# 6. Enters, congruències i equacions diofàntiques

## GEI, GEIADE i GTIDIC


Nacho López

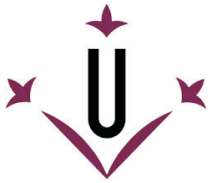
nacho.lopez@udl.cat

Cristina Dalfó

cristina.dalfo@udl.cat

Departament de Matemàtica
Cryptography & Graphs Research Group (C&G)
Universitat de Lleida



# Divisió entera

- **Teorema de la divisió entera**. Si $a$ i $b$ són dos nombres enters amb $b \neq 0$, aleshores existeixen dos únics enters $q$ i $r$ que verifiquen

$$a = b \cdot q + r, \quad \text{on } 0 \leq r < |b|.$$

$$\begin{array}{r|l} a & b \\ \hline r & q \end{array} \qquad \begin{array}{r|l} 13 & 2 \\ \hline 1 & 6 \end{array}$$

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

# Divisió entera

- **Teorema de la divisió entera**. Si $a$ i $b$ són dos nombres enters amb $b \neq 0$, aleshores existeixen dos únics enters $q$ i $r$ que verifiquen

$$a = b \cdot q + r, \quad \text{on } 0 \leq r < |b|.$$

$$\begin{array}{l|l} a & b \\ \hline r & q \end{array} \qquad \begin{array}{l|l} 13 & 2 \\ \hline 1 & 6 \end{array}$$

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

- Donats dos enters $a$ i $b$, es diu que $b$ és un **divisor** de $a$, i s'escriu $b \mid a$, si existeix un enter $c$ tal que $a = b \cdot c$. Exemple: $2|8$.

# Divisió entera

- **Teorema de la divisió entera**. Si $a$ i $b$ són dos nombres enters amb $b \neq 0$, aleshores existeixen dos únics enters $q$ i $r$ que verifiquen

$$a = b \cdot q + r, \quad \text{on } 0 \leq r < |b|.$$

$$\begin{array}{c|c} a & b \\ \hline r & q \end{array} \qquad \begin{array}{c|c} 13 & 2 \\ \hline 1 & 6 \end{array}$$

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

- Donats dos enters $a$ i $b$, es diu que $b$ és un **divisor** de $a$, i s'escriu $b \mid a$, si existeix un enter $c$ tal que $a = b \cdot c$. Exemple: $2|8$.
- En aquesta mateixa situació també es diu que $a$ és un **múltiple** de $b$, i s'escriu $a = \dot{b}$, o que $a$ és **divisible** per $b$. Exemple: $8 = \dot{2}$.

# Divisió entera

- **Teorema de la divisió entera**. Si $a$ i $b$ són dos nombres enters amb $b \neq 0$, aleshores existeixen dos únics enters $q$ i $r$ que verifiquen

$$a = b \cdot q + r, \quad \text{on } 0 \leq r < |b|.$$

$$\begin{array}{r|l} a & b \\ \hline r & q \end{array} \qquad \begin{array}{r|l} 13 & 2 \\ \hline 1 & 6 \end{array}$$

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

- Donats dos enters $a$ i $b$, es diu que $b$ és un **divisor** de $a$, i s'escriu $b \mid a$, si existeix un enter $c$ tal que $a = b \cdot c$. Exemple: $2|8$.
- En aquesta mateixa situació també es diu que $a$ és un **múltiple** de $b$, i s'escriu $a = \dot{b}$, o que $a$ és **divisible** per $b$. Exemple: $8 = \dot{2}$.
- Si $b \neq 0$, dir que $b \mid a$ és equivalent a dir que el residu de la divisió entera de $a$ per $b$ és zero.

# Màxim comú divisor.

- Donats dos enters $a$ i $b$, no tots dos nuls, es diu que $d \in \mathbb{Z}$ és el **màxim comú divisor** de $a$ i $b$, i s'escriu

$$d = \text{mcd}(a, b),$$

si es compleix que:

1) $d \mid a$ i $d \mid b$ ($d$ és un divisor comú de $a$ i $b$).
2) Si $d' \mid a$ i $d' \mid b$ aleshores $d' \leq d$ ($d$ és el divisor comú més gran).

# Màxim comú divisor.

- Donats dos enters $a$ i $b$, no tots dos nuls, es diu que $d \in \mathbb{Z}$ és el **màxim comú divisor** de $a$ i $b$, i s'escriu

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

si es compleix que:

1) $d \mid a$ i $d \mid b$ ($d$ és un divisor comú de $a$ i $b$).
2) Si $d' \mid a$ i $d' \mid b$ aleshores $d' \leq d$ ($d$ és el divisor comú més gran).

- **Propietats del màxim comú divisor**:

1. $\mathrm{mcd}(a, 0) = |a|$.
2. Si $b \neq 0$, aleshores $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$, on $r$ és el residu de la divisió entera de $a$ per $b$.

