Sessions de preparació per a l'olimpíada matemàtica

Sessió d'aritmètica

Jaume Monreal

Revisat octubre 2018

1. Introducció

L'aritmètica és una de les parts més antiga de les matemàtiques, juntament amb la geometria, car per a resoldre problemes aritmètics només cal saber sumar, restar, multiplicar i dividir amb nombres naturals (i, per extensió, amb els enters). El fet de no poder emprar decimals, però, fa que hàgim d'utilitzar propietats matemàtiques i raonaments que caldrà conèixer i dominar.

Exercici 1. Resoleu l'equació $9^m = 4n^2+1$, amb m i n nombres enters (2004)

El concepte de nombre primer és la base de molts resultats i algoritmes d'execució senzilla però que donen molt de joc per a fer construccions elaborades. De fet, la seguretat a internet (correus electrònics, operacions de compra-venta electrònica, etc...) s'han basat durant anys en un senzill mètode criptogràfic purament aritmètic anomenat RSA.

En aquesta sessió veurem conceptes com la relació de divisibilitat, les seves propietats i les equacions Diofàntiques.

2 Divisibilitat. Nombres primers.

Les divivions que nosaltres utilitzarem seran divisions enteres; això és, sense decimals.

123	7
4	17

De fet,

a	b
r	q

on $a=b\cdot q+r$.

> Divisió Euclídea: Donats a i b nombres enters amb $b>0$, sempre existeixen, i són únics, uns nombres naturals q i r de manera que $a=b\cdot q+r$ i $0\leqslant r<b$.
>
> Al nombre b se l'anomena **quocient** i, al nombre r, **residu de la divisió.**

Quan r=0 $(a=b\cdot q)$, direm que **a és múltiple de b** o també que **b divideix a** i ho denotarem com **b|a**.

Propietats de la divisibilitat:

- 1 divideix tots els nombres enters: $1|a \quad \forall a\in Z$
- Tots els enters divideixen a zero: $a|0 \quad \forall a\in Z$
- Tot enter es divideix a sí mateix: $a|a \quad \forall a\in Z$
- Transitivitat: Si $a|b$ i $b|c$ llavors $a|c \quad \forall a,b,c\in Z$
- Si a|b i a|c llavors $a|(m\cdot b+n\cdot c) \quad \forall a,b,c,m,n\in Z$
- Si a|b llavors b = 0 o bé $|a|\leqslant|b| \quad \forall a,b\in Z$
- Antisimetria: Si $a|b$ i $b|a$ llavors $|a|=|b| \quad \forall a,b\in Z$

Observem que el nombre 0 no divideix ningú però és multiple de tots els nombres enters, i que el nombre 1 sols té un divisor (positiu).

En canvi, si $a\in Z^+, a>1$, llavors hi ha sempre dos divisors possibles: 1 i a , anomenats **divisors trivials** del nombre a . Qualsevol altre divisor se'n diu un **divisor propi**.

Per exemple, el nombre 12 té dos divisors trivials, 1 i 12, i quatre divisors propis: 2, 3, 4 i 6.

Un nombre natural n > 1 es diu que és **primer** quan no té divisors propis. Si té divisors propis es diu que és **compost**. El nombre 1 no és ni primer ni compost (és un invertible).

Exercici 2. Troba n enter tal que n=p·q·r (primers), r-q=2p i r·q+p^2=676 (Prova 2001)

Exercici 3. Existeix un nombre infinit de naturals que NO es poden representar de la forma n^2+p, essent n un nombre natural i p un nombre primer? Raonar la resposta. (Prova 2006)

Exercici 4. Siguin a, b, c, d nombres enters positius. Si ab = cd aleshores a + b + c + d és compost.

La "forma" dels nombres naturals"

En dividir els diferents nombres naturals per un nombre b, llavors s'obté una classificació del tipus:

b·k b·k+1 b·k+2 b·k+3 ... b·k+(b-1)

Per exemple, en dividir per 5 els nombres es classifiquen en:

- múltiples de 5: 0, 5, 10, 15...
- múltiples de 5 més 1 unitat: 1, 6, 11, 16...
- múltiples de 5 més 2 unitats: 2, 7, 12, 17...
- múltiples de 5 més 3 unitats: 3, 8, 13, 18...
- múltiples de 5 més 4 unitats: 4, 9, 14, 19...

