

MATEMÀTICA DISCRETA

Resum de cossos finits

Mercè Mora

Facultat d'Informàtica de Barcelona. UPC.

Curs 2006-2007/Q2

I. Cossos finits (2-22)

Repàs d'Àlgebra

R1. Divisibilitat a \mathbb{Z} (23-26)

R2. Congruències (27-28)

I. COSSOS FINITS

1. L'anell dels enters
2. L'anell \mathbb{Z}_m
3. Els cossos \mathbb{F}_p
4. Polinomis
5. L'anell de polinomis $\mathbb{K}[x]$
6. Anells quocients de polinomis
7. Cossos finits

1. L'ANEL·L DELS ENTERS (I)

- $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$; operacions: $+$, \cdot
- $(A, +, \cdot)$ és *anell commutatiu unitari* si $+$, \cdot són operacions binàries internes al conjunt A tals que:

Propietats de $(A, +)$:

associativa

commutativa

existeix e. neutre, $0 \in A$: $\forall a \in A, a + 0 = a$

tot element té simètric: $\forall a \in A, \exists a' \in A, a + a' = 0$

Propietats de (A, \cdot) :

associativa

distributiva respecte la suma

commutativa (anell *commutatiu*)

existeix e. neutre, $1 \in A$: $\forall a \in A, 1 \cdot a = a \cdot 1 = a$ (a. *unitari*)

► $(\mathbb{Z}, +, \cdot)$ és un anell commutatiu unitari

1. L'ANEL·L DELS ENTERS (II)

- ▶ Si $(A, +, \cdot)$ és anell, $\forall a \in A$, $a \cdot 0 = 0 \cdot a = 0$
- Si $(A, +, \cdot)$ és anell unitari, $a \in A$ és *invertible* si existeix $a' \in A$ tal que $a \cdot a' = a' \cdot a = 1$. Notació: a^{-1} representa l'invers de a .
- Notació: $A^* = \{a \in A \mid a \text{ és invertible}\}$
- ▶ Elements invertibles de $(\mathbb{Z}, +, \cdot)$: $1, -1$
- Si $(A, +, \cdot)$ és anell, $a \in A$, $a \neq 0$, a és *divisor de zero* si existeix $b \in A$, $b \neq 0$, tal que $a \cdot b = 0$
- ▶ $(\mathbb{Z}, +, \cdot)$ no té divisors de zero
- ▶ Els elements invertibles d'un anell unitari no són divisors de zero
- $(A, +, \cdot)$ és un *cos* si és un anell commutatiu unitari tal que tot element diferent de zero és invertible, és a dir, $A^* = A \setminus \{0\}$.
- ▶ $(\mathbb{Z}, +, \cdot)$ no és cos; $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ són cossos.

2. L'ANEL·L \mathbb{Z}_m (I)

► Fixat un enter $m \geq 2$, definim:

• Classe de a mòdul m , on $a \in \mathbb{Z}$:

$$\bar{a} = \{b \mid a \equiv b \pmod{m}\} = \{a + km \mid k \in \mathbb{Z}\}$$

► $a \in \bar{a} \neq \emptyset$; $\bigcup_{a \in \mathbb{Z}} \bar{a} = \mathbb{Z}$; $\forall a, b \in \mathbb{Z}$, o bé $\bar{a} = \bar{b}$ o bé $\bar{a} \cap \bar{b} = \emptyset$

• Conjunt d'enters mòdul m : $\mathbb{Z}_m = \{\bar{a} \mid a \in \mathbb{Z}\}$

► $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$, i té exactament m elements

• Operacions a \mathbb{Z}_m . Suma: $\bar{a} + \bar{b} = \overline{a + b}$

Producte: $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

► Resolució de les equacions $\bar{a} + \bar{x} = \bar{b}$, $\bar{a}\bar{x} = \bar{b}$ a \mathbb{Z}_m .

Equival a resoldre les equacions amb congruències

$a + x \equiv b \pmod{m}$, $ax \equiv b \pmod{m}$.

