ARITMÈTICA

Griselda Pascual i Xufré

Introducció.

En aquest capítol ens proposem aprendre a resoldre problemes d'Aritmètica. Segurament que la paraula aritmètica us sonarà a quelcom que vareu aprendre a l'escola primària i que no n'heu sentit a parlar més al llarg dels estudis secundaris. Per això, pensar ara a aprendre a resoldre problemes d'aritmètica us semblarà un xic estrany, potser fins i tot pensareu que està fora de lloc per la seva senzillesa. Si és així, esteu ben lluny de la realitat. Hi ha problemes d'aritmètica molt difícils; tant, que alguns d'ells s'ha tardat molt temps a resoldre a pesar de treballar-hi grans matemàtics. Recentment n'hem tingut un exemple: *El Teorema de Fermat.* Aquest teorema diu: *"Si n és un nombre natural més gran que 2, l'equació $x^n + y^n = z^n$ no té solucions en nombres enters."* El va enunciar Fermat cap a la meitat del segle XVII; fins l'any passat (1995) no s'ha trobat la demostració, i aquesta s'ha obtingut utilitzant mitjans de la més alta matemàtica. El Teorema de Fermat és un problema d'aritmètica perquè imposa que les solucions siguin nombres enters. Hi ha altres problemes d'aritmètica, com per exemple l'anomenada *Conjectura de Goldbach*, enunciada per aquest matemàtic l'any 1742, i que diu *"Tot nombre parell més gran que dos és suma de dos primers"*, que encara no estan resolts.

Si doneu un cop d'ull als problemes proposats, que pretenen ser una mostra dels problemes d'aritmètica que es poden presentar a aquest nivell, veureu que sempre només hi intervenen nombres enters i en algun cas racionals. Per això són problemes d'aritmètica. Han estat seleccionats de manera que els pogueu resoldre, o bé utilitzant propietats dels nombres enters que potser no les heu estudiat mai però teniu prou maduresa matemàtica per entendre-les, o bé amb recursos d'àlgebra i d'anàlisi que heu aprés en el batxillerat. Però si intenteu resoldre'ls, potser moltes vegades no sabreu ni per on començar.

Per això, encara que considerem prioritari revisar les propietats del nombres enters abans

esmentades, en lloc de fer-ne un llistat, ens ha semblat millor escollir de forma adequada uns quants problemes que intentarem pensar conjuntament, i incloure dins la forma de resoldre'ls les definicions i proposicions que siguin necessàries. (Donem per sabudes la definició de nombres enters i llurs operacions).

Observareu que hi ha dos tipus de problemes. Uns demanen que es busquin els nombres enters que satisfacin determinades condicions. Altres que es demostri alguna propietat de determinats nombres enters. Tant per als uns com per als altres hem procurat indicar una metodologia per a la seva resolució. Però, com podreu comprovar, moltes vegades compta molt l'enginy matemàtic que cal cultivar resolent molts problemes.

També veureu que de les proposicions que intercalem en els problemes, algunes van acompanyades de les demostracions i d'altres no. S'ha posat la demostració sempre que aquesta ens podia donar un camí per arribar a la solució del problema. Les altres proposicions podeu o intentar demostrar-les o bé cercar la demostració en algun llibre.

Finalment, només voldríem aconsellar-vos que us fessiu vosaltres un petit promptuari d'aritmètica, extraient dels problemes totes les definicions i propietats que hi trobeu. Crec que us serà útil quan us proposeu de resoldre altres problemes.

Problema 1. Trobeu tots els triangles rectangles de costats enters que tenen el perímetre igual a l'àrea. (És un problema clàssic).

En principi és un problema de geometria, ja que ens cal saber propietats dels triangles rectangles. Però com que l'única cosa que hem d'utilitzar són les mesures dels costats podem enunciar el mateix problema aritmèticament. Si designem per x, y les mesures dels catets i per z la de la hipotenusa, el teorema de Pitàgores diu que $z^2 = x^2 + y^2$; el perímetre del triangle és $x + y + z$ i l'àrea $\frac{1}{2}xy$. Per tant podem enunciar el problema així:

Trobeu totes les solucions en nombres naturals (les mesures són sempre positives) del sistema d'equacions

$$z^2 = x^2 + y^2$$
$$x + y + z = \frac{1}{2}xy.$$

Solució. Fent us dels coneixements d'àlgebra, com que la segona equació és lineal en z,

aïllarem z en aquesta equació i la substituirem a la primera. Obtindrem

$$z = \frac{1}{2}xy - (x+y)$$
$$\left(\frac{1}{2}xy - (x+y)\right)^2 = x^2 + y^2.$$

La segona equació és una equació de segon grau en dues incògnites que, després de desenvolupada i simplicada, queda de la forma:

$$x^2y^2 - 4xy(x+y) + 8xy = 0$$

o sigui

$$xy\,(xy - 4(x+y) + 8) = 0$$

Les solucions d'aquesta equació són $x = 0, y = 0$, i els valors que són solució de l'equació $xy - 4(x+y) + 8 = 0$.

En aquest moment entra l'aritmètica. Quins valors naturals de x, y satisfan aquesta equació? Per trobar-los només necessitem un xic d'enginy. Observem que si en el numerador en lloc d'un 8 hi hagués un 16 les coses serien molt senzilles. Doncs bé, fem entrar el 16 escrivint:

$$x = \frac{4y - 16}{y - 4} + \frac{8}{y - 4} = 4 + \frac{8}{y - 4}.$$

D'aquí resulta que x serà natural si i només si $y - 4$ divideix 8. Com que els divisors de 8 són 8, 4, 2, 1 haurà de ser $y - 4 = 8, 4, 2, 1$ i per tant les solucions són

$$y = 12, x = 5; \quad y = 8, x = 6; \quad y = 6, x = 8; \quad y = 5, x = 12.$$

Els únics triangles rectangles solució del problema seran el que tingui catets 12 i 5 i hipotenusa 13, i el que tingui catets 8 i 6 i hipotenusa 10.

Problema 2. El nombre 9687600 es pot escriure com a producte de nombres enters consecutius, un dels quals és primer. Calculeu quins són aquests factors.

Aquest problema és clarament un problema d'aritmètica; només hi intervenen nombres enters. Necessitem saber què és un nombre primer, amb la qual cosa entrem a la *divisibilitat* de nombres enters. En el problema anterior ja hem utilitzat que els nombres naturals divisors de 8 són 1, 2, 4, 8 sense donar la definició de divisor. Ho fem a continució.

Definició. Donats dos nombres enters a i b es diu que b és múltiple de a o a divisor de b si existeix un nombre enter que multiplicat per a doni b; és a dir si l'equació $ax = b$ té solució en nombres enters. S'escriu $b = \dot{a}$ o bé $a|b$.

Tot nombre natural diferent de 1 té almenys dos divisors que són ell mateix i la unitat.

Definició. Un nombre natural es diu que és primer quan només té dos divisors. Quan té més de dos divisors es diu que és compost. El nombre 1 no és ni primer ni compost; es diu que és una unitat.

El nom de primer ve suggerit pel següent teorema, que per la seva importància, s'anomena

Teorema fonamental. Tot nombre natural compost descompon de manera única (sense tenir en compte l'ordre) en producte de factors primers.

Ara ja tenim el que necessitem per resoldre el problema. Veiem que el nombre 9687600 és compost ja que acaba en dos zeros. Descomponem-lo en factors primers:

$$9687600 = 2^4 \cdot 3^4 \cdot 5^2 \cdot 13 \cdot 23.$$

També aquí fem servir l'enginy per agrupar adequadament els factors i trobem que

$$8687600 = 23 \cdot 24 \cdot 25 \cdot 26.$$

Problema 3. Trobeu totes les solucions enteres de l'equació

$$p(x + y) = xy$$

on p és un nombre primer.

Observem que el primer membre de l'equació és el producte d'un nombre primer per la suma dels dos nombres que hem de cercar, i el segon el producte d'aquests dos nombres. Per resoldre'l utilitzarem la següent

Propietat. Si un nombre primer divideix un producte de dos nombres enters, en divideix almenys un.

