1 Introducció

El conjunt dels nombres enters, que designem per $\mathbb{Z}$, sorgeix de la necessitat d'ampliar els naturals perquè les equacions $x + m = n$ amb $m > n$ tinguin solució, en particular $x + m = 0$ (obtenció dels simètrics o oposats dels naturals). L'operació que es defineixi en aquest conjunt ha d'estendre la de $\mathbb{N}$ de forma natural, i també ha de verificar-se $\mathbb{N} \subset \mathbb{Z}$ de forma canònica.

2 Construcció de $\mathbb{Z}$

Definim a $\mathbb{N} \times \mathbb{N}$ una relació $\sim$ així: $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$. Aquesta relació és d'equivalència:

- Prop. reflexiva: $a + b = b + a \;\Rightarrow\; (a, b) \sim (a, b)$
- Prop. simètrica: $a+d = b+c \;\Leftrightarrow\; c+b = d+a$, per tant $(a, b) \sim (c, d) \;\Leftrightarrow\; (c, d) \sim (a, b)$
- Prop. transitiva: $a+d = b+c,\ c+f = d+e \;\Rightarrow a+d+c+f = b+c+d+e \;\Rightarrow a+f = b+e$, per tant $(a, b) \sim (c, d),\ (c, d) \sim (e, f) \;\Rightarrow (a, b) \sim (e, f)$

Llavors definim $\mathbb{Z}$ com el conjunt quocient $\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/\sim$. Donat $[(a, b)] \in \mathbb{Z}$ podem triar un representant més senzill per la classe distingint tres casos:

- Si $a > b \;\Rightarrow\; a = b + m \;\Rightarrow\; (a, b) \sim (m, 0) \;\Rightarrow\; [(a, b)] = [(m, 0)]$. Escriurem $[(m, 0)] = +m$ o simplement m, i $\mathbb{Z}^+ = \{[(m, 0)] \mid m \in \mathbb{N} - \{0\}\}$ l'anomenarem el conjunt dels *enters positius.*
- Si $a < b \;\Rightarrow\; b = a + m \;\Rightarrow\; (a, b) \sim (0, m) \;\Rightarrow\; [(a, b)] = [(0, m)]$. Escriurem $[(0, m)] = -m$, i $\mathbb{Z}^- = \{[(0, m)] \mid m \in \mathbb{N} - \{0\}\}$ l'anomenarem el conjunt dels *enters negatius.*
- Si $a = b \;\Rightarrow\; (a, b) \sim (0, 0) \;\Rightarrow\; [(a, b)] = [(0, 0)]$. Escriurem $[(0, 0)] = 0$.

Amb això tenim que $\mathbb{Z} = \mathbb{Z}^+ \cup \{0\} \cup \mathbb{Z}^-$, i tenim una funció injectiva trivial $f : \mathbb{N} \longrightarrow \mathbb{Z}$ posant $f(0) = 0,\ f(m) = +m$.

Definim la suma de dos elements de $\mathbb{Z}$ com $[(a, b)] + [(c, d)] = [(a + c, b + d)]$. Es veu molt fàcilment que aquesta suma està ben definida, és a dir, que no depèn dels representats escollits de cada classe. Les seves propietats elementals són, com a $\mathbb{N}$, l'associativa, commutativa, i existència i unicitat d'element neutre (el $[(0,0)]$). A aquestes propietats hi afegim l'existència i unicitat de l'oposat de tot element de $\mathbb{Z}$ (l'oposat de $[(a,b)]$ és el $[(b,a)]$). No les demostrem per trivials.