2. L'ANEL·L \mathbb{Z}_m (II)

► $(\mathbb{Z}_m, +, \cdot)$ és un anell commutatiu unitari

► $\bar{a} \in \mathbb{Z}_m$, \bar{a} és invertible $\Leftrightarrow (a, m) = 1$

▷ Càlcul de l'invers: Identitat de Bézout. Si $ax_0 + my_0 = 1$, llavors \bar{x}_0 és l'invers de \bar{a} a l'anell \mathbb{Z}_m

► $\bar{a} \in \mathbb{Z}_m$, $\bar{a} \neq \bar{0}$, \bar{a} és divisor de zero $\Leftrightarrow (a, m) \neq 1$

▷ Elements de \mathbb{Z}_m :

Si $(a, m) = m$, llavors $\bar{a} = \bar{0}$ i no és ni invertible ni divisor de zero

Si $(a, m) = 1$, llavors \bar{a} és invertible

Si $(a, m) \neq 1, m$, llavors \bar{a} és divisor de zero

3. ELS COSSOS \mathbb{F}_p

► Si $m \geq 2$, $(\mathbb{Z}_m, +, \cdot)$ és un cos $\Leftrightarrow m$ és primer.

▷ Notació: Si p és primer, escriurem \mathbb{F}_p enlloc de \mathbb{Z}_p .

▷ $\mathbb{F}_p^* = \{\bar{a} \in \mathbb{F}_p \mid \bar{a} \text{ és invertible}\} = \{\bar{a} \in \mathbb{F}_p \mid \bar{a} \neq \bar{0}\}$.

► *Teorema de Fermat.* Si p és primer,

$$\bar{a} \in \mathbb{F}_p \Rightarrow \bar{a}^p = \bar{a} \quad (\forall a \in \mathbb{Z}, a^p \equiv a \pmod{p})$$

$$\bar{a} \in \mathbb{F}_p^* \Rightarrow \bar{a}^{p-1} = \bar{1} \quad (\forall a \in \mathbb{Z}, (a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}))$$

▷ Conseqüència. Si $\bar{a} \in \mathbb{F}_p^*$, llavors $(\bar{a})^{-1} = (\bar{a})^{p-2}$

▷ Resolució de sistemes d'equacions lineals, equacions de segon grau i càlcul de potències a \mathbb{F}_p .

4. POLINOMIS (I)

- Si $(A, +, \cdot)$ és un anell, un polinomi amb coeficients en A i indeterminada x és qualsevol expressió $a_0 + a_1x + \cdots + a_nx^n$, on $a_0, a_1, \dots, a_n \in A$ i $n \geq 0$ és un natural. Direm que a_i és el *coeficient* del terme de grau i .

- $A[x]$ és el conjunt format per tots els polinomis amb coeficients en A i indeterminada x .

▷ Si un coeficient és 0, no cal escriure el terme corresponent. Si $a(x) = a_0 + a_1x + \cdots + a_nx^n$ considerarem que per a tot $j > n$, $a_j = 0$.

4. POLINOMIS (II)

- Igualtat de polinomis. Si $a(x) = a_0 + a_1x + \cdots + a_nx^n$ i $b(x) = b_0 + b_1x + \cdots + b_mx^m$, $a(x) = b(x) \Leftrightarrow a_i = b_i$, per a tot $i \geq 0$

- Operacions en $A[x]$.

Si $a(x) = a_0 + a_1x + \cdots + a_nx^n$ i $b(x) = b_0 + b_1x + \cdots + b_mx^m$,

Suma: polinomi tal que el coeficient de grau $i \geq 0$ és $a_i + b_i$

Producte: polinomi tal que el coeficient del terme de grau $i \geq 0$ és $c_i = a_0b_i + a_1b_{i-1} + \cdots + a_ib_0$.