Suposem que p divideix x i posem $x = pt$ amb t un nombre enter. Substituint aquesta expressió a l'equació donada es té:

$$p(pt + y) = pty, \quad \text{d'on} \quad pt + y = ty, \quad \text{o} \quad pt = y(t-1).$$

Com que t i $t-1$ no tenen cap divisor en comú, o p dividiex y, o $p = t-1$ i $y = t$.
Si p divideix y és $y = pu$ amb u un nombre enter, i substituint a l'equació que havíem obtingut resulta $pt = pu(t-1)$ d'on $t = u(t-1)$. Si $t = 0$, com que $t-1$ és diferent de zero ha de ser $u = 0$, i aquests valors ens proporcionen la solució $x = 0$, $y = 0$. Si $t \neq 0$ ha de ser $t - 1 \neq 0$ i $u = \dfrac{t}{t-1} = 1 + \dfrac{1}{t-1}$. Com que u ha de ser un enter diferent de zero, haurà de ser $t - 1 = 1$, és a dir $t = 2$ i $u = 2$, d'on s'obté la solució $x = 2p$, $y = 2p$.
Si $p = t - 1$ i $y = t$ s'obté la solució $y = p + 1$, $x = py = p(p+1)$. Com que l'equació és simètrica en x, y el mateix raonament fet amb la incògnita x es pot fer amb la incògnita y amb la qual cosa obtindrem la solució $x = p + 1, y = p(p+1)$.
Exemple. Si $p = 5$ les solucions són $x = 0, y = 0$; $x = 10, y = 10$; $x = 30, y = 6$; $x = 6, y = 30$.

Problema 4. Trobeu un nombre natural n sabent que adment només dos divisors primers diferents, que el nombre dels seus divisors és 6 i que la suma de tots els seus divisors és 28.

Per resoldre aquest problema ens cal saber calcular el nombre de divisors d'un nombre natural n i la suma de tots els seus divisors. Per això tenim la següent

Proposició. Si n descompon en factors primers de manera que

$$n = {p_1}^{a_1} {p_2}^{a_2} \cdots {p_r}^{a_r}$$

amb p_i, $(i = 1, 2, \ldots, r)$ nombres primers diferents, s'indica per $d(n)$ el nombre de divisors de n i per $s(n)$ la suma de tots aquests divisors, i es compleix

$$d(n) = (a_1 + 1)(a_2 + 1) \cdots (a_r + 1); \quad s(n) = \frac{{p_1}^{a_1+1} - 1}{p_1 - 1} \cdot \frac{{p_2}^{a_2+1} - 1}{p_2 - 1} \cdots \frac{{p_r}^{a_r+1} - 1}{p_r - 1}.$$

Intenteu demostrar aquesta proposició.
Ja estem en condicions de resoldre el problema. Posem $n = p^a q^b$ on p i q representen els dos divisors primers diferents que divideixen n. Per les fòrmules de la proposició ha de ser

$$(a+1)(b+1) = 6; \quad \frac{p^{a+1} - 1}{p - 1} \cdot \frac{q^{b+1} - 1}{q - 1} = 28$$

Com que $a \geq 1$, $b \geq 1$, l'única descomposició possible de 6 vàlida és $6 = 2 \cdot 3$; per tant de la primera equació resulta $a + 1 = 2$, $b + 1 = 3$,o sigui $a = 1$, $b = 2$.
Llavors la segona equació pren la forma

$$\frac{p^2 - 1}{p - 1} \cdot \frac{q^3 - 1}{q - 1} = 28 \quad \text{i simplificant} \quad (p + 1)(q^2 + q + 1) = 2^2.7.$$

Com que p és primer $p+1=4$ i $p = 3$, i de $q^2+q+1 = 7$ resulta $q = 2$. El nombre cercat és per tant $n = 2^2.3 = 12$.

Problema 5. Resoldre amb nombres naturals el sistema d'equacions

$$\left.\begin{array}{c} xy = 51840 \\ \text{mcd}(x, y) = 24 \end{array}\right\}.$$

En aquest problema hi intervé el concepte de màxim comú divisor de dos nombres naturals. Recordem-ho,

> **Definició.** 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 $\text{mcd}(a, b) = d$. Si $d = 1$ és diu que els dos nombres són primers entre si o primers entre ells.

> **Proposició.** Si es divideixen dos nombres a i b pel seu màxim comú divisor, s'obtenen dos nombres primers entre ells.

Ara tenim tot el que necessitem per resoldre el problema.
Posem $x = 24t$, $y = 24u$ on t i u representen enters primers entre si. Llavors $24^2tu = 51840$ i per tant $tu = \dfrac{51840}{576} = 90$. Només ens cal ara, descompondre 90 de totes les maneres possibles amb factors primers entre si, per obtenir totes les solucions del problema. $90 = 45 \cdot 2 = 9 \cdot 10 = 18 \cdot 5$. Fent $t = 45$, $u = 2$ es té $x = 1080$, $y = 48$; fent $t = 9$, $u = 10$ es té $x = 216$, $y = 240$; i finalment fent $t = 18$, $u = 5$ es té $x = 432$, $y = 120$. Permutant la x i la y s'obté una altra terna de solucions.

Per tal de determinar el màxim comú divisor de dos nombres naturals cal tenir en compte que es disposa d'un algoritme molt útil que només fa ús de la divisió entera.

Algorisme d'Euclides. Siguin a i b dos nombres naturals, $a > b$. La divisió entera de a per b ens dóna dos nombres q_1, r_1 que compleixen $a = bq_1 + r_1$, $r_1 < b$. Dividint b per r_1 tindrem $b = r_1q_2 + r_2$ amb $r_2 < r_1$; dividint r_1 per r_2 serà $r_1 = r_2q_3 + r_3$ amb $r_3 < r_2$. Seguint aquest procés, com que els residus formen una successió de nombres naturals decreixent, s'arribarà a un residu 0. L'últim residu no nul obtingut és el màxim comú divisor de a i b. Per facilitar el càlcul s'acostumen a posar els diversos nombres que intervenen a l'algorisme en la forma següent:

	q_1	q_2	$\cdots$	q_{k+1}	q_{k+2}	q_{k+3}
a	b	r_1	$\cdots$	r_k	r_{k+1}	r_{k+2}
r_1	r_2	r_3	$\cdots$	r_{k+2}	0	

$$r_{k+2} = \mathrm{mcd}(a, b)$$

Problema 6. Trobeu dos nombres enters que satisfacin l'equació

$$1547x + 560y = 7.$$

Anem a veure con l'algoritme d'Euclides es pot utilitzar per resoldre aquesta equació. Comencem aplicant-lo per trobar el $\mathrm{mcd}(1547, 560)$.

	2	1	3	4	1	3
1547	560	427	133	28	21	7
427	133	28	21	7	0	

i observeu que $\mathrm{mcd}(1547, 560) = 7$. Escriviu els resultats parcials

$$7 = 28 - 1 \cdot 21$$

$$21 = 133 - 4 \cdot 28$$

$$28 = 427 - 3 \cdot 133$$

$$133 = 560 - 1 \cdot 427$$

$$427 = 1547 - 2 \cdot 560$$

i feu les succesives substitucions:

$$\begin{aligned} 7 &= 28 - 1 \cdot 21 = 28 - 1 \cdot (133 - 4 \cdot 28) = 5 \cdot 28 - 1 \cdot 133 = 5 \cdot (427 - 3 \cdot 133) - 1 \cdot 133 \\ &= 5 \cdot 427 - 16 \cdot 33 = 427 - 16 \cdot (560 - 1 \cdot 427) = 21 \cdot 427 - 16 \cdot 560 \\ &= 21 \cdot (1547 - 2 \cdot 560) - 16 \cdot 560 = 21 \cdot 1547 - 58 \cdot 560. \end{aligned}$$

amb la qual cosa heu obtingut la igualtat

$$1547 \cdot 21 + 560 \cdot (-58) = 7$$

Per tant $x = 21$, $y = -58$ són dos dels nombres cercats. Aquests no són els únics ja que posant

$$x = 21 - 560t \quad y = -58 + 1547t$$

i substituint a l'equació resulta

$$1547 \cdot (21 - 560t) + 560 \cdot (-58 + 1547t) = 7.$$

Donant a t tots els valors enters obtindreu totes les solucions.

