Divisió entera. Ideals

Teorema 1.1 (de la divisió entera) *Donats* $a,b\in\mathbf{Z},\ b\neq 0$, existeixen dos únics nombres enters p i q que compleixen $a=b\cdot q+r$, $0\le r<|b|$. q i r es diuen el *quocient* y la *resta* de la *divisió entera* de a per b.

Exemple:

$$-8=3\cdot(-3)+1,\qquad 3=(-8)\cdot 0+3$$

Si la resta de la divisió entera de a per b és 0, es diu que a és un múltiple de b (escriurem $a=\dot{b}$), que b és un divisor de a (escriurem $b\mid a$).
Indicarem per (b) el conjunt dels múltiples de b. Té les següents propietats:

- És tancat per la suma; és a dir $a,c\in(b)\Rightarrow a+c\in(b)$.
- Si $a\in(b)$ i c és qualsevol enter, aleshores $a\cdot c\in(b)$.

Proposició 1.2 Si el subconjunt $I\subset\mathbf{Z}$ compleix:

1. $a,b\in I\Rightarrow a+b\in I$
2. $a\in I,\ c\in\mathbf{Z}\Rightarrow a\cdot c\in I$

aleshores hi ha un $b\in I$ tal que $I=(b)$.

Un subconjunt I que compleixi 1 i 2 com a (1.2) es diu un *ideal* de $\mathbf{Z}$. L'element b tal que $I=(b)$ es diu *base de l'ideal.*

Mínim comú múltiple i màxim comú divisor

Direm que d és el *màxim comú divisor* de $a_1,\ldots,a_n$ i escriurem

$$d=m.c.d.(a_1,\ldots,a_n).$$

Observem que el màxim comú divisor d és una suma de múltiples de $a_1,\ldots,a_n$,

$$\boxed{d=a_1\cdot r_1+\ldots+a_n\cdot r_n}$$

Aquesta expressió es coneix amb el nom d'identitat de Bézout.

Proposició 2.1 Sigui $a=b\cdot q+r$ la divisió entera de a per b. Aleshores

$$\boxed{m.c.d.(a,b)=m.c.d.(b,r)}$$

Nombres primers entre ells i nombres primers

Es diu que a i b són *nombres primers entre ells* si $m.c.d.(a,b)=1$

Exemple:

1. $m.c.d.(3,8)=1$. Observem que $1=3\cdot 3+8(-1)$.

Teorema 3.1 (d'Euclides) Si i $m.c.d.(a,b)=1$, aleshores $a \mid c$.

Proposició 3.2 Si $m=m.c.m.(a,b)$ i $d=m.c.d.(a,b)$, es compleix $m\cdot d=\pm a\cdot b$.

Qualsevol nombre enter p és divisible per ± 1 i per $\pm p$. Direm que p és *primer* si aquests són els únics divisors. L'1 i el -1 no es consideren nombres primers.

Proposició 3.3 El conjunt dels nombres primers és infinit

Proposició 3.4 Tot nombre enter a no nul, $a\neq \pm 1$, és producte de nombres primers.

Proposició 3.5 Si $p_1 \dots p_n = q_1 \dots p_m$ i tots els factors p_i, q_j, amb $i=1,\dots,n$, $j=1,\dots,m$, són nombres primers, aleshores $n=m$ i els nombres $\{p_1,\dots,p_n\}$ són els mateixos que els $\{q_1,\dots,q_m\}$, llevat del signe (i l'ordre).

Congruències

Sigui A un conjunt. Una relació a A és un criteri que ens permet dir si dos elements qualssevol de A, a i b, "satisfan la relació" o no. Més exactament: donar una relació a A és donar una sèrie de parells ordenats d'elements de A (que seran els elements que "satisfan la relació"); és a dir, donar un subconjunt del producte cartesià $A\times A$. Indiquem per $a\sim b$ el fet que a estigui relacionat amb b.

Una *relació és d'equivalència* si compleix:

- Propietat reflexiva. Per a tot $a\in A$, $a\sim a$.
- Propietat simètrica: $a\sim b \Rightarrow b\sim a$.
- Propietat transitiva: $a\sim b$, $b\sim c \Rightarrow a\sim c$

Classes d'equivalència: està formada per elements relacionats entre ells. Les tres propietats anteriors asseguren que tot element és una i només en una classe. En efecte, designem per $[a]$ la classe de tots els elements relacionats amb . Clarament $a\in[a]$.

Una partició de A és una sèrie de subconjunts de A tals que tot $a\in A$ és en un i només en un d'aquests subconjunts. Una classificació dels elements de A no és una altra cosa que una partició de A.

El conjunt de les classes d'equivalència es diu *conjunt quocient* i es denota per $A/\sim$.

Els anells $Z/(m)$

Un conjunt A amb dues operacions $(a+b, a\cdot b)$ és un *anell* si es compleix

- Propietats de $+$:
  - Associativa: $(a+b)+c=a+(b+c) \qquad \forall a,b,c\in A$
  - Commutativa: $a+b=b+a \qquad \forall a,b\in A$
  - Existeix un element, que anomenarem zero i escriurem 0, tal que $a+0=0+a=a \qquad \forall a\in A$
  - Per a cada $a\in A$ hi ha un element, que anomenarem l'oposat de a i denotarem $-a$ tal que $a+(-a)=0$

- Propietat de $(\cdot)$:
  - Associativa: $(a\cdot b)\cdot c=a\cdot(b\cdot c) \qquad \forall a,b,c\in A$

- Propietats que relacionen $+$ i $(\cdot)$:
  - Distributives:
    - $a\cdot(b\cdot c)=a\cdot b+a\cdot c$
    - $(a+b)\cdot c=a\cdot c+b\cdot c \qquad \forall a,b,c\in A$

Si, a més a més es compleix que la operació $(\cdot)$ és commutativa ($a\cdot b=b\cdot a$, per a tot $a,b\in A$) es diu que A és un *anell commutatiu*. Si existeix un element $e\in A$ tal que $a\cdot e=e\cdot a$, per a tot $a\in A$, es diu que A *té unitat*. L'element e es diu *la unitat de* A i generalment es designa per 1. Un element $a^{-1}\in A$ tal que $a\cdot a^{-1}=a^{-1}\cdot a=1$ es diu *un invers* de a.

Un anell commutatiu amb unitat, en que tot element no zero té invers, és diu un *cos*.

Divisors de zero: un anell commutatiu amb unitat $Z/(m)$ té propietats que no té $\mathbf{Z}$. El producte de dos elements diferents de zero pot ser zero $\mathbf{Z}/(6)=[2]\cdot[3]=[0]$.
En un anell si un element és divisor de zero no pot tenir invers.

Proposició 5.1 Si $m.c.d.(a,m)=1$, $[a]$ té un invers a $\mathbf{Z}/(m)$. Si $m.c.d.(a,m)=d\neq\pm1,\pm m$, $[a]$ és divisor de zero a $\mathbf{Z}/(m)$.

Corol·lari 5.2 L'anell $\mathbf{Z}/(p)$ és un cos si i només si p és primer.