► Si A és un anell commutatiu unitari, $(A[x], +, \cdot)$ és un anell commutatiu unitari

4. POLINOMIS (III)

- *Grau* d'un polinomi. Si $a(x) \in A[x]$, $a(x) \neq 0$, el grau de $a(x)$ és l'enter n més gran tal que el coeficient del terme de grau n és $a_n \neq 0$. El grau del polinomi 0 és $-\infty$ (o bé -1). Notació: $gr(a(x))$, $deg(a(x))$.
 - Si $a(x)$ és un polinomi de grau $n \geq 0$, a_n és el *coeficient principal* de $a(x)$.
 - Si A és un anell unitari, un polinomi és *mònic* si el seu coeficient principal és 1.
-
- ▶ Si $a(x) \neq 0$, $gr(a(x)) \geq 0$
 - ▶ $gr(a(x)) = 0 \Leftrightarrow a(x) = a_0 \in A$, $a_0 \neq 0$
 - ▶ $gr(a(x) + b(x)) \leq \max\{gr(a(x)), gr(b(x))\}$
 - ▶ Si A és un anell sense divisors de zero i $a(x), b(x) \neq 0$, llavors $gr(a(x)b(x)) = gr(a(x)) + gr(b(x))$

5. L'ANEL·L DE POLINOMIS $\mathbb{K}[x]$ (I)

Estudi de $\mathbb{K}[x]$, on \mathbb{K} és un cos (p.e. $\mathbb{F}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$).

► Els elements invertibles de $\mathbb{K}[x]$ són els polinomis de grau 0, és a dir, $\mathbb{K}[x]^* = \mathbb{K}^* = \mathbb{K} \setminus \{0\}$

► *Teorema de la divisió.* Si $a(x), b(x) \in \mathbb{K}[x]$, $b(x) \neq 0$, existeixen $q(x), r(x) \in \mathbb{K}[x]$ únics tals que $a(x) = b(x)q(x) + r(x)$, $gr(r(x)) < gr(b(x))$.

• $q(x)$ i $r(x)$ s'anomenen respectivament *quocient* i *residu* de la divisió de $a(x)$ per $b(x)$.

• Si $a(x), b(x) \in \mathbb{K}[x]$, direm que $b(x)$ *divideix* $a(x)$ (o bé $b(x)$ és *divisor* de $a(x)$, o bé $a(x)$ és *múltiple* de $b(x)$) si el residu de la divisió de $a(x)$ per $b(x)$ és 0. Notació: $b(x)|a(x)$, $a(x) = b(x)q(x)$.

5. L'ANEL·L DE POLINOMIS $\mathbb{K}[x]$ (II)

- Divisors *impropis* de $a(x)$: polinomis de grau 0 i polinomis de la forma $ka(x)$, on $k \in \mathbb{K}^*$.
- Divisors *propis*: divisors no impropis
- Polinomi *irreductible*: polinomi de grau ≥ 1 que no té divisors propis. (El polinomi no es pot descompondre com a producte de dos polinomis de grau estrictament menor).

- $\alpha \in K$ és arrel de $a(x)$ si $a(\alpha) = 0$.

- ▶ Teorema de l'arrel (o residu).

$\alpha \in K$ és arrel de $a(x) \Leftrightarrow (x - \alpha) | a(x)$

- ▶ Si $a(x)$ és polinomi de grau $n \geq 0$, $a(x)$ té com a molt n arrels.

- ▶ Els polinomis de grau 1 són irreductibles i tenen exactament una arrel

- ▶ Si un polinomi de grau ≥ 2 té una arrel, no és irreductible

- ▶ Els polinomis de grau 2 ó 3 són irreductibles \Leftrightarrow no tenen cap arrel

5. L'ANEL·L DE POLINOMIS $\mathbb{K}[x]$ (III)

► Tot polinomi de grau ≥ 1 es pot escriure de forma única com a producte d'un polinomi de grau 0 i polinomis mòncics irreductibles, llevat de l'ordre dels factors:

Si $a(x) \in \mathbb{K}[x]$, $gr(a(x)) \geq 1$, llavors $a(x) = k p_1(x)^{\alpha_1} \dots p_r(x)^{\alpha_r}$, on $p_i(x)$ són polinomis mòncics irreductibles, i $\forall i, \alpha_i > 0$.