Problema 7. Resoleu el sistema d'equacions

$$\left.\begin{array}{c} \text{mcm}(x, y) = 546212 \\ xy = 983016 \end{array}\right\}$$

En aquest problema intervé el concepte de mínim comú múltiple. Recordem la

> **Definició.** 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.

El problema es pot ara reduir al Problema 5 aplicant la següent

> **Propietat.** Es compleix sempre
>
> $$\text{mcm}(a, b) = \frac{ab}{\text{mcd}(a, b)} \quad \text{o bé} \quad \text{mcd}(a, b) = \frac{ab}{\text{mcm}(a, b)}.$$

Resulta

$$\text{mcd}(x, y) = \frac{983016}{54612} = 18$$

i ja estem en les condicions del Problema 5. Seguint aquells passos obtenim les solucions

$$x = 1332, y = 738; \quad x = 1476, y = 666; \quad x = 36, y = 27306.$$

Problema 8. Els tres nombres naturals $1652_{(b}$, $2012_{(b}$, $2042_{(b}$ (escrits en base b) estan en progressió arimètica. Determineu la base b i la raó de la progressió.

En aquest problema hi intervenen dos conceptes, el de base d'un sistema de numeració i el de progressió aritmètica. El primer resulta de la següent

> **Proposició.** Donat un nombre natural $b \geq 2$, tot nombre natural n es pot escriure de manera única de la forma
>
> $$n = a_0 + a_1 b + a_2 b^2 + \cdots + a_r b^r$$
>
> on els a_i, $i = 0, 1, ..., r$ són nombres naturals menors que b amb $a_r \neq 0$. El nombre expressat així es diu que està escrit en el sistema de numeració de base b.

Recordem el segon concepte del problema.

> **Definició.** Una successió de nombres a_1, $a_2, ..., a_i$, $a_{i+1}, ..., a_n, ...$ forma una progressió aritmètica quan la diferència de dos termes consecutius $a_{i+1} - a_i$ és un nombre constant r que s'anomena raó de la progressió.

Sabent això la resolució del problema proposat no presenta cap dificultat.
S'ha de complir

$$(2b^3 + 4b + 2) - (2b^3 + b + 2) = (2b^3 + b + 2) - (b^3 + 6b^2 + 5b + 2)$$

que després d'operar queda de la forma

$$b^3 - 6b^2 - 7b = 0$$

Ara cal resoldre aquesta equació de tercer grau amb l'incògnita b. En aquest cas és fàcil perquè es pot treure b factor comú i resoldre

$$b(b^2 - 6b - 7) = 0$$

Una solució és $b = 0$, i les altres dues les solucions de l'equació de segon grau $b^2 - 6b - 7 = 0$ es veuen immediatament: $b = -1$, $b = 7$. D'aquestes tres solucions la única vàlida pel nostre problema és $b = 7$ ja que s'ha de complir la condició $b \geq 2$.
La raó de la progressió és $r = 3b = 21$.

Problema 9. Trobeu quin és l'exponent de 2 en la descomposició en factors primers de 29!.
Per analitzar el problema escrivim el desenvolupament de 29!.

$$29! = 1 \cdot \underline{2} \cdot 3 \cdot \underline{\underline{4}} \cdot 5 \cdot \underline{6} \cdot 7 \cdot \underline{\underline{\underline{8}}} \cdot 9 \cdot \underline{10} \cdot 11$$

$$\cdot \underline{\underline{12}} \cdot 13 \cdot \underline{14} \cdot 15 \cdot \underline{\underline{\underline{16}}} \cdot 17 \cdot \underline{18} \cdot 19 \cdot \underline{\underline{20}}$$

$$\cdot 21 \cdot \underline{22} \cdot 23 \cdot \underline{\underline{24}} \cdot 25 \cdot \underline{26} \cdot 27 \cdot \underline{28} \cdot 29$$

Subratllem amb una ratlleta els múltiples de 2 i observem que d'aquests n'hi ha uns que només tenen una vegada el factor 2 i d'altres que el tenen més d'una vegada. Subratllem amb una altra ratlleta els que tenen el factor 2 dues vegades és a dir els múltiples de 4; també d'aquests n'hi ha que només el tenen dues vegades i d'altres que el tenen més de dues vegades. Subratllem amb una altra ratlleta els que el tenen més de dues vegades és a dir els múltiples de 8. També d'aquests n'hi ha que el tenen només tres vagades i d'altres que el tenen més de tres vegades és a dir els múltiples de 16 que els subratllem amb una altra ratlleta. Observem que no n'hi ha cap que tingui el factor 2 més de quatre vegades, ja que si algún el tingués cinc vegades seria múltiple de 32 i $32 > 29$. L'exponent amb què figura 2 a la descomposició de 29! és igual al total del nombre de ratlletes que hem dibuixat o sigui 14+7+3+1=25. Si recordem que la part entera d'un nombre x és el nombre enter més gran que és més petit o igual que x, que l'expressem per $[x]$, observarem que $14 = \left[\frac{29}{2}\right]$, $7 = \left[\frac{29}{2^2}\right]$, $3 = \left[\frac{29}{2^3}\right]$, $1 = \left[\frac{29}{2^4}\right]$. Per tant podem escriure que l'exponent amb que figura 2 a la descomposició amb factors primers de 29! és

$$a = \left[\frac{29}{2}\right] + \left[\frac{29}{2^2}\right] + \left[\frac{29}{2^3}\right] + \left[\frac{29}{2^4}\right].$$

El mateix raonament que hem fet amb 29! i el primer 2 és vàlid per a $n!$, n un enter qualsevol i un nombre primer p.
Per exemple, si volem calcular l'exponent a en què figura 7 en la descomposició de 1000!, com que $7^4 = 2041 > 1000$, farem

$$a = \left[\frac{1000}{7}\right] + \left[\frac{1000}{7^2}\right] + \left[\frac{1000}{7^3}\right] = 142 + 20 + 2 = 164.$$

Seria vàlid el raonament si p no fos primer? Intenta amb un exemple donar la resposta.
En general podem enunciar la següent

Proposició. L'exponent a en que figura un primer p en la descomposició de $n!$ en factors primers és

$$a = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots.$$

Encara que hem posat punts suspensius aquesta suma sempre acabarà ja que $\left[\frac{n}{p^k}\right] = 0$ si $p^k > n$.

Problema 10. Determineu les possibles bases de numeració x en les quals el nombre $532_{(x}$ és múltiple de 5.

Pel problema 8 sabem que aquest problema és equivalent a trobar tots els nombres naturals $x \geq 2$ tals que $5x^2 + 3x + 2$ és múltiple de 5.
Observem, en primer lloc, que $5x^2$ és múltiple de 5 per qualsevol valor enter de x; per tant el problema queda reduït a trobar tots els valors enters de $x \geq 2$ tals que $3x + 2$ és múltiple de 5, és a dir $3x + 2 = 5k$ on k ha de ser un nombre enter. Seguint les indicacions del problema 6, i pensant un xic, podríem resoldre en nombres enters l'equació $3x - 5k = 2$ Però podem trobar un camí més curt introduïnt un concepte nou que, com veurem més endavant, ens serà molt útil per resoldre molts problemes. És la noció de *congruència* de nombres enters respecte d'un nombre natural $m > 1$ que s'anomena *mòdul* de la congruència.
Comencem amb un exemple que ens servirà per resoldre el problema proposat.
Considerem el conjunt $\mathbb{Z}$ dels nombres enters on hi tenim definit la suma, el producte, i divisió entera. Prenem $m = 5$ com a mòdul de la congruència. Observem que tot nombre enter o serà múltiple de 5, o en dividir-lo per 5 donarà residus 1, 2, 3, o 4. Això ens permet classificar el conjunt $\mathbb{Z}$ en cinc classes disjuntes que designarem per $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, posant a la classe $\overline{0}$ els múltiples de 5, i a les classes $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$ els nombres que donin respectivament residu 1, 2, 3, 4 en dividir-los per 5. És a dir

$$\overline{0} = 5k, \quad \overline{1} = 5k + 1, \quad \overline{2} = 5k + 2, \quad \overline{3} = 5k + 3, \quad \overline{4} = 5k + 4$$

on en cada cas k pren tots els valors enters. Donem ara la següent

Definició. Dos nombres $a, b \in \mathbb{Z}$ són congrus (o congruents) segons el mòdul 5, i s'indica per $a \equiv b \pmod 5$, quan pertanyen a la mateixa classe, és a dir, quan donen el mateix residu en dividir-los per 5.