Definim el producte de dos elements de $\mathbb{Z}$ com $[(a,b)]\cdot[(c,d)] = [(ac+bd, ad+bc)]$. Aquesta operació no depèn dels representants triats, i es veu fàcilment en dos passos: primer suposar que $[(a,b)] = [(a', b,')]$, $[(c,d)] = [(c', d,')]$ i provar que $[(a,b)]\cdot[(c,d)] = [(a',b')]\cdot[(c,d)]$. Després provar que $[(a',b')]\cdot[(c,d)] = [(a',b')]\cdot[(c',d')]$ i finalment aplicar la transitivitat per concloure que $[(a,b)]\cdot[(c,d)] = [(a',b')]\cdot[(c',d')]$. Les propietats elementals del producte són l'associativa, commutativa, existència i unicitat d'element neutre (el $[(1,0)]$) i distributiva respecte de la suma. N'obviem la prova.

Altres propietats importants del producte són:

- *Llei de simplificació:* $m\cdot n = m\cdot p \;\Rightarrow\; n = p$ per a tot enter $m\neq 0$. En efecte, si $m = [(a,b)]$, $n = [(c,d)]$, $p = [(e,f)]$,

$$\begin{aligned} m\cdot n = m\cdot p \;&\Leftrightarrow\; [(ac+bd, ad+bc)] = [(ae+bf, af+be)] \;\Leftrightarrow \\ &\Leftrightarrow\; ac+bd+af+be = ad+bc+ae+bf \;\Leftrightarrow \\ &\Leftrightarrow\; (a-b)(c+f) = (a-b)(d+e). \end{aligned}$$

  Sabem que $a-b\neq 0$ en ser $m\neq 0$. Si $a<b$ escrivim l'última expressió canviada de signe: $(b-a)(c+f) = (b-a)(d+e)$, i en qualsevol cas podem aplicar la llei de simplificació a $\mathbb{N}$, obtenint $c+f = d+e$, que és $n = p$.

- *Existència d'element absorbent:* $m\cdot 0 = 0$ per a tot m. En efecte, $m\cdot 0 = m\cdot(0+0) = m\cdot 0 + m\cdot 0$. Sumant l'oposat de $m\cdot 0$ a tots dos membres obtenim allò que buscàvem.

- *Absència de divisors de* 0 *no trivials:* $\forall m,n\in\mathbb{Z}$, $m\cdot n = 0 \;\Leftrightarrow\; m = 0$ o $n = 0$ (aquesta propietat també s'enuncia dient que $\mathbb{Z}$ és un *domini d'integritat*). En efecte, si $m = [(a,b)]$, $n = [(c,d)]$,

$$\begin{aligned} m\cdot n = 0 \;&\Leftrightarrow\; [(a,b)]\cdot[(c,d)] = [(0,0)] \;\Leftrightarrow\; [(ac+bd, ad+bc)] = [(0,0)] \;\Leftrightarrow \\ &\Leftrightarrow\; ac+bd = ad+bc \;\Leftrightarrow\; (a-b)c = (a-b)d. \end{aligned}$$

  Si $m = 0$ hem acabat. En cas contrari tindrem $a-b\neq 0$ i, com abans, apliquem la llei de simplificació de $\mathbb{N}$ canviant el signe si convé, obtenint $c = d$ que és $n = 0$.

- *Regla dels signes:*

  - $(+m)\cdot(+n) = [(m,0)]\cdot[(n,0)] = [(mn,0)] = +(mn)$.
  - $(+m)\cdot(-n) = [(m,0)]\cdot[(0,n)] = [(0,mn)] = -(mn)$.

- $(-m) \cdot (+n) = [(0, m)] \cdot [(n, 0)] = [(0, mn)] = -(mn)$.
- $(-m) \cdot (-n) = [(0, m)] \cdot [(0, n)] = [(mn, 0)] = +(mn)$.

Amb totes les propietats vistes, $(\mathbb{Z}, +)$ és un grup abelià i $(\mathbb{Z}, \cdot)$ és un semigrup abelià i unitari amb propietat distributiva, de manera que $(\mathbb{Z}, +, \cdot)$ té una estructura d'*anell commutatiu i unitari*.