● *Màxim comú divisor* de $a(x)$ i $b(x)$: polinomi de grau màxim que és divisor alhora de $a(x)$ i de $b(x)$

Notació: $\text{mcd}(a(x), b(x))$ o bé $(a(x), b(x))$

► Si $d(x)$ és un màxim comú divisor de $a(x)$ i $b(x)$, llavors $k d(x)$, $k \in \mathbb{K}^*$, també ho és.

► Si $d(x)$, $d'(x)$ són màxims comuns divisors de $a(x)$ i $b(x)$, llavors $d'(x) = k d(x)$, per a algun $k \in \mathbb{K}^*$.

5. L'ANEL·L DE POLINOMIS $\mathbb{K}[x]$ (IV)

► *Algorisme d'Euclides.* Si $a(x), b(x)$ són polinomis de $\mathbb{K}[x]$, $b(x) \neq 0$, i considerem les divisions successives

$$a(x) = b(x)q(x) + r_0(x), \text{ gr}(r_0(x)) < \text{gr}(b(x))$$

$$b(x) = r_0(x)q_0(x) + r_1(x), \text{ gr}(r_1(x)) < \text{gr}(r_0(x))$$

$$r_0(x) = r_1(x)q_1(x) + r_2(x), \text{ gr}(r_2(x)) < \text{gr}(r_1(x))$$

$$r_1(x) = r_2(x)q_2(x) + r_3(x), \text{ gr}(r_3(x)) < \text{gr}(r_2(x))$$

...

$$r_{n-2}(x) = r_{n-1}(x)q_{n-1}(x) + r_n(x), \text{ gr}(r_n(x)) < \text{gr}(r_{n-1}(x))$$

$$r_{n-1}(x) = r_n(x)q_n(x) + 0$$

llavors $(a(x), b(x)) = r_n(x)$.

► *Identitat de Bézout.* Si $a(x), b(x)$ són polinomis no nuls de $\mathbb{K}[x]$ tals que $(a(x), b(x)) = d(x)$, existeixen polinomis $p(x), q(x)$ de $\mathbb{K}[x]$ tals que $a(x)p(x) + b(x)q(x) = d(x)$.

5. L'ANEL·L DE POLINOMIS $\mathbb{K}[x]$ (V)

► Càlcul del m.c.d. i de la identitat de Bézout. Si $a(x), b(x) \in \mathbb{K}[x]$, $b(x) \neq 0$ i considerem les divisions successives de l'algorisme d'Euclides, tenim:

1	0	$s_0(x)$	$s_1(x)$	\cdots	$s_{n-2}(x)$	$s_{n-1}(x)$	$s_n(x)$
0	1	$t_0(x)$	$t_1(x)$	\cdots	$t_{n-2}(x)$	$t_{n-1}(x)$	$t_n(x)$
	$q(x)$	$q_0(x)$	$q_1(x)$	\cdots	$q_{n-2}(x)$	$q_{n-1}(x)$	$q_n(x)$
$a(x)$	$b(x)$	$r_0(x)$	$r_1(x)$	\cdots	$r_{n-2}(x)$	$r_{n-1}(x)$	$r_n(x)$
$r_0(x)$	$r_1(x)$	$r_2(x)$	$r_3(x)$	\cdots	$r_n(x)$	0	

on: $s_0(x) = 1$, $t_0(x) = -q(x)$,

$$s_1(x) = -q_0(x), \quad t_1(x) = 1 + q(x)q_0(x),$$

$$\forall i \geq 2, \quad s_i(x) = s_{i-2}(x) - s_{i-1}(x)q_{i-1}(x),$$

$$\forall i \geq 2, \quad t_i(x) = t_{i-2}(x) - t_{i-1}(x)q_{i-1}(x).$$

Llavors: $\forall i \geq 0$, $r_i(x) = a(x)s_i(x) + b(x)t_i(x)$

En particular: $(a(x), b(x)) = r_n(x) = a(x)s_n(x) + b(x)t_n(x)$

6. ANELLS QUOCIENTS DE POLINOMIS (I)

• Si $f(x) \in \mathbb{K}[x]$, $a(x) \equiv b(x) \pmod{f(x)} \Leftrightarrow f(x) \mid b(x) - a(x) \Leftrightarrow$
 \Leftrightarrow al dividir $a(x)$, $b(x)$ entre $f(x)$ s'obté el mateix residu