És fàcil provar que $a \equiv b \pmod 5$ si i només si $a - b$ és múltiple de 5. Per tant es pot donar la definició equivalent

> **Definició.** Es diu que dos nombres enters a i b són congrus (o congruents) segons el mòdul 5 quan $a - b$ és múltiple de 5.

Les classes $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$ s'anomenen classes de congruències mòdul 5.
Observem que el mateix que hem fet amb el 5, podem fer-ho agafant per mòdul qualsevol enter $m > 1$ i per tant donar en general la següent

> **Definició.** Dos nombres enters a, b són congrus (o congruents) segons el mòdul m quan donen el mateix residu en dividir-los per m. S'escriu $a \equiv b \pmod m$.

O equivalentment

> **Definició.** Dos nombres enters a, b són congrus (o congruents) segons el mòdul m quan la diferència $a - b$ és múltiple de m.

(Intentem demostrar l'equivalència d'aquestes dues definicions).

Segons el mòdul m es tenen m classes de congruència que corresponen als diferents residus 0, 1, 2, 3,...,$m - 1$ que s'obtenen en dividir un nombre enter per m.
La relació $a \equiv b \pmod m$ és una relació de congruència o abreujadament es diu que és una congruència.
Les congruències tenen les següents

Propietats.

1) Si $a \equiv b \pmod m$ i $c \equiv d \pmod m$, llavors $a + c \equiv b + d \pmod m$.
2) Si $a \equiv b \pmod m$ i c és un enter qualsevol, llavors $ca \equiv cb \pmod m$.
3) Si $a \equiv b \pmod m$ i $c \equiv d \pmod m$, llavors $ac \equiv bd \pmod m$.
4) Si $a \equiv b \pmod m$ i d divideix m, llavors $a \equiv b \pmod d$ i $a \equiv b \pmod{m/d}$.
5) Si $ca \equiv cb \pmod m$ i $\text{mcd}(c, m) = 1$, llavors $a \equiv b \pmod m$.

Observeu que a la propietat 5) és necessari que $\text{mcd}(a,b) = 1$. Per exemple $10 \equiv 16 \pmod 6$ i $5 \not\equiv 8 \pmod 6$.

(Intentem demostrar aquestes propietats).

Apliquem ara les congruències a la resolució del problema proposat.

Ha de ser $5x^2 + 3x + 2 \equiv 0 \pmod 5$. Com que per tot enter x és $5x^2 \equiv 0 \pmod 5$, els valors buscats seran tots els enters x més grans que 1 que satisfacin la congruència $3x + 2 \equiv 0 \pmod 5$, o sigui $3x \equiv -2 \pmod 5$. Però $-2 \equiv 3 \pmod 5$ per tant $3x \equiv 3 \pmod 5$ i simplificant $x \equiv 1 \pmod 5$.

D'aquí resulta que les bases de numeració possibles són tots els enters de la forma $x = 5k+1$ on k representa qualsevol enter positiu.

Problema 11. Trobeu tots els enters positius n tals que $2^n - 1$ és divisible per 7.

Solució. Escriviu l'enunciat en la forma $2^n - 1 \equiv 0 \pmod 7$ o sigui $2^n \equiv 1 \pmod 7$. Només cal veure quines potències de 2 són congrues amb 1 segons el mòdul 7. Es té:

$$2^0 \equiv 1(\text{mod } 7), \quad 2^1 \equiv 2(\text{mod } 7), \quad 2^2 \equiv 4(\text{mod } 7), \quad 2^3 \equiv 1(\text{mod } 7).$$

A partir d'aquí, per les propietats de les congruències, els residus s'aniran repetint de 3 en 3, és a dir

$$2^4 \equiv 2(\text{mod } 7), \quad 2^5 \equiv 4(\text{mod } 7), \quad 2^6 \equiv 1(\text{mod } 7), \text{etc.}$$

D'aquí resulta que

$$2^n \equiv 1(\text{mod } 7) \Longleftrightarrow n \equiv 0(\text{mod } 3)$$

$$2^n \equiv 2(\text{mod } 7) \Longleftrightarrow n \equiv 1(\text{mod } 3)$$

$$2^n \equiv 4(\text{mod } 7) \Longleftrightarrow n \equiv 2(\text{mod } 3).$$

Com que $2^n - 1$ és múltiple de 7 si i només si n és múltiple de 3, les solucions del problema són tots els enters positius múltiples de 3.

Fixeu-vos que a més a més de resoldre el problema proposat hem obtingut tots aquests altres resultats.

La solució amb enters positius de l'equació $2^n + 6 \equiv 0 \pmod 7$ la formen tots els enters positius $n \equiv 0 \pmod 3$.

Les solucions amb enters positius de les equacions $2^n - 2 \equiv 0$ i $2^n + 5 \equiv 0 \pmod 7$ les formen tots els enters positius $n \equiv 1 \pmod 3$.

Les solucions amb enters positius de les equacions $2^n - 4 \equiv 0$ i $2^n + 3 \equiv 0 \pmod 7$ les formen tots els enters positius $n \equiv 2 \pmod 3$.

Les equacions $2^n - 6 \equiv 0$, $2^n + 1 \equiv 0$, $2^n - 3 \equiv 0$, $2^n + 4 \equiv 0 \pmod 7$ no tenen solució amb enters positius.

Problema 12. Trobeu totes les parelles de nombres enters (x, y) tals que $x^2 = 21 + 4y^2$.

Aquest és un problema d'aritmètica que té una interpretació geomètrica important. L'equació donada es pot escriure en la forma $\dfrac{x^2}{21} - \dfrac{y^2}{\frac{21}{4}} = 1$, on reconeixem que es tracta de l'equació d'una hipèrbola de semieixos $a = \sqrt{21}$, $b = \dfrac{1}{2}\sqrt{21}$. Per tant el problema s'hauria pogut enunciar així:

Trobeu tots els punts de coordenades enteres de la cònica $x^2 = 21 + 4y^2$.

Aquest és un cas particular del problema següent: Trobar els punts de coordenades enteres d'una cónica donada per una equació amb coeficients enters.

En general aquest és un problema d'aritmètica difícil, però en casos particulars com per exemple la nostra cònica, es pot resoldre fàcilment.

Si escrivim l'equació de la cónica en la forma $x^2 - 4y^2 = 21$, observarem que el primer membre és una diferència de quadrats i per tant es pot posar en la forma $(x-2y)(x+2y) = 21$. Com que x, y han de ser enters, també ho han de ser $x - 2y$, $x + 2y$ i aquests podran prendre tants valors com possibles descomposicions en factors enters del nombre 21. Com que $21 = 1 \cdot 21 = (-1) \cdot (-21) = 3 \cdot 7 = (-3) \cdot (-7)$, les solucions estaran entre les dels sistemes:

$$\left.\begin{matrix} x - 2y = 1 \\ x + 2y = 21 \end{matrix}\right\} \quad \left.\begin{matrix} x - 2y = 21 \\ x + 2y = 1 \end{matrix}\right\} \quad \left.\begin{matrix} x - 2y = -1 \\ x + 2y = -21 \end{matrix}\right\} \quad \left.\begin{matrix} x - 2y = -21 \\ x + 2y = -1 \end{matrix}\right\}$$

$$\left.\begin{matrix} x - 2y = 3 \\ x + 2y = 7 \end{matrix}\right\} \quad \left.\begin{matrix} x - 2y = 7 \\ x + 2y = 3 \end{matrix}\right\} \quad \left.\begin{matrix} x - 2y = -3 \\ x + 2y = -7 \end{matrix}\right\} \quad \left.\begin{matrix} x - 2y = -7 \\ x + 2y = -3 \end{matrix}\right\}$$

Aquestes són respectivament $(11, 5)$, $(11, -5)$, $(-11, -5)$, $(-11, 5)$, $(5, 1)$, $(5, -1)$, $(-5, 1)$, i com que totes són enteres, totes són solucions del problema. Per tant els únics punts de coordenades enteres de la hipèrbola d'equació $x^2 = 21 + 4y^2$ són els que acabem de trobar. Intenteu dibuixar aquesta hipèrbola.

