Sessions de preparació per a l'olimpíada matemàtica

Sessions 2 i 3 d'aritmètica

Jaume Monreal i Gemma Rado

Octubre 2012

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). Ja veureu, però, que els conceptes que van apareixent no són tan senzills com això. De fet, la seguretat a internet (correus electrònics, operacions de compra-venta electrònica, etc...) se basa en un senzill mètode criptogràfic purament aritmètic anomenat *RSA*. En aquestes sessions veurem conceptes relacionats amb la relació de divisibilitat, les equacions diofàntiques i les congruències.

2 Divisibilitat. Nombres primers.

En aquesta secció introduïm els conceptes bàsics de l'aritmètica.

Les definicions bàsiques de l'aritmètica són la de múltiple i la de divisor d'un nombre.

Definició 2.1. *Donats dos nombres a i b, es diu que a divideix b (o que a és un divisor de b o que b és un múltiple de a si existeix un nombre enter x t.q. $a \cdot x = b$. Escriurem $a|b$ (es llegeix a divideix b).*

Els divisors i múltiples dels nombres tenen unes propietats molt útils a l'hora de resoldre problemes. Comencem recordant que tot nombre té com a divisors 1 i ell mateix i zero és múltiple de qualsevol nombre.

$$\forall a \in Z \quad 1|a, \quad a|a \text{ i } a|0$$

Proposició 2.2. *Si a divideix b llavors o bé $b = 0$ o bé $|a| \leq |b|$.*

Definició 2.3. *Donat un nombre enter n qualsevol, els nombres 1 i n se n'anomenen **divisors trivials** de n. Qualsevol altre divisor se'n diu un **divisor propi**.*

Exemple 1 i 24 són els divisors trivials de 24. En són exemples de divisors propis els nombres 2, 6 i 8, entre d'altres.

Així mateix, se sap que si un nombre a divideix a dos nombres n i m llavors també en divideix la seva suma, la seva diferència i, en general, qualsevol combinació lineal seva (α, $\beta \in \mathbb{Z}$):

$$\text{Si } a|n \text{ i } a|m \Rightarrow \ a|(n+m), \quad a|(n-m) \ \text{ i } \ a|(\alpha \cdot n + \beta \cdot m)$$

L'arimètica està basada en la definició de múltiple i divisor. Les peces fonamentals d'aquesta són els nombres primers.

Definició 2.4. *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.*

Exercici 2.5.

a) Provar que un nombre primer major que 3 és de la forma $6k + 1$ o $6k + 5$.

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

Exercici 2.6. *Siguin a, b, c, d quatre nombres enters. Si $ab = cd$ aleshores $a + b + c + d$ és compost.*

Proposició 2.7 (Teorema d'Euclides)**.** *Si a, b i n són nombres enters tal que $mcd(a, n) = 1$ i $n|ab$ llavors $n|b$.*

Un cas particular d'aquest teorema és la següent

Proposició 2.8. *Si p és un nombre primer que divideix un producte $a \cdot b$ llavors $p|a$ o $p|b$.*

Observem que la proposició pot ser falsa si p no és un nombre primer. Per exemple, 6 és un divisor de $3 \cdot 4$ i, en canvi, 6 no és divisor ni de 3 ni de 4.

Exercici 2.9 (Olimpíada 2000, Fase Nacional)**.** *Troba el major nombre enter N que cumpleix les condicions:*

a) $E(\frac{N}{3})$ té les seves tres xifres iguals.

b) $E(\frac{N}{3})$ és suma de nombres naturals consecutius començant en 1, és a dir, existeix un natural n tal que: $E(\frac{N}{3}) = 1 + 2 + \ldots + (n-1) + n$

Nota: $E(x)$ és la part entera de x (p. ex. $E(1.42) = 1$, $E(\pi) = 3$; $E(\frac{1}{3}) = 0$;$E(-1.5) = -2$).

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

Teorema 2.10 (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 2.11. *La descomposició factorial és $756 = 2^2 \cdot 3^3 \cdot 7$.*

Exercici 2.12. *Demostrau que el nombre real $log_2 3$ és irracional.*

Exercici 2.13. *Trobar tots els nombres enters positius n tals que $3^n + 5^n$ és múltiple de $3^{n-1} + 5^{n-1}$.*

Exercici 2.14. *Cerqueu el menor enter positiu n tal que $\frac{n}{2}$ sigui un quadrat, $\frac{n}{3}$ sigui un cub i $\frac{n}{7}$ sigui una potència elevada a 7.*

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

Proposició 2.15. *Sigui m un nombre enter amb descomposició factorial $m = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_r^{a_r}$, on $p_1, p_2, ..., p_r$ són nombres primers diferents dos a dos. Aleshores el nombre de divisors del nombre m és*

$$div(m) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot ... \cdot (\alpha_r + 1)$$

La demostració d'aquesta proposició és un interessant exercici de combinatòria. De fet, l'enunciat de l'exemple següent ha aparegut en una fase local d'olimpíades.