► Fixat un polinomi no nul $f(x) \in \mathbb{K}[x]$, $a(x) \equiv b(x) \pmod{f(x)}$ és una relació d'equivalència a $\mathbb{K}[x]$, tal que:

▷ Classe d'equivalència de $a(x) \in \mathbb{K}[x]$:

$$\begin{aligned}\overline{a(x)} &= \{b(x) \mid a(x) \equiv b(x) \pmod{f(x)}\} = \\ &= \{a(x) + k(x)f(x) \mid k(x) \in \mathbb{K}[x]\}\end{aligned}$$

▷ Conjunt quocient: $\mathbb{K}[x]/(f(x)) = \{\overline{a(x)} \mid a(x) \in \mathbb{K}[x]\}$

▷ $\mathbb{K}[x]/(f(x))$ té tants elements com possibles residus de dividir polinomis per $f(x)$: si $\text{gr}(f(x)) = n$, n'hi tants com polinomis de $K[x]$ de grau $< n$.

► Operacions a $\mathbb{K}[x]/(f(x))$

$$\text{Suma: } \overline{a(x)} + \overline{b(x)} = \overline{a(x) + b(x)}$$

$$\text{Producte: } \overline{a(x)} \cdot \overline{b(x)} = \overline{a(x) \cdot b(x)}$$

6. ANELLS QUOCIENTS DE POLINOMIS (II)

- $(\mathbb{K}[x]/(f(x)), +, \cdot)$ és un anell commutatiu unitari.
- ▶ Els elements invertibles de $(\mathbb{K}[x]/(f(x)), +, \cdot)$ són les classes $\overline{a(x)}$ tals que $(a(x), f(x)) = 1$. Càlcul de l'invers: amb la Identitat de Bézout.
- ▶ $(\mathbb{K}[x]/(f(x)), +, \cdot)$ és un cos $\Leftrightarrow f(x)$ és un polinomi irreductible
- ▶ Si $\mathbb{K} = \mathbb{F}_p$ i $f(x)$ és un polinomi irreductible de grau d , llavors $(\mathbb{F}_p[x]/(f(x)), +, \cdot)$ és un cos amb p^d elements.

7. COSSOS FINITS (I)

- *Ordre* d'un cos: nombre d'elements del cos
- *Cos finit*: cos d'ordre finit

▷ Notació: \mathbb{F}_q representa un cos finit d'ordre q . El conjunt d'elements invertibles de \mathbb{F}_q és $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$

► Hi ha cossos finits d'ordre p^d , per a tot p primer i $d \geq 1$

Construcció:

Si $d = 1$, \mathbb{F}_p és un cos d'ordre p

Si $d \geq 2$, $\mathbb{F}_{p^d} = \mathbb{F}_p[x]/(f(x))$, on $f(x)$ és un polinomi irreductible de $\mathbb{F}_p[x]$ de grau d

7. COSSOS FINITS (II)

• L'ordre de $a \in \mathbb{F}_q^*$ és l'enter $t \geq 1$ més petit tal que $a^t = 1$

► Si $a \in \mathbb{F}_q^*$ és un element d'ordre t :

(1) $t | q - 1$

(2) $a^s = 1 \Leftrightarrow t | s$

(3) $a^{q-1} = 1$

(4) l'ordre de a^i és $t / (i, t)$

► El nombre d'elements d'ordre d de \mathbb{F}_q^* és $\begin{cases} \Phi(d), & \text{si } d | q - 1, \\ 0, & \text{altrament.} \end{cases}$

• $a \in \mathbb{F}_q^*$ és un element *primitiu* de \mathbb{F}_q si té ordre $q - 1$

► Tot cos finit té almenys un element primitiu

► El nombre d'elements primitius de \mathbb{F}_q és $\Phi(q - 1)$

7. COSSOS FINITS (III)

► Si a és un element primitiu de \mathbb{F}_q , llavors $\mathbb{F}_q = \{0, a, a^2, a^3, \dots, a^{q-1}\}$ i el producte de dos elements de \mathbb{F}_q és $a^i a^j = a^{i+j}$