# Màxim comú divisor.

- Donats dos enters $a$ i $b$, no tots dos nuls, es diu que $d \in \mathbb{Z}$ és el **màxim comú divisor** de $a$ i $b$, i s'escriu

$$d = \text{mcd}(a, b),$$

si es compleix que:

1) $d \mid a$ i $d \mid b$ ($d$ és un divisor comú de $a$ i $b$).
2) Si $d' \mid a$ i $d' \mid b$ aleshores $d' \leq d$ ($d$ és el divisor comú més gran).

- **Propietats del màxim comú divisor**:
  1. $\text{mcd}(a, 0) = |a|$.
  2. Si $b \neq 0$, aleshores $\text{mcd}(a, b) = \text{mcd}(b, r)$, on $r$ és el residu de la divisió entera de $a$ per $b$.
- **Exemples:**
  1. $\text{mcd}(15, 6) = \text{mcd}(3 \cdot 5, 2 \cdot 3) = 3$.
  2. $\text{mcd}(45, 18) = \text{mcd}(3^2 \cdot 5, 2 \cdot 3^2) = 9$.

# Algorisme d'Euclides

- Donats dos enters $a$ i $b$, podem aplicar reiteradament el teorema de la divisió entera, fins que el residu sigui zero, de la manera següent:

$$\left.\begin{array}{rcll} a & = & b \cdot q_1 + r_1, & r_1 < |b| \\ b & = & r_1 \cdot q_2 + r_2, & r_2 < r_1 \\ & \vdots & & \\ r_{n-2} & = & r_{n-1} \cdot q_n + r_n, & r_n < r_{n-1} \\ r_{n-1} & = & r_n \cdot q_{n+1} + r_{n+1}, & r_{n+1} = 0 \end{array}\right\} \Rightarrow \text{mcd}\,(a,b) = r_n.$$

# Algorisme d'Euclides

- Donats dos enters $a$ i $b$, podem aplicar reiteradament el teorema de la divisió entera, fins que el residu sigui zero, de la manera següent:

$$\left.\begin{array}{rcll} a & = & b \cdot q_1 + r_1, & r_1 < |b| \\ b & = & r_1 \cdot q_2 + r_2, & r_2 < r_1 \\ & \vdots & & \\ r_{n-2} & = & r_{n-1} \cdot q_n + r_n, & r_n < r_{n-1} \\ r_{n-1} & = & r_n \cdot q_{n+1} + r_{n+1}, & r_{n+1} = 0 \end{array}\right\} \Rightarrow \text{mcd}\,(a,b) = r_n.$$

- Disposició d'aquest esquema en forma de taula:

| | $q_1$ | $q_2$ | $q_3$ | $\cdots$ | $q_{n-1}$ | $q_n$ | $q_{n+1}$ |
|---|---|---|---|---|---|---|---|
| $a$ | $b$ | $r_1$ | $r_2$ | $\cdots$ | $r_{n-2}$ | $r_{n-1}$ | $r_n$ |
| $r_1$ | $r_2$ | $r_3$ | $r_4$ | $\cdots$ | $r_n$ | 0 | |

$$\Rightarrow \quad \text{mcd}\,(a,b) = r_n.$$

# Algorisme d'Euclides

- Donats dos enters $a$ i $b$, podem aplicar reiteradament el teorema de la divisió entera, fins que el residu sigui zero, de la manera següent:

$$\left.\begin{array}{rcll} a & = & b \cdot q_1 + r_1, & r_1 < |b| \\ b & = & r_1 \cdot q_2 + r_2, & r_2 < r_1 \\ & \vdots & & \\ r_{n-2} & = & r_{n-1} \cdot q_n + r_n, & r_n < r_{n-1} \\ r_{n-1} & = & r_n \cdot q_{n+1} + r_{n+1}, & r_{n+1} = 0 \end{array}\right\} \Rightarrow \operatorname{mcd}(a,b) = r_n.$$

- Disposició d'aquest esquema en forma de taula:

| | $q_1$ | $q_2$ | $q_3$ | $\cdots$ | $q_{n-1}$ | $q_n$ | $q_{n+1}$ |
|---|---|---|---|---|---|---|---|
| $a$ | $b$ | $r_1$ | $r_2$ | $\cdots$ | $r_{n-2}$ | $r_{n-1}$ | $r_n$ |
| $r_1$ | $r_2$ | $r_3$ | $r_4$ | $\cdots$ | $r_n$ | 0 | |

$$\Rightarrow \quad \operatorname{mcd}(a,b) = r_n.$$

- **Exemple:**

| | 10 | 1 | 2 |
|---|---|---|---|
| 32 | 3 | 2 | 1 |
| 2 | 1 | 0 | |

$$\Rightarrow \quad \operatorname{mcd}(32,3) = 1.$$

- **Identitat de Bezout.** Si $d = \text{mcd}(a, b)$ aleshores existeixen enters $r$ i $s$ tals que

$$d = a \cdot r + b \cdot s,$$

és a dir, $d$ s'expressa com una **combinació lineal entera** de $a$ i $b$.