3 Ideals a $\mathbb{Z}$

La teoria de la divisibilitat a $\mathbb{Z}$ és conseqüència del següent important teorema:

Teorema de la divisió entera. *Donats $a, b \in \mathbb{Z}$, $b \neq 0$, existeixen $q, r \in \mathbb{Z}$ únics tal que $a = bq + r$ amb $0 \leq r < |b|$. q i r s'anomenen el* quocient *i la* resta *de la divisió entera de a per b.*

Demostració. Suposem que $b > 0$ (el cas $b < 0$ es demostra anàlogament). Sigui $S = \{a - bn \mid n \in \mathbb{Z} \text{ i } a - bn \in \mathbb{N}\} \neq \emptyset$ doncs per $n = -a^2$, $a - bn = a(1 + ab) \geq 0$. Pel principi de bona ordenació de $\mathbb{N}$, $\exists r = \min(S) \Rightarrow r = a - bq$ per algun $q \in \mathbb{Z} \Rightarrow a = bq + r$ amb $r \geq 0$. A més $r < b$, en efecte, suposem $r \geq b \Rightarrow 0 \leq r - b = a - bq - b = a - b(q+1)$. Per tant $r - b \in S$ amb $r - b < r$, en contradicció amb $r = \min(S)$.

Per veure la unicitat suposem que existeixen $q, r, q', r' \in \mathbb{Z}$ tals que $a = bq + r = bq' + r'$ amb $0 \leq r < b$, $0 \leq r' < b$. Sense pèrdua de generalitat podem suposar $r' \leq r$. Llavors tenim que $b(q' - q) = r - r'$. Com $b > 0$ i $r - r' \geq 0$ tenim $q' - q \geq 0$. Però $r - r' < b$ i aleshores $b(q' - q) < b \Rightarrow q - q' = 0 \Rightarrow q = q'$, $r = r'$. $\square$

Si la resta de la divisió entera de a per b és 0 diem que b *divideix* a o que és un *divisor* de a (i escrivim $b|a$), o bé que a és *divisible* per b, o un *múltiple* de b. Escrivim el conjunt de múltiples de b com (b) i és evident que aquest conjunt verifica: $\forall m, n \in (b)$, $c \in \mathbb{Z} \Rightarrow m + n \in (b)$, $mc \in (b)$.

Algunes propietats bàsiques que es dedueixen immediatament de la definició de divisibilitat són:

- Reflexivitat: $a|a \ \forall a \in \mathbb{Z}$, doncs $a = a \cdot 1$.
- $a|0 \ \forall a \in \mathbb{Z}$, doncs $0 = a \cdot 0$.
- Transitivitat: $a|b$, $b|c \Rightarrow a|c$, doncs $ak = b$, $bl = c \Rightarrow akl = c \Rightarrow a|c$.

- $a|b,\ b|a \ \Rightarrow \ a = \pm b$, doncs $ak = b,\ bl = a \ \Rightarrow \ akl = a$. Si $a = 0 \ \Rightarrow \ b = 0$, i si $a \neq 0 \ \Rightarrow \ kl = 1 \ \Rightarrow \ k = l = 1$ ó $k = l = -1$.
- $a|b,\ a|c \ \Rightarrow \ a|b + c$, doncs $b = ak,\ c = al \ \Rightarrow \ b + c = a(k + l)$.
- $a|b \ \Rightarrow \ a|bc\ \forall c \in \mathbb{Z}$, doncs $b = ak \ \Rightarrow \ bc = a(kc)$.

Direm que un subconjunt no buit $I \subset \mathbb{Z}$ és un *ideal* si verifica: $\forall m, n \in I,\ c \in \mathbb{Z} \ \Rightarrow \ m + n \in I,\ mc \in I$. Per exemple, el conjunt de múltiples d'un nombre, (b), verifica la definició d'ideal.