• Polinomi *primitiu* de $\mathbb{F}_p[x]$: polinomi irreductible tal que $\alpha = \bar{x}$ és un element primitiu del cos $\mathbb{F}_p[x]/(f(x))$

► Si $\mathbb{F}_q = \mathbb{F}_p[x]/(f(x))$ i $f(x)$ és un polinomi primitiu, tots els elements de \mathbb{F}_q^* es poden expressar com a potències de $\alpha = \bar{x}$:
 $\mathbb{F}_q = \{0, \alpha, \alpha^2, \dots, \alpha^{q-1}\}$

Per a operar en aquest cos es construeixen taules de logaritmes en base α :

i	1	2	...	$q-1$
α^i	α	α^2	...	1

Per a multiplicar dos elements només cal sumar els exponents respecte de α (logaritmes en base α) i per a sumar utilitzem l'expressió com a classe d'un polinomi de grau menor que $d = \text{gr}(f(x))$.

7. COSSOS FINITS (IV)

- *Funció μ de Möbius.* Per a a enter positiu, definim:

$$\mu(a) = \begin{cases} 1, & \text{si } a = 1, \\ (-1)^k, & \text{si } a \text{ és producte de } k \text{ primers diferents,} \\ 0, & \text{si per a algun primer } p, p^2|a. \end{cases}$$

► El polinomi $x^{q^n} - x$ és el producte de tots els polinomis de $\mathbb{F}_q[x]$ mòncics irreductibles de grau d , $d|n$.

► El nombre de polinomis mòncics irreductibles de grau r de $\mathbb{F}_q[x]$ és

$$N_q(r) = \frac{1}{r} \sum_{d|r} \mu(d) q^{r/d}$$

7. COSSOS FINITS (V)

- *Característica* d'un cos:

$$\begin{cases} 0, & \text{si els elements } 1, 1 + 1, 1 + 1 + 1, \dots \text{ són tots diferents} \\ k, & \text{si } \overbrace{1 + \dots + 1}^{k)} = 0, \text{ i } \overbrace{1 + \dots + 1}^{h)} \neq 0 \text{ si } h < k, . \end{cases}$$

- ▶ La característica d'un cos és 0 o bé un nombre primer.
- ▶ $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ són cossos de característica 0
- ▶ Si $q = p^d$, p primer, \mathbb{F}_q és un cos de característica p .

R1. DIVISIBILITAT A \mathbb{Z} (I)

► *Teorema de la divisió.* Per a tot parell d'enters a i b , $b \neq 0$, existeixen enters q, r únics tals que $a = bq + r$, $0 \leq r < |b|$.

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

- Si $a, b \in \mathbb{Z}$, direm que b *divideix* a (o bé b és *divisor* de a , o bé a és *múltiple* de b) si el residu de fer la divisió entera de a entre b és 0. Notacions: $b|a$, $a = \dot{b}$.

- Divisors *impropis* de a : $1, -1, a, -a$

- Divisors *propis*: divisors no impropis.

- Nombre *primer*: enter $a \geq 2$ tal que els únics divisors de a són els divisors impropis, $1, -1, a, -a$

- *Màxim comú divisor* de a, b : l'enter més gran que és alhora divisor de a i de b . Notació: (a, b)

- Els enters a, b són *relativament primers* si $(a, b) = 1$

R1. DIVISIBILITAT A \mathbb{Z} (II)

- ▶ El m.c.d. de dos enters és un enter positiu únic
- ▶ Si $b > 0$, $b|a \Leftrightarrow (a, b) = b$
- ▶ $a = bq + r \Rightarrow (a, b) = (b, r)$
- ▶ *Algorisme d'Euclides.* Si a, b són enters positius, $a \geq b > 0$, i considerem les divisions enteres successives

$$a = bq + r_0$$

$$b = r_0q_0 + r_1$$

$$r_0 = r_1q_1 + r_2$$

$$r_1 = r_2q_2 + r_3$$

...

$$r_{n-2} = r_{n-1}q_{n-1} + r_n$$

$$r_{n-1} = r_nq_n + 0,$$

llavors $(a, b) = r_n$.