Això depèn del valor del residu. La propera sessió de congruències es basarà en això.

La forma dels nombres primers: Tot nombre primer és de la forma 6k+1 o 6k+5 (demostreu-ho!)

Exercici 5. Provar que si $p\neq 3$ és un nombre primer llavors p^2+2 és compost.

Exercici 6. Prova que si $3|x^2+y^2$ llavors 3|x i 3|y. [Millor per congruències]

Siguin $a,b,p\in Z$, p primer. Si $p|a\cdot b$ llavors $p|a$ o $p|b$

La condició que p sigui primer és imprescindible perquè el resultat sigui cert. Per exemple, 6|12 i 12 = 3·4, però ni 6|3 ni 6|4.

Exercici 7. (Olimpíada 2000, Fase Nacional). Troba el major nombre enter N que cumpleix les condicions:

a) $E(N/3)$ té les seves tres xifres iguals.

b) $E(N/3)$ és suma de nombres naturals consecutius començant en 1, és a dir, existeix un natural n tal que: $E(N/3)=1+2+...+n$

Nota: E(x) és la part entera de x. Per exemple, E(1,42) = 1, E(π) = 3, E(-1,5) = -2.

El resultat que ve a continuació és la base de tot el que coneixem de l'aritmètica.

Teorema fonamental de l'aritmètica: Tot nombre natural compost admet una descomposició en factors primers. A més a més, aquesta descomposició és única si no es té en compte l'ordre dels factors.

Exemple: $756 = 2^2 \cdot 3^3 \cdot 7$

Exercici 8. Demostra que $\sqrt{n}$ i $\log_2 3$ són irracionals.

Exercici 9. *Demostra que per a tot nombre primer p diferent de 2 i de 5, existeixen infinits múltiples de la forma 11111.....1 (només uns).*

Exercici 10. *Trobar raonadament, dos nombres enters positius a i b tals que* b^2 sigui múltiple de a, a^3 sigui múltiple de b^2, b^4 sigui múltiple de a^3, a^5 sigui múltiple de b^4 *però* b^6 *no sigui múltiple de* a^5.

Exercici 11. Troba els nombres enters positius n tals que 3^n+5^n és múltiple de $3^{n-1}+5^{n-1}$

Exercici 12. Cerca el menor enter positiu n tal que n^2 sigui un quadrat, n^3 sigui un cub i n^7 sigui una poténcia elevada a 7.

El resultat següent mostra com calcular el nombre de divisors d'un nombre a partir de la seva descomposició factorial.

Sigui $m \in Z$ amb descomposició factorial $m = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}$, on p_1, p_2, ..., p_r són nombres primers diferents dos a dos. Aleshores el nombre de divisors del nombre m és

$$\text{div}(m) = (a_1 + 1) \cdot (a_2 + 1) \cdot \ldots \cdot (a_r + 1)$$

La demostració d'aquest resultats és un senzill exercici de combinatòria. Intenta demostrar-lo!

També ho pots intentar amb aquest:

Exercici 13. Els quadrats perfectes tenen un nombre imparell de divisors.

Exercici 14. Determinau els enters N que contenen solament els factors 2 i 3 i tals que el nombre de divisors de N^2 és triple del nombre de divisors de N.

Exercici 15. Un nombre descomposat en factors primers $N = a^x \cdot b^y \cdot c^z$ disminueix el nombre dels seus divisors en 72, 48 o 54 en dividir-lo per a, per b o per c, respectivament. Trobar el valor de N.

3. Màxim comú divisor i mínim comú múltiple

El **màxim comú divisor** de dos nombres naturals a i b és el nombre natural d que divideix a i b, de manera que tot altre divisor de a i b el divideix. Si d = mcd(a,b), llavors:

- d|a i també d|b (d és un divisor comú)
- si c|a i c|b (és a dir, c és un divisor comú de a i b) llavors c|d (d és el major!)

Si d = 1 es diu que els dos nombres, a i b, són **coprimers** (o primers entre ells).

Si d = mcd(a,b) llavors $mcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Exercici 16.

a) Provar que dos nombres enters consecutius no tenen cap divisor comú.

b) Demostrar que la fracció $\frac{n^2+n-1}{n^2+2n}$ és irreductible per a tot nombre enter positiu n.