Proposició. *Tots els ideals $I \subset \mathbb{Z}$ són de la forma $I = (b)$ per algun b.*

Demostració. Si $I = \{0\}$ llavors $I = (0)$. Si $I \neq \{0\}$ $\exists a \neq 0,\ a \in I$, i I conté elements positius (si $a < 0$ també conté $-a = a \cdot (-1)$). Sigui b el positiu més petit de I. Per definició d'ideal, $(b) \subset I$. Per veure la inclusió en l'altre sentit, sigui $a \in I$ i, pel teorema de la divisió entera, escrivim $a = bq + r$. Llavors $r = a + b(-q) \in I$ amb $0 \leq r < b$, i com b era el positiu més petit de I ha de ser $r = 0$ i per tant $a \in (b)$. $\square$

Amb tot això observem que podem expressar la divisibilitat en termes d'inclusions d'ideals: $b|a \ \Leftrightarrow \ (a) \subset (b)$.

4 Mínim comú múltiple i màxim comú divisor

Donats els enters $a_1, \ldots a_n$, la intersecció d'ideals $(a_1) \cap \cdots \cap (a_n)$ és el conjunt dels enters que són múltiples comuns a tots ells. És evident que aquest conjunt compleix la definició d'ideal, i per tant, per la proposició anterior existeix un m tal que $(a_1) \cap \cdots \cap (a_n) = (m)$, de manera que m és múltiple comú dels a_i i qualsevol altre m' múltiple comú dels a_i complirà $m' \in (m) \ \Rightarrow \ m|m'$. Direm que aquest m és el *mínim comú múltiple* de $a1, \ldots, a_n$ i escriurem $m = \mathrm{mcm}(a_1, \ldots, a_n)$. Segons la definició tenim que $-m$ també és mcm de $a_1, \ldots, a_n$, però per conveni triarem el valor positiu.

Si considerem ara la unió $(a_1) \cup \cdots \cup (a_n)$, en general no és un ideal. Però construïm un subconjunt $I \subset \mathbb{Z}$ que contingui aquesta unió i verifiqui les condicions d'ideal. Sigui $I = \{a_1c_1 + \cdots + a_nc_n \mid c_1, \ldots, c_n \in \mathbb{Z}\}$, que és un ideal i per tant $I = (d)$ per algun $d \in \mathbb{Z}$. Notarem $I = (a_1, \ldots, a_n) = (d)$. Com $a_i \in I = (d)\ \forall i = 1, \ldots, n$, tenim que d és divisor comú dels a_i. Si d' és un altre divisor comú dels a_i llavors $a_i \in (d')$ i per tant $\{a_1c_1 + \cdots + a_nc_n \mid c_i \in \mathbb{Z}\} \subset (d')$, és a dir, $(d) \subset (d')$, que vol dir $d'|d$. Direm que aquest d és el *màxim comú divisor* de $a1, \ldots, a_n$ i escriurem $d = \mathrm{mcd}(a_1, \ldots, a_n)$. Com abans, $-d$ també és mcd de $a_1, \ldots, a_n$, però per conveni triarem el valor positiu.

En el transcurs d'aquesta definició hem demostrat una propietat important:

Identitat de Bézout. *Si* $d = \mathrm{mcd}(a_1, \ldots, a_n)$ *llavors existeixen* $c_1, \ldots, c_n \in \mathbb{Z}$ *tals que* $d = a_1c_1 + \cdots + a_nc_n$. $\square$

El següent resultat ens proporciona un mètode pràctic per calcular el mcd de dos nombres:

Proposició. *Si* $a = bq + r$ *és la divisió entera de* a *per* b*, llavors* $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$.