Exemple 2.16. *El quadrat dels nombres naturals tenen un nombre senar de divisors.*

Exercici 2.17. *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 2.18. *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

La definició següent cal analitzar-la bé, terme a terme, doncs explica propietats del màxim comú divisor que sovint passen desaparcebudes en la manera clàssica en què es treballa als centres.

Definició 3.1. *El màxim comú divisor de dos nombres naturals a i b és el nombre natural d que divideix a i b i que tot altre divisor de a i b el divideix. S'indica per $mcd(a, b) = d$. Si $d = 1$ es diu que els dos nombres, a i b, són coprimers (o primers entre ells).*

Proposició 3.2. *Si es divideixen dos nombres a i b pel seu màxim comú divisor $d = mcd(a, b)$, llavors s'obtenen dos nombres coprimers.*

Exercici 3.3.

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

b) Determinar per quins nombres enters positius n la fracció $\frac{n^2+n-1}{n^2+2n}$ és irreductible.

La definició següent explica, com la del màxim comú divisor, propietats del mínim comú múltiple que sovint passen desaparcebudes en la manera clàssica en què es treballa als centres.

Definició 3.4. *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. S'indica per $mcm(a, b) = m$.*

La proposició següent relaciona el màxim comú divisor amb el mínim comú múltiple:

Proposició 3.5. *Siguin a i b dos nombres enters. Aleshores es cumpleix que*

$$mcd(a, b) \cdot mcm(a, b) = a \cdot b$$

o, el que és el mateix,

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

Exercici 3.6. *Trobar tots els parells de nombres naturals a i b tal que $mcd(a, b) = 18$ i $mcm(a, b) = 540$.*

4 Algorisme d'Euclides

Proposició 4.1 (Divisió Euclídea)**.** *Considerem a i b dos nombres enters. Llavors existeixen dos únics nombres enters q i r que satisfan $a = bq + r$ amb $0 \leq r < b$.*

L'**Algorisme d'Euclides** permet calcular el màxim comú divisor de dos nombres enters utilitant la divisió euclídea. Fixeu-vos en l'exemple següent, on calculam el màxim comú divisor de 204 i 144 fent divisions euclídees successivament:

$$\begin{aligned} 204 &= 144 \cdot 1 + 60 \\ 144 &= 60 \cdot 2 + 24 \\ 60 &= 24 \cdot 2 + 12 \\ 24 &= 12 \cdot 2 \end{aligned}$$

Observau que aturam el procés quan la divisió és exacta. És aleshores quan podem afirmar que $mcd(204, 144) = 12$ perquè 12 és el darrer residu diferent de zero que hem obtingut.

Dos nombres enters qualsevols estan relacionats d'una forma especial amb el seu màxim comú divisor. En el nostre exemple,

$$204 \cdot 5 + 144 \cdot (-7) = 12$$

En general,

Proposició 4.2. *Siguin a i b dos nombres enters, i sigui $d = mcd(a, b)$. Aleshores existeixen m i n enters tals que*

$$a \cdot m + b \cdot n = d$$

(Identitat de Bézout).

Ara, doncs, retornant a l'exemple, fixem-nos que podem anar desfent les igualtats que hem obtingut amb la intenció d'arribar a una identitat de Bézout ($204 \cdot x + 144 \cdot y = 12$).

$60 = 24 \cdot 2 + 12 \Rightarrow 60 - 24 \cdot 2 = 12.$

$144 = 60 \cdot 2 + 24 \Rightarrow 24 = 144 - 60 \cdot 2 \Rightarrow 60 - (144 - 60 \cdot 2) \cdot 2 = 12 \Rightarrow 60 \cdot 5 - 144 \cdot 2 = 12.$

$204 = 144 \cdot 1 + 60 \Rightarrow 60 = 204 - 144 \cdot 1 \Rightarrow (204 - 144 \cdot 1) \cdot 5 - 144 \cdot 2 = 12 \Rightarrow 204 \cdot 5 - 144 \cdot 7 = 12$

Exercici 4.3. *Aplica l'algorisme d'Euclides per a determinar el màxim comú divisor de 54 i 75, i determina'n una Identitat de Bézout.*

Exercici 4.4. *Troba dos nombres enters, x i y, que satisfacin cada una de les equacions següents:*

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

Aquesta secció enllaça perfectament amb l'anterior, tal i com observareu en la definició següent:

Definició 5.1. *Siguin a, b i c tres nombres enters. Una equació diofàntica és una equació sobre* Z *del tipus*

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

amb $x, y \in \mathrm{Z}$

Com veis, aquestes equacions són les mateixes per a les quals cercàvem una solució particular en la secció anterior. Com veurem en aquestes dues proposicions que segueixen, una equació diofàntica o no té solució o té infinites solucions.