Problema 13. Per cada nombre natural n escrivim

$$(1 + \sqrt{2})^{2n+1} = a_n + b_n\sqrt{2}$$

i així tenim dues successions de nombres enters

$$a_1, a_2, ..., a_n, ... \qquad b_1, b_2, ..., b_n, ...$$

a) Demostreu que a_n i b_n són senars per tot nombre natural n.

b) Demostreu que b_n és la hipotenusa d'un triangle rectangle de catets

$$\frac{a_n + 1}{2}, \qquad \frac{a_n - 1}{2}.$$

Observeu que en aquest cas es tracta de demostrar unes propietats que les satisfan tots els nombres naturals. Per als problemes d'aquest tipus és sempre molt útil tenir present una propietat que és característica del conjunt dels nombres naturals, i que ara enunciarem.

Principi d'inducció matemàtica.

Si C és un conjunt de nombres naturals que compleix

1) 1 pertany a C
2) si un nombre natural k pertany a C, el seu següent $k + 1$ també pertany a C

llavors C és el conjunt de tots els nombres naturals.

Aquest principi és un axioma pel conjunt dels nombres naturals, és a dir no es demostra. El podem aplicar sempre que volguem demostrar que una propietat és certa per tots els nombres naturals. N'hi ha prou a provar que és certa per a 1 i que si és certa per a un natural arbitrari k també ho és per al seu següent $k + 1$.

És interessant veure com induint podriem descobrir les propietats enunciades en el problema.

Part a). Calculeu el valor de l'expressió $(1 + \sqrt{2})^{2n+1}$ per uns quants nombres naturals consecutius, començant per $n = 1$.

$$\begin{aligned}
n=1 \quad & (1+\sqrt{2})^3 = (1+\sqrt{2})(1+\sqrt{2})^2 = (1+\sqrt{2})(3+2\sqrt{2}) = 7+5\sqrt{2} \\
n=2 \quad & (1+\sqrt{2})^5 = (1+\sqrt{2})^3(1+\sqrt{2})^2 = (7+5\sqrt{2})(3+2\sqrt{2}) = 41+29\sqrt{2} \\
n=3 \quad & (1+\sqrt{2})^7 = (1+\sqrt{2})^5(1+\sqrt{2})^2 = (41+29\sqrt{2})(3+2\sqrt{2}) = 239+169\sqrt{2}
\end{aligned}$$

Podeu continuar un xic més donant a n uns quants valors més, i observem que en tots els casos és

$$(1 + \sqrt{2})^{2n+1} = a_n + b_n\sqrt{2}$$

on a_n i b_n són nombres enters imparells. Ens preguntem si això serà cert per tots els valors de n. La resposta la trobem aplicant el principi d'inducció.

Ja hem vist que és cert per a $n = 1$.

Suposem que és cert per a un natural qualsevol $n = k$, és a dir que se satisfà

$$(1+\sqrt{2})^{2k+1} = a_k + b_k\sqrt{2}$$

on a_k i b_k són nombres naturals imparells. Calculem

$$\begin{aligned}(1+\sqrt{2})^{2(k+1)+1} &= (1+\sqrt{2})^{2k+3} = (1+\sqrt{2})^{2k+1}(1+\sqrt{2})^2 = (a_k + b_k\sqrt{2})(3+2\sqrt{2}) \\ &= (3a_k + 4b_k) + (2a_k + 3b_k)\sqrt{2}.\end{aligned}$$

Com que a_k i b_k són per hipòtesi nombres naturals imparells, $a_{k+1} = 3a_k + 4b_k$ i $b_{k+1} = 2a_k + 3b_k$ també seran imparells, i pel principi d'inducció seran imparells per tot valor natural de n

Part b). És clar que en ser a_n imparell, $\dfrac{a_n - 1}{2}$ i $\dfrac{a_n + 1}{2}$ seran enters. Calculem-los per uns quants valors de n.

$$\begin{aligned}
n = 1 \quad & \frac{a_1 - 1}{2} = 3 \quad \frac{a_1 + 1}{2} = 4 \quad b_n = 5 \\
n = 2 \quad & \frac{a_2 - 1}{2} = 20 \quad \frac{a_2 + 1}{2} = 21 \quad b_n = 29 \\
n = 3 \quad & \frac{a_3 - 1}{2} = 119 \quad \frac{a_3 + 1}{2} = 120 \quad b_n = 169
\end{aligned}$$

Observem que és $3^2 + 4^2 = 25 = 5^2$, $20^2 + 21^2 = 881 = 29^2$, $119^2 + 121^2 = 28651 = 169^2$ és a dir que les ternes (3, 4, 5), (20, 21, 29), (119, 120, 169) són solucions de l'equació $x^2 + y^2 = z^2$ i per tant compleixen el teorema de Pitàgoras.

Per demostrar que per a tot n se satisfà

$$\left(\frac{a_n - 1}{2}\right)^2 + \left(\frac{a_n + 1}{2}\right)^2 = {b_n}^2$$

escrivim aquesta igualtat en la forma

$$a_n^2 + 1 = 2b_n^2$$

que ja hem vist que és certa per a $n = 1$. Suposem que és certa per a un natural qualsevol $n = k$ és a dir que $a_k^2 + 1 = 2b_k^2$ i anem a provar que també ho és per a $n = k + 1$. Com que $a_{k+1} = 3a_k + 4b_k$ i $b_{k+1} = 2a_k + 3b_k$ resulta

$${a_{k+1}}^2 + 1 = (3a_k + 4b_k)^2 + 1 = 8a_k^2 + 24a_k b_k + 18b_k^2 = 2(2a_k + 3b_k)^2 = 2b_{k+1}^2.$$

Pel principi d'inducció queda demostrat que per a tot natural n, $\frac{a_n-1}{2}$ i $\frac{a_n+1}{2}$ són els catets d'un triangle rectangle de hipotenusa b_n.

Problema 14. Proveu que si $n \in \mathbb{Z}$ és positiu i p és primer, llavors $n^p - n$ és múltiple de p.

Com que un enter positiu s'identifica amb un nombre natural podem aplicar el principi d'inducció.

Per a $n = 1$ és $1^p - 1 = 0$ i com que el zero és múltiple de tots els nombres, és múltiple de p.

Suposem que per a un nombre natural qualsevol k és $k^p - k$ múltiple de p, i calculem

$$\begin{aligned}(k+1)^p - (k+1) &= k^p + \binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + \cdots + \binom{p}{j}k^{p-j} + \cdots + \binom{p}{p-1}k + 1 \\ &\quad - (k+1) \\ &= k^p - k + \binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + \cdots + \binom{p}{j}k^{p-j} + \cdots + \binom{p}{p-1}k.\end{aligned}$$

Com que per la hipòtesi d'inducció $k^p - k$ és múltiple de p, només cal demostrar que la suma restant és múltiple de p. Demostrarem que cada sumand és múltiple de p (que és més fort que el que ens demanen), provant que $\binom{p}{j}k^{p-j}$ $j = 1, 2, ..., p-1$ és múltiple de p. Sabem de la teoria combinatòria que

$$\binom{p}{j} = \frac{p!}{j!(p-j)!}$$

i que és un nombre natural; pel problema 9 sabem que l'exponent en que figura p en $p!$ és 1, i com que $j < p$ i $p - j < p$ en $j!$ i en $(p-j)!$ hi figurarà amb exponent 0 per tant en el quocient $\frac{p!}{j!(p-j)!}$ amb exponent 1, és a dir és múltiple de p.