Teorema d'Euclides: Si d|a·b i mcd(a,d)= 1 llavors d|b

Exercici 17. Resoleu l'equació p(x+y) = x·y (Prova 2007)

El mínim comú múltiple de dos nombres naturals a i b és el nombre natural m que és múltiple de a i b i que divideix tot altre múltiple de a i b. Si m=mcm(a; b), llavors

- a|m i també b|m (m és un múltiple comú)
- si a|c i b|c (és a dir, c és un múltiple comú) llavors m|c (m és el menor!)

Siguin a i b dos nombres enters. Aleshores es cumpleix que

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

Exercici 18. Trobar tots els parells de nombres naturals a i b tal que:

$$\begin{cases} mcd(a,b) = 18 \\ mcm(a,b) = 540 \end{cases}$$

4. Algorisme d'Euclides

L'Algorisme d'Euclides permet calcular el màxim comú divisor de dos nombres enters utilitzant la divisió Euclídea. Si a,b són dos nombres enters positius i anam fent successives divisions:

- $a = b \cdot q_1 + r_1$
- $b = r_1 \cdot q_2 + r_2$
- $r_1 = r_2 \cdot q_3 + r_3$
- etc... FINS que $r_k = 0$ per algun k.

$\text{mcd}(a,b) = \text{mcd}(b,r_1) = \text{mcd}(r_1, r_2) = \ldots \text{mcd}(r_{k-2}, r_{k-1}) = r_{k-1}$

Exemple: siguin a = 138 i b=63.

- $138 = 63 \cdot 2 + 12$
- $63 = 12 \cdot 5 + 3$
- $12 = 3 \cdot 4 + 0$

Aleshores mcd(138, 63) = 3.

Si d = mcd(a,b) llavors existeixen x i y enters tal que $a \cdot x + b \cdot y = d$

En el nostre exemple, $138 \cdot (-5) + 63 \cdot 11 = 3$

L'expressió $a \cdot x + b \cdot y = d$ on d=mcd(a,b) es coneix amb el nom d'**identitat de Bézout**.

Exercici 19. Aplica l'algorisme d'Euclides per a determinar el màxim comú divisor de 54 i 75, i determina'n una Identitat de B#ezout.

Exercici 20. Troba dos nombres enters, x i y, que satisfacin cada una de les equacions seg uents:

i. $5244x + 1428y = 12$. (Sol: $5244 \cdot (-58) + 1428 \cdot 213 = 12$)

ii. $36x + 20y = 12$. (Sol: $36 \cdot (-3) + 20 \cdot 6 = 12$)

5. Equacions Diofàntiques

Siguin a, b i c tres nombres enters positius. Una **equació Diofàntica** és una equació sobre Z (cercam solucions enteres) del tipus $a \cdot x + b \cdot y = c$.

Sigui $a \cdot x + b \cdot y = c$ una equació Diofàntica. Aquesta equació té solucions enteres si i només si $\text{mcd}(a,b) | c$ (és a dir, c és múltiple del mcd(a,b))

En efecte, $a \cdot x + b \cdot y = c$ té solució i d = mcd(a, b), posem $a = d \cdot a'$ i $b = d \cdot b'$ i, en substituir, resulta $d \cdot a' + d \cdot b' = c$, és a dir, d|c.

Per altra banda, si d|c llavors tenim $a = d \cdot a'$, $b = d \cdot b'$ i $c = d \cdot c'$, i l'equació queda $a'x + b'y = c'$, amb $\text{mcd}(a',b') = 1$. Per tant tenim valors m i n enters tal que $a'm + b'n = 1$. Si prenem $x = m \cdot c'$ i $y = n \cdot c'$, llavors $ax + by = c$.

Sigui $a \cdot x + b \cdot y = c$ una equació Diofàntica de la qual en coneixem una solució: $a \cdot p + b \cdot q = c$. Aleshores totes les solucions de l'equació són:

$$\begin{cases} x = p + b \cdot t \\ y = q + a \cdot t \end{cases}, \quad t \in Z$$

En efecte, d'una banda es pot comprovar fàcilment que aquestes expressions són solucions.

De l'altra banda, si x i y és una solució llavors....

Exercici 21. Un home cobra un xec per valor de d euros i c cèntims en un banc. Per error li donen c dòlars i d cèntims, però l'home no s'adona fins que es gasta 23 cèntims, moment en què compta els diners i observa que li queda el doble del que havia de cobrar. Quin és el valor del xec? (Sol: 25,51€).