- **Identitat de Bezout.** Si $d = \text{mcd}(a, b)$ aleshores existeixen enters $r$ i $s$ tals que

$$d = a \cdot r + b \cdot s,$$

és a dir, $d$ s'expressa com una **combinació lineal entera** de $a$ i $b$.

- **Exemple:**

$$1 = 32 \cdot (-1) + 3 \cdot 11.$$

# Nombres primers entre ells i nombres primers

- Dos enters $a$ i $b$ són **primers entre ells** si $\text{mcd}(a, b)=1$.

# Nombres primers entre ells i nombres primers

- Dos enters $a$ i $b$ són **primers entre ells** si $\text{mcd}(a, b)=1$.
- **Teorema d'Euclides.** Si $a$ i $b$ són dos nombres primers entre ells i $a \mid (b \cdot c)$, aleshores $a \mid c$.
  **Exemple:** 4 i 5 són primers entre ells. Com que $4 \mid (5 \cdot 12)$, aleshores $4 \mid 12$.

# Nombres primers entre ells i nombres primers

- Dos enters $a$ i $b$ són **primers entre ells** si $\text{mcd}(a, b)=1$.
- **Teorema d'Euclides.** Si $a$ i $b$ són dos nombres primers entre ells i $a \mid (b \cdot c)$, aleshores $a \mid c$.
  **Exemple:** 4 i 5 són primers entre ells. Com que $4 \mid (5 \cdot 12)$, aleshores $4 \mid 12$.
- **Nombres primers.** Un nombre enter $p$ és un **nombre primer** si els seus únics divisors són $\pm 1$ i $\pm p$.
  L'1 i el $-1$ no es consideren nombres primers.

# Nombres primers entre ells i nombres primers

- Dos enters $a$ i $b$ són **primers entre ells** si $\text{mcd}(a,b)=1$.
- **Teorema d'Euclides.** Si $a$ i $b$ són dos nombres primers entre ells i $a \mid (b \cdot c)$, aleshores $a \mid c$.
  **Exemple:** 4 i 5 són primers entre ells. Com que $4 \mid (5 \cdot 12)$, aleshores $4 \mid 12$.
- **Nombres primers.** Un nombre enter $p$ és un **nombre primer** si els seus únics divisors són $\pm 1$ i $\pm p$.
  L'1 i el $-1$ no es consideren nombres primers.
- **Teorema fonamental de l'aritmètica.** Tot enter $a$ no nul i diferent de $\pm 1$, és primer o s'expressa com a producte de factors primers,

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$

de manera única (llevat de l'ordre i dels signes.)

# Equacions diofàntiques lineals

- Resoldre una **equació diofàntica lineal** amb dues incògnites $x$ i $y$, és buscar les solucions enteres d'una equació del tipus

$$a \cdot x + b \cdot y = c,$$

on $a, b$ i $c$ són nombres enters.

# Equacions diofàntiques lineals

- Resoldre una **equació diofàntica lineal** amb dues incògnites $x$ i $y$, és buscar les solucions enteres d'una equació del tipus

$$a \cdot x + b \cdot y = c,$$

on $a, b$ i $c$ són nombres enters.

- **Resolució.** Sigui $d = \text{mcd}(a, b)$. Aleshores, es verifica que:
  1) L'equació diofàntica té solució si, i només si, $d \mid c$;

# Equacions diofàntiques lineals

- Resoldre una **equació diofàntica lineal** amb dues incògnites $x$ i $y$, és buscar les solucions enteres d'una equació del tipus

$$a \cdot x + b \cdot y = c,$$

on $a, b$ i $c$ són nombres enters.

- **Resolució.** Sigui $d = \text{mcd}(a, b)$. Aleshores, es verifica que:
  1) L'equació diofàntica té solució si, i només si, $d \mid c$;
  2) Si $d \mid c$, aleshores l'equació diofàntica es pot escriure com $a' \cdot x + b' \cdot y = c'$, on $a' = \dfrac{a}{d}$, $b' = \dfrac{b}{d}$, $c' = \dfrac{c}{d}$, i les solucions vénen donades per:

$$\left.\begin{array}{rcl} x & = & x_0 + n \cdot b' \\ y & = & y_0 - n \cdot a' \end{array}\right\}$$

amb $n \in \mathbb{Z}$ i $(x_0, y_0)$ és una **solució particular** de $a' \cdot x + b' \cdot y = c'$.

# Equacions diofàntiques lineals

**Problem (82($a$))**

*Resoleu l'equació diofàntica* $25x + 15y = 5$.

**Problem (82($a$))**

*Resoleu l'equació diofàntica* $25x + 15y = 5$.

**Resolució.**

**Problem (82($a$))**

*Resoleu l'equació diofàntica* $25x + 15y = 5$.

**Resolució.**

- Tenim que $a = 25$, $b = 15$ i $c = 5$.

**Problem (82($a$))**

*Resoleu l'equació diofàntica* $25x + 15y = 5$.

**Resolució.**

- Tenim que $a = 25$, $b = 15$ i $c = 5$.
- $\text{mcd}(a, b) = \text{mcd}(25, 15) = 5$.