Als matemàtics, meditar sobre un problema resolt els porta quasi sempre a fer-se noves preguntes. Anem a fer-nos-en nosaltres. Fixeu-vos que a l'enunciat del problema s'imposa la condició que n sigui un enter positiu, i això ens ha permès fer la demostració per inducció.

Primera pregunta. És pot afirmar el mateix quan n és negatiu? És clar que la demostració per inducció no és vàlida. Però considereu alguns casos particulars. Per exemple poseu $p = 5$ i calculeu $n^5 - n$ per uns quants valors negatius de n, i trobareu que sempre és múltiple de 5. Abans de arriscar-nos a conjecturar res proveu per a alguns altres

nombres primers per exemple $p = 7, 11$ i trobareu que sempre se satisfà. Ara ens atrevim a conjecturar

Per tot enter a i tot primer p, $a^p - a$ és múltiple de p.

Cal intentar de trobar una demostració.

Per això posarem $a^p - a = a(a^{p-1} - 1)$. Si a és múltiple de p és obvi que $a(a^{p-1} - 1)$ és múltiple de p. Però si p no divideix a i la conjectura és certa, p ha de dividir $a^{p-1} - 1$ que és el que hem de demostrar. Això és cert, i és una proposició molt important d'aritmètica que s'anomena *Congruència de Fermat*, fent honor al matemàtic que la va enunciar per primera vegada. Pel seu nom ja deveu sospitar que per demostrar-la utilitzarem les congruències que varem introduir en el problema 10. Anunciarem la proposició així:

> **Congruència de Fermat.** Si p és un nombre primer, i a un enter qualsevol primer amb p, és compleix
>
> $$a^{p-1} \equiv 1 (\text{mod } p).$$

Demostració. Considerem els nombres 1,2,...$p-1$. Cadascun d'ells pertany a una classe diferent mòdul p, i com que són tots els residus possibles que es podem obtenir en dividir un enter per p, les classes a les quals pertanyen són totes les classes possibles. Considerem ara els nombres $a \cdot 1$, $a \cdot 2$,...,$a \cdot (p-1)$. Aquests nombres són incongrus dos a dos ja que si $a \cdot k \equiv a \cdot l \pmod{p}$, $1 \leq k, l \leq p-1$ seria $a \cdot k - a \cdot l = a(k-l)$ múltiple de p i com que p no divideix a, p hauria de dividir $k - l$ o sigui que seria $k \equiv l \pmod{p}$ en contra del que hem dit abans. Per tant com que en tenim $p-1$, cadascun d'ells haurà de ser congru amb un i només un dels 1,2,...,$p-1$. Aplicant les propietats de les congruències és pot escriure

$$a \cdot 1 \cdot a \cdot 2 \cdot a \cdot 3 \cdots p-1 \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

o sigui $a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$. Com que $\text{mcd}(p, (p-1)!) = 1$ és pot simplificar la congruència dividint els dos membres per $(p-1)!$ i s'obté

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

que és el que voliem demostrar.

Segona pregunta. Què passa quan el mòdul no és un nombre primer? Comenceu amb un cas particular prenent, per exemple, per mòdul $m = 6$ i fent $a = 5$. És $\text{mcd}(5, 6) = 1$,

i $a^{m-1} = 5^5 \equiv 5 \pmod 6$, per tant no es compleix la congruència de Fermat. Alguna cosa de la demostració falla quan el mòdul no és primer. Repaseu-la a veure si ho trobeu. Podriem deixar aquí la qüestió per acabada, però encara ens farem una

Tercera pregunta. Pot ser que per un altre exponent $\phi(m)$ relacionant amb el mòdul d'una manera que es pugui determinar, resulti que si $\mathrm{mcd}(a,m) = 1$ és $a^{\phi(m)} \equiv 1 \pmod m$? La resposta és afirmativa, i anem a veure qui pot ser $\phi(m)$. Hem vist que en el cas en què m no és primer, la interpretació de l'exponent com el mòdul menys 1 no és vàlida; però es pot trobar una altra interpretació de l'exponent que si que sigui vàlida. Fixem-nos que si p és primer, els nombres 1, 2, 3,...,$p-1$ són tots primers amb p, per tant $p-1$ és també el nombre de nombres naturals primers amb p i menors que p. Serà aquesta la interpretació vàlida de l'exponent? Tornem al cas $m = 6$. Els nombres primers amb 6 i menors que 6 són 1 i 5, és a dir n'hi ha dos. Calculem $5^2 = 25 \equiv 1 \pmod 6$. És cert!. Proveu-ho per alguns altres nombres i veureu que sempre és cert. Si heu fet el que us he dit de mirar on fallava la demostració, probablement ja us haureu adonat que els nombres que presentaven dificultats eren els menors que m i no primers amb m, per tant la conclusió a la que hem arribat tampoc és estranya. Procedim a enunciar correctament i a demostrar la següent proposició que s'anomena

> **Congruència d'Euler.** Si m és un nombre natural $m > 1$, a és un nombre enter primer amb m, i s'indica per $\phi(m)$ el nombre de nombres naturals primers amb m i menors que m, es compleix:
>
> $$a^{\phi(m)} \equiv 1 \pmod m.$$

Observeu que la congruència de Fermat és un cas particular de la congruència d'Euler.

Demostració. Siguin b_1, b_2,...,$b_{\phi(m)}$ tots els nombres naturals primers amb m i menors que m. Ara només cal seguir el raonament fet a la congruència de Fermat. Aquests nombres són incòngrus dos a dos segons el mòdul m. Com que $\mathrm{mcd}(a,m) = 1$, els nombres $a \cdot b_1$, $a \cdot b_2$,...,$a \cdot b_{\phi(m)}$ seran també incongrus dos a dos i cadascun d'ells congru amb un i només un dels b_1, b_2,...,$b_{\phi(m)}$. Per tant

$$a \cdot b_1 \cdot a \cdot b_2 \cdots a \cdot b_{\phi(m)} \equiv b_1 \cdot b_2 \cdots b_{\phi(m)} \pmod m$$

o sigui

$$a^{\phi(m)}(b_1 \cdot b_2 \cdots b_{\phi(m)}) \equiv b_1 \cdot b_2 \cdots b_{\phi(m)} \pmod m$$

Com que cada b_i és primer amb m és pot simplificar la congruència i s'obté

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

que és el que voliem demostrar.
Ens queda encara una

Quarta pregunta. Com podem calcular el nombre $\phi(m)$ anomenat *indicador* de m? És clar que si m és un nombre primer $\phi(m)$ és $m-1$. El pas següent que sembla natural fer és calcular $\phi(p^a)$ on p és un nombre primer. Els nombres menors que p^a i que són primers amb p^a són els nombres compresos entre 1 i p^a que no són múltiples de p. Com que múltiples de p n'hi ha p^{a-1} d'aquí resulta que

$$\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$$

Si m no és la potència d'un primer podem pensar en descompondre m en factors primers, és a dir $m = p^{a_1} \cdot p^{a_2} \cdots p^{a_n}$, però no sabem com es comporta l'indicador respecte del producte. Com sempre posem-nos un exemple. Volem calcular $\phi(18)$; si contem quants nombres hi ha primers amb 18 i menors que 18 veurem que n'hi ha 6. Posem 18=3.6=2.9; si l'indicador del producte fós igual al producte dels indicadors resultaria $\phi(18)=\phi(3)\,\phi(6)=4$, la qual cosa és falsa. Però en canvi si posem $\phi(18)=\phi(2)\,\phi(9)=6$ i això és cert. Observem que l'indicador del producte no és sempre igual al producte dels indicadors dels factors; ha resultat fals en el cas en què els dos factors tenen un divisor comú, i vertader quan són primers entre si. El que hem observat és cert i podem enunciar la següent proposició que no demostrarem perquè encara no tenim tots els recursos necessaris.