Proposició 5.2. *Sigui $a \cdot x + b \cdot y = c$ una equació diofàntica. Aquesta equació és compatible si i només si c és un múltiple del $mcd(a, b)$.*

En efecte, si diem $d = mcd(a, b)$ i posem $a = d{\cdot}a'$ i $b = d{\cdot}b'$. Aleshores, l'equació queda $d{\cdot}a'{\cdot}x + d{\cdot}b'{\cdot}y = c$, d'on resulta que $d|c$.

Proposició 5.3. *Sigui $a \cdot x + b \cdot y = c$ una equació diofàntica tal que $mcd(a, b)|c$. Sigui $a \cdot p + b \cdot q = c$ una solució particular. Aleshores* $\begin{cases} x = p + bt \\ y = q - at \end{cases}$ *amb $t \in \mathrm{Z}$ en són totes les solucions.*

Observau que si substituïm aquests valors en l'equació diofàntica inicial, aquesta es satisfà:

$$a \cdot (pc + bt) + b \cdot (qc - at) = ap + abt + bq - abt = ap + bq = c$$

Exercici 5.4. *Un home cobra un xec per valor de d dòlars i c centaus en un banc. El caixer per error li dóna c dòlars i d centaus. L'home no se n'adona fins que gasta 23 centaus i a més observa que en aquell moment té el doble del que havia de cobrar. Quin és el valor del xec?*

6 Congruències

6.1 Definicions i propietats

Entram ara en l'apartat de les congruències, o de treball en base n. La idea és adonar-nos que en dividir qualsevol nombre enter a entre n, el residu de la divisió ha de ser necessàriament un nombre $0 \leq r \leq n-1$. Així s'estableix de forma senzilla una classificació, per a cada n, dels nombres enters. Per exemple, per a $n = 4$ tendrem 4 *classes d'equivalència* que són:

[0] = { nombres enters que en dividir-los per 4 el residu és 0 },

[1] = { nombres enters que en dividir-los per 4 el residu és 1 },

[2] = { nombres enters que en dividir-los per 4 el residu és 2 },

[3] = { nombres enters que en dividir-los per 4 el residu és 3 }.

Observau que la classe del zero, [0], és el conjunt dels múltiples de 4.

Definició 6.1. *Dos nombres enters a i b són congruents mòdul n, fet que s'indica per*

$$a \equiv b \ (mod\ n)$$

si pertanyen a una mateixa classe d'equivalència (si el residu és el mateix en dividir-los per n).

Equivalentment,

Proposició 6.2. *Donats dos nombres enters a i b, $a \equiv b \ (mod\ n)$ si i només si $a - b$ és múltiple de n.*

De l'exemple anterior, $3 \equiv 23 \ (mod\ 4)$, $28 \equiv 0 \ (mod\ 4)$, $42 \equiv -14 \ (mod\ 4)$.

Proposició 6.3. *Sigui n un nombre enter qualsevol. Aleshores:*

i. $a \equiv a \ (mod\ n)$ *(Reflexivitat)*
ii. Si $a \equiv b \ (mod\ n)$ *aleshores* $b \equiv a \ (mod\ n)$. *(Conmutativitat)*
iii. Si $a \equiv b \ (mod\ n)$ *i* $b \equiv c \ (mod\ n)$ *aleshores* $a \equiv c \ (mod\ n)$. *(Transitivitat)*
iv. Si $a \equiv b \ (mod\ n)$ *aleshores* $mcd(a, n) = mcd(b, n)$.
v. Si $a \equiv b \ (mod\ n)$ *aleshores* $a + k \equiv b + k \ (mod\ n)$.
vi. Si $a \equiv b \ (mod\ n)$ *aleshores* $a \cdot k \equiv b \cdot k \ (mod\ n)$.
vii. Si $a \equiv b \ (mod\ n)$ *i* $c \equiv d \ (mod\ n)$ *aleshores* $a + c \equiv b + d$.
viii. Si $a \equiv b \ (mod\ n)$ *i* $c \equiv d \ (mod\ n)$ *aleshores* $a \cdot c \equiv b \cdot d$.
ix. Si $c \cdot a \equiv c \cdot b \ (mod\ n)$ *i* $mcd(c, n) = 1$ *aleshores* $a \equiv b \ (mod\ n)$. *(Simplificació)*