**Problem (82($a$))**

*Resoleu l'equació diofàntica* $25x + 15y = 5$.

**Resolució.**

- Tenim que $a = 25$, $b = 15$ i $c = 5$.
- $\text{mcd}(a, b) = \text{mcd}(25, 15) = 5$.
- L'equació té solució si $\text{mcd}(a, b) | c$, és a dir, si $5|5$. Per tant, l'equació té solució.

**Problem (82($a$))**

*Resoleu l'equació diofàntica* $25x + 15y = 5$.

**Resolució.**

- Tenim que $a = 25$, $b = 15$ i $c = 5$.
- $\text{mcd}(a, b) = \text{mcd}(25, 15) = 5$.
- L'equació té solució si $\text{mcd}(a, b) | c$, és a dir, si $5|5$. Per tant, l'equació té solució.
- Dividim tota l'equació per $\text{mcd}(25, 15)$, és a dir, per 5: $5x + 3y = 1$.

**Problem (82($a$))**

*Resoleu l'equació diofàntica* $25x + 15y = 5$.

**Resolució.**

- Tenim que $a = 25$, $b = 15$ i $c = 5$.
- $\text{mcd}(a, b) = \text{mcd}(25, 15) = 5$.
- L'equació té solució si $\text{mcd}(a, b) | c$, és a dir, si $5|5$. Per tant, l'equació té solució.
- Dividim tota l'equació per $\text{mcd}(25, 15)$, és a dir, per 5: $5x + 3y = 1$.
- Busquem una solució particular. Per a $x = -1$, tenim $-5 + 3y = 1$. Per tant, $y = 2$.

**Problem (82($a$))**

*Resoleu l'equació diofàntica* $25x + 15y = 5$.

**Resolució.**

- Tenim que $a = 25$, $b = 15$ i $c = 5$.
- $\text{mcd}(a, b) = \text{mcd}(25, 15) = 5$.
- L'equació té solució si $\text{mcd}(a, b) | c$, és a dir, si $5|5$. Per tant, l'equació té solució.
- Dividim tota l'equació per $\text{mcd}(25, 15)$, és a dir, per 5: $5x + 3y = 1$.
- Busquem una solució particular. Per a $x = -1$, tenim $-5 + 3y = 1$. Per tant, $y = 2$.
- La solució és

$$\left.\begin{array}{rcl} x & = & x_0 + n \cdot b' = -1 + 3n \\ y & = & y_0 - n \cdot a' = 2 - 5n \end{array}\right\}$$

amb $n \in \mathbb{Z}$.

# Congruències

- Donat un enter $m \neq 0$, es diu que dos nombres enters $a$ i $b$ són **congruents mòdul** $m$ si $a - b$ és un múltiple de $m$, i s'escriu

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

- **Exemples:** $13 \equiv 1 \pmod{12}$, $145 \equiv 1 \pmod{12}$.

# Congruències

- Donat un enter $m \neq 0$, es diu que dos nombres enters $a$ i $b$ són **congruents mòdul** $m$ si $a - b$ és un múltiple de $m$, i s'escriu

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

- **Exemples:** $13 \equiv 1 \pmod{12}$, $145 \equiv 1 \pmod{12}$.
- $a \equiv b \pmod{m}$ és equivalent a que $b$ és de la forma $a + k \cdot m$, on $k \in \mathbb{Z}$.

# Congruències

- Donat un enter $m \neq 0$, es diu que dos nombres enters $a$ i $b$ són **congruents mòdul** $m$ si $a - b$ és un múltiple de $m$, i s'escriu

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

- **Exemples:** $13 \equiv 1 \pmod{12}$, $145 \equiv 1 \pmod{12}$.
- $a \equiv b \pmod{m}$ és equivalent a que $b$ és de la forma $a + k \cdot m$, on $k \in \mathbb{Z}$.
- El **conjunt quocient de** $\mathbb{Z}$ per la relació de congruència mòdul $m$, que es representa per $\mathbb{Z}_m$ o també per $\mathbb{Z}/(m)$ o $\mathbb{Z}/m\mathbb{Z}$, està format per totes les classes de congruència diferents mòdul $m$, és a dir,

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}, \text{ on } \overline{a} = \{a + k \cdot m \mid k \in \mathbb{Z}\}.$$

# Congruències

- Donat un enter $m \neq 0$, es diu que dos nombres enters $a$ i $b$ són **congruents mòdul** $m$ si $a - b$ és un múltiple de $m$, i s'escriu

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

- **Exemples:** $13 \equiv 1 (\mathrm{mod}\, 12)$, $145 \equiv 1 (\mathrm{mod}\, 12)$.
- $a \equiv b \pmod{m}$ és equivalent a que $b$ és de la forma $a + k \cdot m$, on $k \in \mathbb{Z}$.
- El **conjunt quocient de** $\mathbb{Z}$ per la relació de congruència mòdul $m$, que es representa per $\mathbb{Z}_m$ o també per $\mathbb{Z}/(m)$ o $\mathbb{Z}/m\mathbb{Z}$, està format per totes les classes de congruència diferents mòdul $m$, és a dir,