Demostració. És conseqüència del fet que $(a, b) = (b, r)$. En efecte, $ac_1 + bc_2 \in (a, b)$ és $ac_1 + bc_2 = b(qc_1 + c_2) + rc_1 \in (b, r)$ i, recíprocament, $bn_1 + rn_2 \in (b, r)$ és $bn_1 + rn_2 = an_2 + b(n_1 - qn_2) \in (a, b)$. $\square$

L'*algorisme d'Euclides* consisteix a aplicar reiteradament aquesta proposició:

$$\begin{array}{lll} a = bq + r & (a, b) = (b, r) & r < |b| \\ b = rq_1 + r1 & (b, r) = (r, r_1) & r_1 < r \\ r = r_1q_2 + r_2 & (r, r_1) = (r_1, r_2) & r_2 < r_1 \\ \cdots & \cdots & \cdots \end{array}$$

Obtenim una successió decreixent de restes, per tant arribarà un moment que tindrem una resta igual a 0:

$$\begin{array}{lll} r_{k-2} = r_{k-1}\, q_k + r_k & (r_{k-2}, r_{k-1}) = (r_{k-1}, r_k) & r_k < r_{k-1} \\ r_{k-1} = r_k\, q_{k+1} + 0 & (r_{k-1}, r_k) = (r_k, 0) = (r_k). & \end{array}$$

Així doncs $(a, b) = (r_k)$, és a dir, $r_k = \mathrm{mdc}(a, b)$. Si hem de calcular el mcd de més de dos nombres aplicarem $\mathrm{mcd}(a_1, a_2, a_3) = \mathrm{mcd}(\mathrm{mcd}(a_1, a_2), a_3)$ i, en general, $\mathrm{mcd}(a_1, \ldots, a_n) = \mathrm{mcd}(\mathrm{mcd}(a_1, \ldots, a_{n-1}), a_n)$.

Un cop desenvolupat l'algorisme d'Euclides, fent una substitució enrere podem obtenir la identitat de Bézout. En efecte, $d = r_k = r_{k-2} - r_{k-1}\, q_k$. Però r_{k-1} també es pot escriure com una suma de múltiples de r_{k-2} i r_{k-3}; r_{k-2} és suma de múltiples de r_{k-3} i r_{k-4}, i així succesivament fins a obtenir la identitat de Bézout: $d = ar + bs$.

Direm que dos enters a, b són *primers entre ells* o *coprimers* si $\mathrm{mcd}(a, b) = 1$.

Teorema d'Euclides. *Si* $a|bc$ *i* $\mathrm{mcd}(a, b) = 1$ *llavors* $a|c$.

Demostració. La identitat de Bézout ens permet escriure $ar + bs = 1$. Multiplicant per c tenim $acr + bcs = c$, i com a divideix els dos sumands, tenim que $a|c$. $\square$

El següent resultat ens permet trobar immediatament el mcm de dos nombres coneixent el mcd, i viceversa:

Proposició. *Si $m = \mathrm{mcm}(a,b)$ i $d = \mathrm{mcd}(a,b)$ llavors $md = |ab|$.*

Demostració. Posem $a = da'$, $b = db'$ i volem veure que $m = d|a'b'|$ és el mcm de a i b. Que és múltiple comú de a i b és evident. Sigui n un altre múltiple comú de a i b: $n = ar = bs$. Llavors $a'dr = b'ds \Rightarrow a'r = b's$ amb $\mathrm{mcd}(a', b') = 1$. Pel teorema d'Euclides tenim que $a'|s \Rightarrow s = a't \Rightarrow n = b'ds = da'b't$ i per tant n és múltiple de $da'b'$. □

5 Els nombres primers

Un nombre enter $p \in \mathbb{Z} - \{\pm 1\}$ es diu *primer* si els seus únics divisors són ± 1 i $\pm p$.