Proposició. Si k i l són dos nombres naturals tals que $\mathrm{mcd}(k,l) = 1$, llavors

$$\phi(k \cdot l) = \phi(k)\phi(l)$$

Aquesta proposició ens diu com hem de calcular $\phi(m)$. Si $m = p^{a_1} \cdot p^{a_2} \cdots p^{a_n}$, com que $\mathrm{mcd}(p_i^{a_i}, p_j^{a_j}) = 1$ per $i,j = 1,2,...,r$, es té la fórmula següent:

$$\phi(m) = p_1^{a_1-1} \cdot p_2^{a_2-1} \cdots p_r^{a_r-1} \cdot (p_1-1) \cdot (p_2-1) \cdots (p_r-1).$$

Encara un parell d'observacions.

1) La congruència d'Euler afirma que si $\text{mcd}(a,m) = 1$ és $a^{\phi(m)} \equiv 1 \pmod{m}$. Però es poden donar casos que per alguns nombres a (que poden ser tots segons quin sigui el mòdul m) existeixin nombres k menor que $\phi(m)$ tals que $a^k \equiv 1 \pmod{m}$. Per exemple per $m = 11$, $\phi(11)$=10 però $3^5 \equiv 1 \pmod{11}$. És clar que k ha de ser sempre un divisor de $\phi(m)$; efectivament 5 divideix 10.

2) Hem de fixar-nos molt bé en el que s'afirma en una proposició. Per exemple algú podria caure en la temptació de pensar que si segons un mòdul m es compleix la congruència de Fermat, aquest mòdul és primer. Això seria un gran error perquè afirmaria la recíproca de la congruència de Fermat. I efectivament no és cert, ja que existeixen nombres compostos que la compleixen, i aquests nombres s'anomenen nombres de Carmichael. El més petit d'ells és $m = 561 = 3 \cdot 11 \cdot 17$, és a dir es compleix que si $\text{mcd}(a, 561) = 1$, $a^{560} \equiv 1 \pmod{561}$.

Problema 15. Proveu que $\sqrt{7}$ no és racional.

Aquest problema és equivalent a demostrar que l'equació $x^2 = 7$ no té cap solució en nombres racionals.

Observeu que n'hi ha prou provant que no té cap solució racional positiva, ja que si un nombre és solució també ho és el seu oposat.

És clar que no en té cap d'entera. Demostrarem que no en té cap de fraccionaria fent la demostració per reducció a l'absurd, que consisteix a suposar que té una solució i veure que s'arriba a una contradicció.

Suposem que $\frac{p}{q}$ és el representant irreductible d'una solució de l'equació $x^2 = 7$, és a dir, $\text{mcd}(p,q) = 1$ i $(\frac{p}{q})^2 = 7$. D'aquí resulta $\frac{p^2}{q^2} = 7$, i $p^2 = 7q^2$. Com que 7 és primer i 7 divideix p^2, també 7 divideix p. Posant $p = 7p'$ resulta $7^2(p')^2 = 7q^2$, i simplificant $7p'^2 = q^2$. Repetint el raonament, com que 7 és primer i divideix q^2, també divideix q, per tant 7 divideix p i q contra l'hipòtesi de ser $\text{mcd}(p,q) = 1$.

Problema 16. Sigui la successió 3, 7, 11, 15,...Demostreu que en aquesta successió hi ha infinits nombres primers.

Aquest problema conté implicitament la afirmació que de nombres primers n'hi ha infinits, i això per ara no ho sabem, ja que podria ocòrrer que a partir d'un nombre endavant tots els nombres naturals fossin compostos. Llavors el nostre problema no tindria sentit. Aquesta pregunta se la van formular els grecs i Euclides en va donar una resposta afirmativa

demostrant per reducció a l'absurd la següent

Proposició. La serie natural conté infinits primers.

La demostració és aquesta. Si només n'hi hagués un nombre finit hi hauria un primer p que seria el més gran. Formem el producte $2\cdot3\cdot5\cdot7\cdot11\cdots p$ de tots els nombres primers i considerem el nombre

$$N = 2\cdot3\cdot5\cdot7\cdot11\cdots p+1$$

Com que N és més gran que 1 o és primer o descompon en producte de factors primers. No pot ser primer perquè tots els primers figuren en el producte $2\cdot3\cdot5\cdot7\cdot11\cdots p$ i N és més gran que aquest producte, per tant més gran qualsevol dels factors. Sigui q un factor primer de N. Com que el producte $2\cdot3\cdot5\cdot7\cdot11\cdots p$ conté tots els nombres primers, q ha de ser un d'ells. Per tant com que q divideix N i divideix $2\cdot3\cdot5\cdot7\cdot11\cdots p$, q divideix 1, i això és una contradicció. D'aquí resulta que ha d'existir un primer q més gran que p i per tant, infinits.

Altres vegades hem anunciat una proposició i hem omès la desmostració, però en aquest cas l'hem feta per veure com ens pot inspirar per resoldre el nostre problema. Observem que la proposició que hem demostrat la podriem enunciar de la forma equivalent:

La progressió aritmètica de terme general $2n+1$ *conté infinits nombres primers.* Per altra part observem que la successió del problema és una progressió aritmètica de primer terme 3 i raó 4 és a dir de terme general $4n-1$, $\quad n=1,2,\ldots.$

Resolució del problema. Procedim com abans per reducció l'absurd, és a dir, suposem que a partir d'un primer endavant tots els primers són de la forma $4n+1$, ja que tot nombre imparell és de una de les dues formes $4n-1$ o $4n+1$. Sigui p el primer més gran de la forma $4n-1$. Seguint la demostració anterior formem un nombre N adequat

$$N = 4\cdot3\cdot5\cdots p-1$$

on el producte $3\cdots(p-1)$ conté tots els primers imparells menors o igual a p. Com que N és de la forma $4n-1$ i és més gran que p no pot ser primer; per tant descompondrà en producte de factors primers. Tot primer que divideix N ha de ser més gran que p, ja que si no dividiria N i el producte $4\cdot3\cdots p-1$ i per tant dividiria 1, la qual cosa és absurda. Com que p és el més gran de la forma $4n-1$, tot primer que divideixi a N ha de ser de la forma $4n+1$ i per tan el seu producte N també de la forma $4n+1$ i això és fals tal com s'ha construït N.

Per tant la progressió aritmètica considerada conté infinits nombres primers.

Observem que en el raonament que acabem de fer hi entra d'una manera molt clara la forma particular de la progressió. Això ja ens fa pensar que potser en alguns altres casos particulars és podran fer raonaments anàlegs, però que en general, per qualsevol progressió aritmètica no.

Considerem per exemple la progressió 5, 8, 11, 14,... és a dir la de terme general $4n+1$, que és la primera que ens salta a la vista. Seguim el raonament anterior i veiem que tot va bé fins que arribem a formar el producte de primers de la forma $4n-1$ ja que el producte d'un nombre parell d'ells és de la forma $4n+1$ i per tant no hi ha contradicció.

Intentem cercar un altre camí de demostració que, per aquest cas, veurem que també el tenim; es tracta de demostrar que donat un nombre natural qualsevol $N > 1$ sempre existeix un primer de la forma $4n+1$ que és més gran que n. Per això utilitzarem la Congruència de Fermat.

Considerem un nombre natural $N > 1$ i formem el nombre imparell

$$m = (N!)^2 + 1$$

Sigui p el factor primer més petit de m, que serà més gran que N ja que tot nombre menor o igual a N divideix $N!$. Com que p divideix $m = (N!)^2 + 1$ serà $(N!)^2 \equiv -1 \pmod{p}$. Elevant els dos membres d'aquesta congruència al quadrat s'obté

$$(N!)^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Com que p no divideix $N!$ per la congruència de Fermat és

$$(N!)^{p-1} \equiv 1 \pmod{p}.$$

Per tant de les dues congruències resulta $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Si $\frac{p-1}{2}$ fos imparell seria $-1 \equiv 1 \pmod{p}$ és a dir $p = 2$ la qual cosa no és possible perquè m és imparell. Per tant $\frac{p-1}{2} = 2n$ és a dir p és de la forma $4n+1$ i per tant pertany a la progressió donada.