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}, \text{ on } \overline{a} = \{a + k \cdot m \mid k \in \mathbb{Z}\}.$$

- **Exemple:**

$$\begin{aligned}\mathbb{Z}_4 &= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} = \{0 (\mathrm{mod}\, 4), 1 (\mathrm{mod}\, 4), 2 (\mathrm{mod}\, 4), 3 (\mathrm{mod}\, 4)\} \\ &= \{0, 4, 8, \ldots\} \cup \{1, 5, 9, \ldots\} \cup \{2, 6, 10, \ldots\} \cup \{3, 7, 11, \ldots\}.\end{aligned}$$

# Congruències

- En el conjunt $\mathbb{Z}_m$ es defineixen dues operacions internes:

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{i} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

# Congruències

- En el conjunt $\mathbb{Z}_m$ es defineixen dues operacions internes:

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{i} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

# Congruències

- En el conjunt $\mathbb{Z}_m$ es defineixen dues operacions internes:

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{i} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

- Resoldre la congruència lineal

$$a \cdot x \equiv b \pmod{m}$$

és equivalent a resoldre l'equació $\overline{a} \cdot \overline{x} = \overline{b}$ en $\mathbb{Z}_m$ i, al mateix temps, és, en certa forma equivalent, a resoldre l'equació diofàntica lineal $a \cdot x + m \cdot y = b$, tenint en compte que només ens importen els valors de $x$.

# Congruències lineals

**Resolució de** $a \cdot x \equiv b \pmod{m}$:

# Congruències lineals

**Resolució de** $a \cdot x \equiv b \pmod{m}$:

Sigui $d = \text{mcd}(a, m)$. Aleshores, es verifica que:

**Resolució de** $a \cdot x \equiv b \pmod{m}$:

Sigui $d = \text{mcd}(a, m)$. Aleshores, es verifica que:

1) $a \cdot x \equiv b \pmod{m}$ té solució si, i només si, $d \mid b$;

**Resolució de** $a \cdot x \equiv b \pmod{m}$:

Sigui $d = \text{mcd}(a, m)$. Aleshores, es verifica que:

1) $a \cdot x \equiv b \pmod{m}$ té solució si, i només si, $d \mid b$;

2) Si $d \mid b$ llavors $a \cdot x \equiv b \pmod{m}$ té exactament $d$ solucions i són de la forma

$$x = x_0 + \lambda \cdot m' \pmod{m}, \quad \lambda = 0, 1, \ldots, d-1,$$

on $m' = \dfrac{m}{d}$ i $x_0$ és una **solució particular** de la congruència

$$a' \cdot x \equiv b' \pmod{m'},$$

amb $a' = \dfrac{a}{d}$ i $b' = \dfrac{b}{d}$.

# Congruències lineals

**Problem (87($a$))**

*Resoleu la congruència lineal* $4x \equiv 8 \pmod{12}$.

**Problem (87(*a*))**

*Resoleu la congruència lineal* $4x \equiv 8 \pmod{12}$.

**Resolució.**

**Problem (87($a$))**

*Resoleu la congruència lineal* $4x \equiv 8 \pmod{12}$.

**Resolució.**

- Tenim que $a = 4$, $b = 8$ i $m = 12$.

**Problem (87(*a*))**

*Resoleu la congruència lineal* $4x \equiv 8 \pmod{12}$.

**Resolució.**

- Tenim que $a = 4$, $b = 8$ i $m = 12$.
- $d = \text{mcd}(a, m) = \text{mcd}(4, 12) = 4$. Com que $4|8$, té solució.

**Problem (87(*a*))**

*Resoleu la congruència lineal* $4x \equiv 8 \pmod{12}$.

**Resolució.**

- Tenim que $a = 4$, $b = 8$ i $m = 12$.
- $d = \text{mcd}(a, m) = \text{mcd}(4, 12) = 4$. Com que $4|8$, té solució.
- Dividim per $d = 4$: $x \equiv 2 \pmod{3}$.

**Problem (87(*a*))**

*Resoleu la congruència lineal* $4x \equiv 8 \pmod{12}$.

**Resolució.**

- Tenim que $a = 4$, $b = 8$ i $m = 12$.
- $d = \text{mcd}(a, m) = \text{mcd}(4, 12) = 4$. Com que $4|8$, té solució.
- Dividim per $d = 4$: $x \equiv 2 \pmod{3}$.
- Agafem com a solució particular $x_0 = 2 \pmod{3}$.

**Problem (87(*a*))**

*Resoleu la congruència lineal* $4x \equiv 8 \pmod{12}$.

**Resolució.**

- Tenim que $a = 4$, $b = 8$ i $m = 12$.
- $d = \text{mcd}(a, m) = \text{mcd}(4, 12) = 4$. Com que $4|8$, té solució.
- Dividim per $d = 4$: $x \equiv 2 \pmod 3$.
- Agafem com a solució particular $x_0 = 2 \pmod 3$.
- La solució de forma compacta és, amb $\lambda = 0, 1, 2, 3$,

$$x = x_0 + \lambda m' \pmod m = 2 + 3\lambda \pmod{12}.$$

**Problem (87(a))**

*Resoleu la congruència lineal* $4x \equiv 8 \pmod{12}$.