- ▶ *Identitat de Bézout.* Si $(a, b) = d$, existeixen enters x, y tals que $ax + by = d$.

R1. DIVISIBILITAT A \mathbb{Z} (III)

► Donats a, b enters tals que $(a, b) = d$, l'equació $ax + by = c$ té solució si, i només si, $d|c$. Càlcul d'una solució: a partir de la identitat de Bézout.

► Càlcul del m.c.d. i de la identitat de Bézout. Si a, b són enters, $a > b > 0$, considerem les divisions successives obtingudes a l'algorisme d'Euclides:

1	0	s_0	s_1	\cdots	s_{n-2}	s_{n-1}	s_n
0	1	t_0	t_1	\cdots	t_{n-2}	t_{n-1}	t_n
	q	q_0	q_1	\cdots	q_{n-2}	q_{n-1}	q_n
a	b	r_0	r_1	\cdots	r_{n-2}	r_{n-1}	r_n
r_0	r_1	r_2	r_3	\cdots	r_n	0	

on: $s_0 = 1, t_0 = -q, s_1 = -q_0, t_1 = 1 + q q_0,$

$\forall i \geq 2, s_i = s_{i-2} - s_{i-1} q_{i-1}, t_i = t_{i-2} - t_{i-1} q_{i-1}.$

Llavors: $\forall i \geq 0, r_i = a s_i + b t_i$

En particular: $(a, b) = r_n = a s_n + b t_n$

R1. DIVISIBILITAT A \mathbb{Z} (IV)

▶ $r|a, r|b \Rightarrow r|(a, b)$

▶ Si p és primer, $p|ab \Rightarrow p|a$ ó $p|b$

▶ $a|bc$ i $(a, b) = 1 \Rightarrow a|c$

▶ *Teorema fonamental de l'aritmètica.* Tot enter $a \geq 2$ es pot expressar com a producte de nombres primers de forma única, llevat l'ordre dels factors.

▶ Notació: $a \in \mathbb{Z}$ és pot expressar de forma única com:

$$a = (\pm 1)p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad p_1 < p_2 < \cdots < p_k \text{ primers, } \forall i, \alpha_i > 0.$$

R2. CONGRUÈNCIES (I)

- Enters *congruents mòdul* m : $a \equiv b \pmod{m} \Leftrightarrow m|b - a$

► Les condicions següents són equivalents:

(1) $m|b - a$

(2) $b = a + m$

(3) la divisió entera de a i b entre m dóna el mateix residu

(4) $\{a + mk \mid k \in \mathbb{Z}\} = \{b + mk \mid k \in \mathbb{Z}\}$

► Propietats:

(1) $a \equiv a \pmod{m}$

(2) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

(3) $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

(4) $a \equiv b \pmod{m}, a' \equiv b' \pmod{m} \Rightarrow$
 $\Rightarrow a + a' \equiv b + b' \pmod{m}, aa' \equiv bb' \pmod{m}$

(5) $a \equiv b \pmod{m}, d|m \Rightarrow a \equiv b \pmod{d}$

(6) $a \equiv b \pmod{r}, a \equiv b \pmod{s} \Rightarrow a \equiv b \pmod{\text{mcm}(r, s)}$

(7) $ra \equiv rb \pmod{m} \Leftrightarrow a \equiv b \pmod{m/(m, r)}$

R2. CONGRUÈNCIES (II)

Equacions amb congruències:

► L'equació $a + x \equiv b \pmod{m}$ sempre té solució, i és $x \equiv b - a \pmod{m}$

► L'equació $ax \equiv b \pmod{m}$ té solució $\Leftrightarrow (a, m) | b$.

En aquest cas, podem trobar una solució a partir de la identitat de Bézout:

$(a, m) = d = ax_0 + my_0 \Rightarrow \frac{x_0 b}{d}$ és una solució