Exemple: Com a exemple, demostrem els criteris de divisibilitat coneguts:

1. Un nombre és divisible per 2 quan acaba en xifra parell.
2. Un nombre és divisible per 3 quan la suma de les seves xifres és també múltiple de 3.
3. Un nombre és divisible per 4 quan les dues darreres xifres és múltiple de 4.
4. Un nombre és divisible per 5 quan acaba en 0 o en 5.
5. Un nombre és divisible per 9 quan la suma de les seves xifres és també un múltiple de 9.
6. Un nombre és divisible per 10 quan acaba en zero.
7. Un nombre és divisible per 11 quan la suma de les xifres de posició senar menys la suma de la xifres de posició parell resulta un nombre múltiple de 11.
8. Un nombre és múltiple de 25 quan acaba en 00, 25, 50 o 75.

Apliqueu les congruències per a fer l'exercici següent:

Exercici 6.4. *Trobeu tots els enters positius n tals que $2^n - 1$ és divisible per 7. Així mateix, demostreu que no existeix cap enter positiu tal que $2^n + 1$ sigui divisible per 7.*

Exercici 6.5.

1. *Demostra que tot quadrat perfecte és congruent amb 0 o amb 1 mòdul 4.*
2. *(Olimpíades 2004) Troba totes les possibles maneres d'escriure 2003 com a suma de dos quadrats de nombres enters positius.*

Exercici 6.6. *Sobre una cinta mètrica de dos metres subdividida en mil·límetres, fem un senyal verd cada 11 mil·límitres i un senyal vermell cada 17 mil·límetres, ambdós començant des del mateix extrem. Trobar quants senyals verds estan a 1 mil·límetre d'un senyal vermell.*

Exercici 6.7. *A l'illa de Camelot viuen 13 camaleons vermells, 15 verds i 17 grocs. Quan dos de diferent color es troben cambien al tercer color. Podria donar-se la situació que tots tinguin el mateix color?*

Proposició 6.8 (Petit Teorema de Fermat)**.** *Sigui p un nombre primer i sigui a un nombre enter que no sigui múltiple de p. Aleshores*

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

Demostració: Considerem a, $2a$, $3a$, $\ldots$, $(p-1)\cdot a$. Provarem que si $a \cdot i \equiv a \cdot j \pmod{p}$ per $0 < i, j \leq p-1$ llavors $i = j$.

Suposem que $a \cdot i \equiv a \cdot j \pmod{p}$ per algun $i \neq j$ amb $0 < i, j \leq p-1$. Podem suposar sense pèrdua de generalitat que $i > j$. Llavors $a \cdot (i-j) \equiv 0 \pmod{p}$. Això vol dir que $p | a \cdot (i-j)$; però com que p no divideix a llavors hauria de ser que $p|(i-j)$, cosa impossible doncs $i - j < p$.

Llavors, d'una banda tenim que $a \cdot i \equiv r_i \pmod{p}$, per algun r_i tal que $0 < r_i \leq p-1$ i, a més $r_i \neq r_j$ quan $i \neq j$. Així doncs, cada un dels termes a, $2a$, $\ldots$, $(p-1)\cdot a$ és congruent amb algun dels nombres $1, 2, \ldots, p-1$, no necessàriament amb aquest ordre.

I d'altra banda,

$$a \cdot 2a \cdot \ldots \cdot (p-1) \cdot a = a^{p-1} \cdot (1 \cdot 2 \cdot \ldots \cdot (p-1)) = a^{p-1} \cdot (p-1)!$$

Per tant,

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$$

I com que $(p-1)!$ no és múltiple de p, podem simplificar i obtenim que

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

Exercici 6.9. *Provar que per qualsevol nombre primer p diferent de 2 i 5 existeix un múltiple de p que té totes les seves xifres formades per 9's.*

7 Bibliografia utilitzada i recomanada

1. Bujalance, Emilio i altres. *Elementos de Matemática Discreta*, Ed. Sanz y Torres, 1997.
2. García Capitán, F.J. *Un pequeño Manual para la Resolución de Problemas*
3. Moreno, M.A., Tellechea, E. *Colectivo de Problemas resueltos para Estudiantes de Alto Rendimiento*
4. *http://www.iecat.net/institucio/societats/SCMatematiques/index.asp* i cerqueu *publicacions electròniques*