**Resolució.**

- Tenim que $a = 4$, $b = 8$ i $m = 12$.
- $d = \text{mcd}(a, m) = \text{mcd}(4, 12) = 4$. Com que $4|8$, té solució.
- Dividim per $d = 4$: $x \equiv 2 \pmod 3$.
- Agafem com a solució particular $x_0 = 2 \pmod 3$.
- La solució de forma compacta és, amb $\lambda = 0, 1, 2, 3$,

$$x = x_0 + \lambda m' \pmod m = 2 + 3\lambda \pmod{12}.$$

- La solució final és $x = x_0 + \lambda \cdot m' \pmod m$:

$$\begin{aligned} \lambda = 0: &\quad x = 2 + 0 = 2 \pmod{12}, \\ \lambda = 1: &\quad x = 2 + 3 = 5 \pmod{12}, \\ \lambda = 2: &\quad x = 2 + 6 = 8 \pmod{12}, \\ \lambda = 3: &\quad x = 2 + 9 = 11 \pmod{12}. \end{aligned}$$

# Teorema xinès dels residus.

Si $m_1, m_2, \ldots, m_n$ són enters primers dos a dos, és a dir, $\text{mcd}(m_i, m_j) = 1$ si $i \neq j$, i $b_1, b_2, \ldots, b_n$ són enters, aleshores el sistema de congruències lineals

$$\begin{cases} x & \equiv & b_1 \pmod{m_1} \\ x & \equiv & b_2 \pmod{m_2} \\ & \vdots & \\ x & \equiv & b_n \pmod{m_n}, \end{cases}$$

té solució i és única mòdul $M = m_1 \cdot m_2 \cdots m_n$, en el sentit que si $x_1$ i $x_2$ són dues solucions d'aquest sistema, aleshores $x_1 \equiv x_2 \pmod{M}$.

# Càlcul de residus de potències

- **Teorema "petit"de Fermat.** Si $p \in \mathbb{Z}^+$ és un nombre primer i $a$ és un enter no divisible per $p$, aleshores

$$a^{p-1} \equiv 1 \pmod{p}.$$

# Càlcul de residus de potències

- **Teorema "petit"de Fermat.** Si $p \in \mathbb{Z}^+$ és un nombre primer i $a$ és un enter no divisible per $p$, aleshores

$$a^{p-1} \equiv 1 \pmod{p}.$$

- **Exemple.** $2^{3-1} \equiv 1 (\mathrm{mod}\, 3)$.
- **Funció phi d'Euler.** Si $n$ és un enter positiu, la funció phi d'Euler per a aquest valor $n$, que denotem $\phi(n)$, és el nombre d'enters positius més petits o iguals que $n$ i primers amb $n$, és a dir,

$$\phi(n) = \text{Card}\,\{m \in \mathbb{Z}^+ \mid 1 \leq m \leq n \text{ i m.c.d.}(m,n) = 1\}.$$

# Càlcul de residus de potències

- **Propietats de la funció $\phi$**:

# Càlcul de residus de potències

- **Propietats de la funció $\phi$**:
  1. Si $p$ és primer, $\phi(p) = p - 1$;

# Càlcul de residus de potències

- **Propietats de la funció $\phi$**:
  1. Si $p$ és primer, $\phi(p) = p - 1$;
  2. Si $p$ és primer i $\alpha \in \mathbb{Z}^+$, aleshores $\phi(p^\alpha) = p^{\alpha-1} \cdot (p-1)$;

- **Propietats de la funció $\phi$**:
  1. Si $p$ és primer, $\phi(p) = p - 1$;
  2. Si $p$ és primer i $\alpha \in \mathbb{Z}^+$, aleshores $\phi(p^\alpha) = p^{\alpha-1} \cdot (p-1)$;
  3. Si $m$ i $n$ són primers entre ells, aleshores $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$;

- **Propietats de la funció $\phi$**:
  1. Si $p$ és primer, $\phi(p) = p - 1$;
  2. Si $p$ és primer i $\alpha \in \mathbb{Z}^+$, aleshores $\phi(p^\alpha) = p^{\alpha-1} \cdot (p-1)$;
  3. Si $m$ i $n$ són primers entre ells, aleshores $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$;
  4. Si $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ és la descomposició en factors primers de $n$, aleshores

$$\phi(n) = p_1^{\alpha_1-1} \cdot (p_1 - 1) \cdot p_2^{\alpha_2-1} \cdot (p_2 - 1) \cdots p_r^{\alpha_r-1} \cdot (p_r - 1).$$

- **Propietats de la funció $\phi$:**
  1. Si $p$ és primer, $\phi(p) = p - 1$;
  2. Si $p$ és primer i $\alpha \in \mathbb{Z}^+$, aleshores $\phi(p^\alpha) = p^{\alpha-1} \cdot (p-1)$;
  3. Si $m$ i $n$ són primers entre ells, aleshores $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$;
  4. Si $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ és la descomposició en factors primers de $n$, aleshores

$$\phi(n) = p_1^{\alpha_1-1} \cdot (p_1 - 1) \cdot p_2^{\alpha_2-1} \cdot (p_2 - 1) \cdots p_r^{\alpha_r-1} \cdot (p_r - 1).$$

- **Exemples.**
  - $\phi(9) = \phi(3^2) = 3^1 \cdot 2 = 6$ (els 6 nombres serien 1,2,4,5,7,8).