Proposició. *Si p és primer i $p|ab$ llavors $p|a$ o $p|b$.*

Demostració. Si $p \not| a$ com els únics divisors positius de p són 1 i p, tenim que $\mathrm{mcd}(p, a) = 1$. Llavors, pel teorema d'Euclides, $p|b$. □

Proposició. *El conjunt de nombres primers és infinit.*

Demostració. Si tenim un conjunt finit de primers $S = \{p_1, \dots, p_n\}$ podem trobar un nou primer $p \notin S$. En efecte, sigui $a = p_1 \cdots p_n + 1$ i sigui p el menor divisor positiu de a diferent de 1. Clarament p és primer i no és cap dels p_i, doncs si ho fos dividiria a $a - p_1 \cdots p_n = 1$, que no és possible en ser $p \neq 1$. Per tant $p \notin S$. □

Teorema fonamental de l'aritmètica. *Tot enter $a \neq 0$, $a \neq \pm 1$ s'escriu com a producte de nombres primers. Aquesta factorització és única llevat de l'ordre dels factors i el signe.*

Demostració. Com ja hem vist, a sempre tindrà un divisor primer $p_1 \neq \pm 1$. Llavors $a = p_1 a_1$ i $|a| > |a_1|$. De la mateixa manera, si $a_1 \neq \pm 1$ tindrà un divisor primer $p_2 \neq \pm 1$, i $a = p_1 a_1 = p_1 p_2 a_2$. Repetint el procés successivament obtenim $|a| > |a_1| > |a_2| > \cdots$, i arribarà un moment en què tindrem la factorització $a = p_1 \cdots p_n a_n$ amb $|a_n| = 1$.
Suposem ara que tenim dues factoritzacions $a = p_1 \cdots p_n = q_1 \cdots q_m$ amb p_i, q_j primers. Si p, q són primers, o bé $\mathrm{mcd}(p, q) = 1$ o bé $p = \pm q$. En l'expressió anterior, p_1 divideix $p_1 \cdots p_n = q_1(q_2 \cdots q_m)$, i pel teorema d'Euclides, o bé $p_1 | q_2 \cdots q_m$ quan $\mathrm{mcd}(p_1, q_1) = 1$, o bé $p_1 = \pm q_1$. En el primer cas tindrem $p_1 | q_2(q_3 \cdots q_m)$, i aplicant el mateix raonament tindrem que $p_1 | q_3 \cdots q_m$ o bé $p_1 = \pm q_2$. Iterant el procés acabarem obtenint que p_1 és algun dels q_j llevat del signe, o bé arribarem a $p_1 | q_{m-1} q_m$, d'on $p_1 = \pm q_{m-1}$ o $p_1 = \pm q_m$.
Per tant p_1 coincideix, llevat del signe, amb un dels q_j, que podem suposar que és el q_1 canviant l'ordre. Llavors $p_2 \cdots p_n = \pm q_2 \cdots q_m$. El mateix raonament prova que p_2 és un dels q_j llevat del signe, i així successivament. Si $n < m$ arribem a la situació $1 = \pm q_{n+1} \cdots q_m$ que és impossible en ser tots els q_j diferents de ± 1. Si $n > m$ obtenim

$\pm p_{m+1} \cdots p_n = 1$, també impossible. Per tant $n = m$ i ambdúes factoritzacions coindideixen llevat dels signes dels factors i llur ordre. $\square$

Donat un nombre enter n existeix un mètode pràctic per trobar tots els primers inferiors a n, que rep el nom de *garbell d'Eratostenes*: s'escriu la successió de tots els naturals fins a n. Llavors es ratllen tots els múltiples de 2 començant en el seu quadrat $2^2 = 4$. A continuació el següent nombre sense ratllar és el 3, i ratllem tots els seus múltiples començant pel seu quadrat $3^2 = 9$. Iterem el procés fins arribar a un nombre el quadrat del qual superi n. Els nombres que han quedat sense ratllar són tots els primers inferiors a n.

