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ i $m' = \frac{m}{d}$. Si s és la solució única de l'equació anterior (cas 1), aleshores les d solucions de l'equació original en $\mathbb{Z}_m$ són:

  $$s, \; s + m', \; s + 2m', \; \ldots \;, s + (d-1)m'$$

- **Cas 3**: $\text{mcd}(a, m)$ no divideix b.

  En aquest cas l'equació $\bar{a} \cdot \bar{x} = \bar{b}$ en $\mathbb{Z}_m$ no té solució.

Resolució d'equacions en congruències

Càlcul de la solució de $ax \equiv b(\mathbf{mod}\, m)$ si $\mathrm{mcd}(a, m) = 1$

Siga a un nombre enter amb $0 < a < m$ i $\mathrm{mcd}(a, m) = 1$, i considerem els quocients $q_1, q_2, \ldots, q_n$ de les divisions de l'algorisme d'Euclides per calcular $\mathrm{mcd}(a, m)$. Si definim $P_0 = 1,\ P_1 = q_1$, i

$$P_i = q_i P_{i-1} + P_{i-2} \qquad \text{per a } \ i = 2, 3, \ldots, n,$$

aleshores

$$x = (-1)^{n-1} \cdot P_{n-1} \cdot b, \quad \text{en } \ \mathbb{Z}_m, \text{ és la solució de l'equació.}$$

El càlcul dels P_i pot esquematitzar-se mitjançant el següent quadre:

i	0	1	2	3	$\ldots$	$n-1$	n
q_i		q_1	q_2	q_3	$\ldots$	q_{n-1}	q_n
P_i	1	q_1	P_2	P_3	$\ldots$	P_{n-1}	m

Exemple (cas 1)

Resoleu l'equació en congruències $11 \cdot x \equiv 6 \pmod{27}$ o, equivalentment, l'equació

$$\overline{11} \cdot \overline{x} = \overline{6}, \quad \text{en} \quad \mathbb{Z}_{27}$$

Com que $\text{mcd}(11, 27) = 1$, sabem que l'equació té una única solució (Cas 1).

Per calcular-ne la solució, farem servir l'esquema anterior. Hem de calcular en primer lloc els quocients de l'algorisme d'Euclides per calcular $\text{mcd}(11, 27)$:

$$\begin{array}{cc} 27 & |\underline{11} \\ 5 & \underbrace{2}_{q_1} \end{array} \qquad \begin{array}{cc} 11 & |\underline{5} \\ 1 & \underbrace{2}_{q_2} \end{array} \qquad \begin{array}{cc} 5 & |\underline{1} \\ 0 & \underbrace{5}_{q_3} \end{array}$$

Tot seguit calculem els P_i

q_i		2	2	5
P_i	1	2	5	27

Per tant la solució de l'equació és

$$x = (-1)^2 \cdot P_2 \cdot 6 = 1 \cdot 5 \cdot 6 = 30 = 3 \text{ en } \mathbb{Z}_{27}.$$

Exemple (cas 2)

Resoleu l'equació en congruències $18 \cdot x \equiv 6 \pmod{15}$ o, equivalentment, l'equació

$$\overline{18} \cdot \overline{x} = \overline{6}, \quad \text{en} \quad \mathbb{Z}_{15}$$

Abans de resoldre l'equació, observem que $\overline{18} = \overline{3}$ en $\mathbb{Z}_{15}$. Per tant, l'equació original és equivalent a l'equació:

$$\overline{3} \cdot \overline{x} = \overline{6}, \quad \text{en} \quad \mathbb{Z}_{15}.$$

Directament, per simple inspecció, veiem que $x = 2$ és una solució d'aquesta equació, però no n'és l'única. Com que $\text{mcd}(3, 15) = 3 \neq 1$ però divideix 6 (l'altre coeficient), l'equació té <u>3 solucions</u> (Cas 2).

Com que els dos coeficients i el mòdul són divisibles per 3, podem dividir-los i obtenim una equació equivalent a l'original, però en mòdul 5:

$$\overline{1} \cdot \overline{x} = \overline{2}, \quad \text{en} \quad \mathbb{Z}_5. \quad \text{(equació de Cas 1)}$$

La solució d'aquesta equació és $x = 2$ en $\mathbb{Z}_5$.

Així, tenim 3 solucions diferents de l'equació original en $\mathbb{Z}_{15}$:

$$\begin{aligned} x_0 &= 2 \\ x_1 &= 2 + 5 = 7 \\ x_2 &= 2 + 2 \cdot 5 = 12 \end{aligned}$$