# Càlcul de residus de potències

- **Propietats de la funció $\phi$:**
  1. Si $p$ és primer, $\phi(p) = p - 1$;
  2. Si $p$ és primer i $\alpha \in \mathbb{Z}^+$, aleshores $\phi(p^\alpha) = p^{\alpha-1} \cdot (p-1)$;
  3. Si $m$ i $n$ són primers entre ells, aleshores $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$;
  4. Si $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ és la descomposició en factors primers de $n$, aleshores

$$\phi(n) = p_1^{\alpha_1-1} \cdot (p_1 - 1) \cdot p_2^{\alpha_2-1} \cdot (p_2 - 1) \cdots p_r^{\alpha_r-1} \cdot (p_r - 1).$$

- **Exemples.**
  - $\phi(9) = \phi(3^2) = 3^1 \cdot 2 = 6$ (els 6 nombres serien 1,2,4,5,7,8).
  - $\phi(36) = \phi(2^2 \cdot 3^2) = 2^1 \cdot 1 \cdot 3^1 \cdot 2 = 12$.

# Teorema d'Euler.

- **Teorema d'Euler.** Si $n$ és un enter positiu i $a$ és un enter primer amb $n$, aleshores

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

# Teorema d'Euler.

- **Teorema d'Euler.** Si $n$ és un enter positiu i $a$ és un enter primer amb $n$, aleshores
$$a^{\phi(n)} \equiv 1 \pmod{n}.$$
- **Càlcul dels residus de potències mòdul $m$.** Calcular el residu de la potència $a^n$ mòdul $m$ és trobar l'enter $r$, amb $0 \leq r < m$, tal que $a^n \equiv r \pmod{m}$.

# Teorema d'Euler.

- **Teorema d'Euler.** Si $n$ és un enter positiu i $a$ és un enter primer amb $n$, aleshores
$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

- **Càlcul dels residus de potències mòdul $m$.** Calcular el residu de la potència $a^n$ mòdul $m$ és trobar l'enter $r$, amb $0 \leq r < m$, tal que $a^n \equiv r \pmod{m}$.

- En el cas que $\text{mcd}(a, m) = 1$ i $n > \phi(m)$, si considerem la divisió entera de $n$ per $\phi(m)$,
$$n = \phi(m) \cdot q + s, \quad \text{on } 0 \leq s < \phi(m),$$
i, aplicant el teorema de Fermat, obtenim que $a^n \equiv a^s \pmod{m}$.

# Algorisme de càlcul del residu de la potència $a^n$ mòdul $m$.

1) Expresseu l'exponent $n$ en base 2. Denotem $(b_k b_{k-1} \ldots b_1 b_0)_2$ la representació de $n$ en base 2.

# Algorisme de càlcul del residu de la potència $a^n$ mòdul $m$.

1) Expresseu l'exponent $n$ en base 2. Denotem $(b_k b_{k-1} \ldots b_1 b_0)_2$ la representació de $n$ en base 2.
2) Substituïu en la representació binària anterior cada 1 pel parell de lletres $SX$, i cada 0 per la lletra $S$. A més, cal eliminar el parell $SX$ situat més a l'esquerra, és a dir, el parell $SX$ corresponent a l'element $b_k = 1$.

$$\begin{aligned} 1 &\longrightarrow SX \\ 0 &\longrightarrow S \end{aligned}$$

# Algorisme de càlcul del residu de la potència $a^n$ mòdul $m$.

1) Expresseu l'exponent $n$ en base 2. Denotem $(b_k b_{k-1} \dots b_1 b_0)_2$ la representació de $n$ en base 2.
2) Substituïu en la representació binària anterior cada 1 pel parell de lletres $SX$, i cada 0 per la lletra $S$. A més, cal eliminar el parell $SX$ situat més a l'esquerra, és a dir, el parell $SX$ corresponent a l'element $b_k = 1$.

$$\begin{aligned} 1 &\longrightarrow SX \\ 0 &\longrightarrow S \end{aligned}$$

3) Apliqueu a l'enter $a$ les següents regles de càlcul determinades per la seqüència de $S$'s i $X$'s obtinguda en el pas 2):
   - $S$ : eleveu al quadrat i reduïu mòdul $m$;
   - $X$ : multipliqueu per la base $a$ i reduïu mòdul $m$.