El garbell d'Eratostenes és un mètode eficient per trobar nombres primers "petits", de fins a 5 o 6 xifres. Per comprovar la primalitat de nombres més grans (15 o més xifres) cal plantejar-se tests de primalitat més enginyosos que fan servir potents eines de la Teoria de Nombres. El nombre primer més gran conegut fins al moment té gairebé 13 milions de xifres i és $2^{43112609} - 1$. Va ser trobat el 23 d'agost de 2008 dins el projecte col·laboratiu d'Internet *GIMPS* (Great Internet Mersenne Prime Search), que es dedica a comprovar la primalitat dels nombres de Mersenne $M_p = 2^p - 1$ amb p primer, usant el test de primalitat de Lucas-Lehmer. Aquest test proporciona un algorisme de p passos que dóna una condició necessària i suficient per la primalitat de M_p.

6 Congruències

Sigui $m \in \mathbb{Z},\ m \neq 0$. Direm que dos enters a i b són *congruents mòdul* m, i ho escriurem $a \equiv b \pmod m$, si $a - b \in (m)$.

Proposició. $a \equiv b \pmod m \ \Leftrightarrow$ *les divisions enteres de a i b per m tenen la mateixa resta.*

Demostració. Sigui $a = mq_1 + r_1,\ b = mq_2 + r_2,\ \Rightarrow\ a - b = m(q_1 + q_2) + (r_1 - r_2)$ amb $|r_1 - r_2| < |m|$. Per tant $a - b \in (m)$ si i només si $r_1 = r_2$. $\square$

Clarament, la relació de congruència mòdul m és una relació d'equivalència, ja que és reflexiva ($a \equiv a \pmod m$ en ser $0 \in (m)$), simètrica ($a \equiv b \pmod m \ \Leftrightarrow\ b \equiv a \pmod m$) i transitiva ($a \equiv b \pmod m$ i $b \equiv c \pmod m \ \Rightarrow\ a \equiv c \pmod m$, doncs $a - b = km$, $b - c = lm \ \Rightarrow\ a - c = (k + l)m$). Podem construir llavors el conjunt quocient $\mathbb{Z}/(m)$ que té m classes d'equivalència, anomenades *classes de restes mòdul* m:

$[0] = \{n \in \mathbb{Z} \mid n \text{ dóna resta 0 al dividir-lo per } m\} = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}$
$[1] = \{n \in \mathbb{Z} \mid n \text{ dóna resta 1 al dividir-lo per } m\} = \{\ldots, -m + 1, 1, m + 1, 2m + 1, \ldots\}$
$\ldots$

$[m-1] = \{n \in \mathbb{Z} \mid n \text{ dóna resta } m-1 \text{ al dividir-lo per } m\} = \{\ldots, -1, m-1, 2m-1, \ldots\}$

Tenim una propietat elemental de les congruències però important: si $a \equiv a' \pmod{m}$ i $b \equiv b' \pmod{m}$ llavors $a + b \equiv a' + b' \pmod{m}$ i $ab \equiv a'b' \pmod{m}$. La prova és trivial a partir de la definició de congruència. Aquesta propietat ens garanteix que podem definir unes operacions suma i producte a $\mathbb{Z}/(m)$ que són consistents, és a dir, que no depenen dels representants escollits de cada classe. Així, si $[a], [b] \in \mathbb{Z}/(m)$ definim $[a]+[b] = [a+b]$ i $[a] \cdot [b] = [ab]$. Aquestes operacions heteren les propietats de les equivalents a $\mathbb{Z}$ i doten a $\mathbb{Z}/(m)$ d'estructura d'*anell commutatiu i unitari*.

Ara bé, $\mathbb{Z}/(m)$ té propietats que no tenia $\mathbb{Z}$: podem tenir divisors de zero i elements que tenen invers respecte del producte. Per exemple, a $\mathbb{Z}/(6)$, $[2] \cdot [3] = [0]$ i $[5] \cdot [5] = [1]$). També hi ha propietats de $\mathbb{Z}$ que en general no són certes a $\mathbb{Z}/(m)$, con la llei de cancel·lació pel producte. Per exemple, a $\mathbb{Z}/(6)$, $[2] \cdot [3] = [4] \cdot [3]$ i en canvi $[2] \neq [4]$. Aquesta llei, però, funciona afegint-hi una condició:

Proposició. *Siguin $a, b, c, m \in \mathbb{Z}$. $ac \equiv bc \pmod{m}$ i $\operatorname{mcd}(c, m) = 1 \;\Rightarrow\; a \equiv b \pmod{m}$.*

DEMOSTRACIÓ. $ac \equiv bc \pmod{m} \;\Rightarrow\; m | ac - bc = c(a-b)$. Com $\operatorname{mcd}(c, m) = 1$, pel teorema d'Euclides $m | a - b \;\Rightarrow\; a \equiv b \pmod{m}$. □

Treballant amb aritmètica modular obtenim de forma immediata els criteris de divisibilitat en base 10 més coneguts. En efecte, si escrivim un nombre $a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k$, tenim:

- $10 \equiv 0 \pmod{2} \Rightarrow 10^n \equiv 0 \pmod{2}\ \forall n \in \mathbb{N}$. Així $a \equiv 0 \pmod{2} \Leftrightarrow a_0 \equiv 0 \pmod{2}$ (a és parell si i només si la xifra de les unitats ho és). El criteri mòdul 5 és idèntic en ser també $10 \equiv 0 \pmod{5}$.

- $10 \equiv 1 \pmod{3} \Rightarrow 10^n \equiv 1^n \equiv 1 \pmod{3}\ \forall n \in \mathbb{N}$. Així $a \equiv 0 \pmod{3} \Leftrightarrow a_0 + a_1 + \cdots + a_k \equiv 0 \pmod{3}$ (a és múltiple de 3 si i només si la suma de les seves xifres ho és). El criteri mòdul 9 és idèntic en ser també $10 \equiv 1 \pmod{9}$.

- $10 \equiv 2 \pmod{4} \Rightarrow 10^2 \equiv 2^2 \equiv 0 \pmod{4} \Rightarrow 10^n \equiv 0 \pmod{4}\ \forall n \geq 2$. Així $a \equiv 0 \pmod{4} \Leftrightarrow a_0 + 2a_1 \equiv 0 \pmod{4}$ (a és múltiple de 4 si i només si la xifra de les unitats més el doble de la de les desenes ho és).

- $10 \equiv -1 \pmod{11} \Rightarrow 10^n \equiv (-1)^n \pmod{11}\ \forall n \in \mathbb{N}$. Així $a \equiv 0 \pmod{11} \Leftrightarrow a_0 - a_1 + a_2 - \cdots + (-1)^k a_k \equiv 0 \pmod{11}$ (a és múltiple d'11 si i només si la suma de les xifres que ocupen un lloc senar menys la suma de les que ocupen un lloc parell també és múltiple d'11).

Acabem el tema donant una caracterització dels elements inversibles de $\mathbb{Z}/(m)$:

Proposició. *Si* $\mathrm{mcd}(a, m) = 1$ *llavors* $[a]$ *té un invers a* $\mathbb{Z}/(m)$. *Si* $\mathrm{mcd}(a, m) = d > 1$ *llavors* $[a]$ *és un divisor de 0 a* $\mathbb{Z}/(m)$ *i no pot tenir invers.*

Demostració. Si $\mathrm{mcd}(a, m) = 1$, per la identitat de Bézout $1 = ar + ms \Rightarrow [1] = [ar] = [a][r]$, per tant $[r]$ és l'invers de $[a]$. $\mathrm{mcd}(a, m) = d > 1$ escrivim $a = da'$, $m = dm'$ (amb $0 < |m'| < |m|$) i llavors $am' = a'm \Rightarrow [a][m'] = [0]$ amb $[m'] \neq [0]$. I en aquesta situació $[a]$ no pot tenir invers, ja que si existís un $[a]^{-1}$ tindríem $[a]^{-1}[a][m'] = [a]^{-1}[0] \Rightarrow [m'] = [0]$, en contra del què hem suposat. $\square$