**Problema**

*Calculeu* $3^{2026}$ *mòdul 100.*

**Problema**

*Calculeu* $3^{2026}$ *mòdul 100.*

**Resolució:**

**Problema**

*Calculeu $3^{2026}$ mòdul 100.*

**Resolució:**

- Com que $\phi(100) = \phi(2^2 \cdot 5^2) = 2^1 \cdot 1 \cdot 5^1 \cdot 4 = 40$ i $2026 = 40 \cdot 50 + 26$, pel teorema d'Euler resulta que $3^{2026} \equiv 3^{40 \cdot 50 + 26} \pmod{100} \equiv (3^{40})^{50} \cdot 3^{26} \pmod{100} \equiv 3^{26} \pmod{100}$.

**Problema**

*Calculeu $3^{2026}$ mòdul 100.*

**Resolució:**

- Com que $\phi(100) = \phi(2^2 \cdot 5^2) = 2^1 \cdot 1 \cdot 5^1 \cdot 4 = 40$ i $2026 = 40 \cdot 50 + 26$, pel teorema d'Euler resulta que $3^{2026} \equiv 3^{40 \cdot 50 + 26} \pmod{100} \equiv (3^{40})^{50} \cdot 3^{26} \pmod{100} \equiv 3^{26} \pmod{100}$.

**Problema**

*Calculeu $3^{2026}$ mòdul 100.*

**Resolució:**

- Com que $\phi(100) = \phi(2^2 \cdot 5^2) = 2^1 \cdot 1 \cdot 5^1 \cdot 4 = 40$ i $2026 = 40 \cdot 50 + 26$, pel teorema d'Euler resulta que $3^{2026} \equiv 3^{40 \cdot 50 + 26} \pmod{100} \equiv (3^{40})^{50} \cdot 3^{26} \pmod{100} \equiv 3^{26} \pmod{100}$.
- 1) $26 = (11010)_2$.

**Problema**

*Calculeu $3^{2026}$ mòdul 100.*

**Resolució:**

- Com que $\phi(100) = \phi(2^2 \cdot 5^2) = 2^1 \cdot 1 \cdot 5^1 \cdot 4 = 40$ i $2026 = 40 \cdot 50 + 26$, pel teorema d'Euler resulta que $3^{2026} \equiv 3^{40 \cdot 50 + 26} \pmod{100} \equiv (3^{40})^{50} \cdot 3^{26} \pmod{100} \equiv 3^{26} \pmod{100}$.
- 1) $26 = (11010)_2$.
  2) $11010 \longrightarrow SXSXSSXS \longrightarrow SXSSXS$.

**Problema**

*Calculeu $3^{2026}$ mòdul 100.*

**Resolució:**

- Com que $\phi(100) = \phi(2^2 \cdot 5^2) = 2^1 \cdot 1 \cdot 5^1 \cdot 4 = 40$ i $2026 = 40 \cdot 50 + 26$, pel teorema d'Euler resulta que $3^{2026} \equiv 3^{40 \cdot 50 + 26} \pmod{100} \equiv (3^{40})^{50} \cdot 3^{26} \pmod{100} \equiv 3^{26} \pmod{100}$.
- 1) $26 = (11010)_2$.
  2) $11010 \longrightarrow SXSXSSXS \longrightarrow SXSSXS$.
  3)

$$3 \xrightarrow{S} 3^2 = 9 \xrightarrow{X} 3^3 = 27 \xrightarrow{S} 27^2 = 729 \equiv 29 \xrightarrow{S} 29^2 = 841 \equiv 41$$

$$\xrightarrow{X} 3 \cdot 41 = 123 \equiv 23 \xrightarrow{S} 23^2 = 629 \equiv 29$$

**Problema**

*Calculeu $3^{2026}$ mòdul 100.*

**Resolució:**

- Com que $\phi(100) = \phi(2^2 \cdot 5^2) = 2^1 \cdot 1 \cdot 5^1 \cdot 4 = 40$ i $2026 = 40 \cdot 50 + 26$, pel teorema d'Euler resulta que $3^{2026} \equiv 3^{40 \cdot 50 + 26} \pmod{100} \equiv (3^{40})^{50} \cdot 3^{26} \pmod{100} \equiv 3^{26} \pmod{100}$.
- 1) $26 = (11010)_2$.
  2) $11010 \longrightarrow SXSXSSXS \longrightarrow SXSSXS$.
  3)

$$3 \xrightarrow{S} \underset{=9}{3^2} \xrightarrow{X} \underset{=27}{3^3} \xrightarrow{S} \underset{\equiv 29}{\underset{=729}{27^2}} \xrightarrow{S} \underset{\equiv 41}{\underset{=841}{29^2}} \xrightarrow{X} \underset{\equiv 23}{\underset{=123}{3 \cdot 41}} \xrightarrow{S} \underset{\equiv 29}{\underset{629}{23^2}}$$

- **Solució:** $3^{26} \equiv 29 \pmod{100} \quad \Rightarrow \quad 3^{2026} \equiv 29 \pmod{100}$.