Per a algunes altres progressions aritmètiques particulars podríem trobar mètodes com aquests (o encara que un xic més difícils), que sense gaire esforç es poden arribar a entendre. Però queda la pregunta general:

Tota progressió aritmètica conté infinits termes primers? La resposta és afirmativa si en té un. És clar que si el primer terme i la raó de la progressió tenen algun factor comú, la progressió no té cap terme primer. Però pels altres casos és compleix el següent

> **Teorema.** Si $\mathrm{mcd}(a,r)=1$ la progressió aritmètica $a+rn$ $n=1,2,...$ conté infinits nombres primers.

Aquest és un teorema molt important de l'aritmètica, i és de demostració molt difícil. Es necessiten mètodes analítics que van més enllà, però molt més enllà, del que es pot entendre a aquests nivells.

Problema 17. Determineu tots els triangles rectangles de costats enters.
Aquest problema és equivalent al problema aritmètic següent:
Trobeu totes les solucions enteres positives de l'equació

$$X^2+Y^2=Z^2.$$

Observeu en primer lloc que si tenim una solució (X_0,Y_0,Z_0), qualsevol terna $(\lambda X_0,\lambda Y_0,\lambda Z_0)$, on λ és qualsevol nombre enter positiu, serà també solució; i si els tres membres de la terna tenen un divisor comú, s'obtindrà una altra solució dividint-los per aquest divisor comú. Per tant n'hi ha prou a cercar totes les solucions en les que X, Y, Z són primers entre si. Aquestes solucions s'anomenen primitives i a partir d'elles s'obtindran totes les altres multiplicant-les per tots els nombres naturals. També és clar per la forma de l'equació que, si els tres nombres X_0, Y_0, Z_0 són primers entre si, també seran primers entre si dos a dos. Feta aquesta observació, passem a resoldre el problema. Com que Z ha de ser diferent de 0, podem dividir els dos menbres per Z^2 i s'obté l'equació

$$\left(\frac{X}{Z}\right)^2+\left(\frac{Y}{Z}\right)^2=1$$

y posant $\dfrac{X}{Z}=x$, $\dfrac{Y}{Z}=y$ obtenim una equació de la forma

$$x^2+y^2=1$$

que representa una circumferència de centre l'origen de coordenades i radi 1.
Si X, Y, Z són nombres enters $Z\neq 0$, $\dfrac{X}{Z}$, $\dfrac{Y}{Z}$ seran nombres racionals, i per tant a les solucions del nostre problema els correponen punts racionals de la circumferència. Intentem doncs de resoldre aquest altre

Problema. Trobeu tots els punts de coordenades racionals de la circunferència d'equació $x^2 + y^2 = 1$.

Obseveu en primer lloc que el punt $A(-1,0)$ pertany a la circumferència. Escriviu l'equació del feix de rectes que passen per aquest punt $y = t(x+1)$ on t és un paràmetre. Busqueu els punts d'intersecció de les rectes d'aquest feix amb la circumferència, resolent el sistema d'equacions amb les incògnites x, y

$$\left.\begin{array}{l} x^2 + y^2 = 1 \\ y = t(x+1) \end{array}\right\}$$

Es té $x^2 + t^2(x+1)^2 = 1$, o sigui $x^2 - 1 + t^2(x+1)" = 0$ i traient $x+1$ factor comú

$$(x+1)(x - 1 + t^2(x+1)) = 0$$

Una solució es troba fent $x + 1 = 0$, o sigui $x = -1$, que correspon al punt $A(-1,0)$ que pertany a la circumferència i a totes les rectes del feix. L'altra s'obté resolent l'equació $x - 1 + t^2(x+1) = 0$ o sigui $x(1+t^2)^2 = 1 - t^2$ d'on resulta

$$x = \frac{1-t^2}{1+t^2}, \quad y = t(x+1) = t\left(\frac{1-t^2}{1+t^2} + 1\right) = \frac{2t}{1+t^2}$$

A cada valor real de t correspondrà un punt de la circumferència i a cada punt de la circumferència menys $A(-1,0)$ que ja l'haviem trobat abans, un valor real de t.

Si x, y son nombres racionals diferents de -1, $t = \dfrac{y}{x+1}$ serà un nombre racional, y si t és un nombre racional, pels resultats obtinguts x, y seran nombres racionals.

Suposeu t racional i sigui $\dfrac{m}{n}$ el seu representant irreductible. Substituint t per aquest valor a les expressions obtingudes per x, y resulta:

$$x = \frac{n^2 - m^2}{n^2 + m^2}, \quad y = \frac{2mn}{n^2 + n^2}.$$

Donant a m i n tots els parells de valors enters primers entre si obtindreu tots els punts racionals de la circumferència $x^2 + y^2 = 1$ menys el punt $A(-1,0)$.

Tornem al nostre problema:

Com que haviem posat $\dfrac{X}{Z} = x$, $\dfrac{Y}{Z} = y$ serà

$$\frac{X}{Z} = \frac{n^2 - m^2}{n^2 + m^2}, \quad \frac{Y}{Z} = \frac{2mn}{n^2 + m^2}$$

i com que haviem suposat que $\mathrm{mcd}(X,Z) = 1$, $\mathrm{mcd}(Y,Z) = 1$ ha de ser

$$n^2 - m^2 = \lambda X, \quad 2mn = \lambda Y, \quad n^2 + n^2 = \lambda Z$$

per a algun valor enter de λ que cal calcular: λ divideix $n^2 - m^2$ i $n^2 + m^2$ i per tant divideix la seva suma $2n^2$ i la seva diferència $2m^2$, i per tant ha de dividir 2 ja que hem suposat m i n primers entre si. És a dir λ només pot ser 1 o 2. Anem a veure que no pot ser 2.

X, Y no poden ser a la vegada parells ni a la vegada imparells. El primer és clar ja que $\text{mcd}(X, Y) = 1$. Si fossin ambdos imparells, observant que el quadrat d'un nombre imparell és sempre congru amb 1 segons el mòdul 4, seria $X^2 + Y^2 \equiv 2 \pmod 4$ i $Z^2 \equiv 0, 1 \pmod 4$. Per tant o bé X serà parell i Y imparell o al revés, però n'hi ha prou en considerar un dels dos casos ja que l'equació $X^2 + Y^2 = Z^2$ és simètrica respecte les incògnites X, Y. Suposem X parell i $\lambda = 2$. λX seria divisible per 2 però no per 4 i $n^2 - m^2 \equiv 2 \pmod 4$. Però m^2 i n^2 seran o un congru amb 0 i l'altre congru amb 1 segons el mòdul 4 o tots dos seran congrus amb 1 segons el mòdul 4. Per tant λ no pot ser 2; és a dir ha de ser $\lambda = 1$.

Hem arribat així a la solució del problema:

Les longituts dels costats dels triangles rectangles primitius s'obtenen posant

$$X = n^2 - m^2, \quad Y = 2mn, \quad Z = n^2 + m^2$$

i donant a m, n totes les parelles de valors naturals possibles primers entre si.

Problema 18. Trobeu totes les solucions amb nombres naturals de l'equació

$$x^3 + y^3 = 1729.$$

Si mireu un xic detingudament el nombre 1729, observereu sense gran esforç que

$$1729 = 1000 + 729 = 10^3 + 9^3 \quad \text{i també} \quad 1729 = 1 + 1728 = 1^3 + 12^3$$

per tant ja heu obtingut les quatre solucions

$$x = 10, y = 9; \quad x = 9, y = 10; \quad x = 1, y = 12; \quad x = 12, y = 1.$$

Però el problema ens les demana totes. N'hi ha d'altres? Anem a veure que són les úniques. Per això escrivim l'equació proposada d'una altra manera observant que

$$x^3 + y^3 = (x + y)(x^2 - xy + y^2) \quad \text{i que} \quad 1729 = 7 \cdot 13 \cdot 19.$$

$$\text{i per tant} \qquad (x + y)(x^2 - xy + y^2) = 7 \cdot 13 \cdot 17.$$

Ara es tracta d'igualar de totes les maneres possibles els factors del primer membre amb factors del segon membre, però per evitar-nos feina farem un raonament més general. Posem

$$\left.\begin{array}{c} x+y=a \\ x^2-xy+y^2=b \end{array}\right\} \quad \text{amb} \quad ab = 1729 = 7.13.19$$

Resolem el sistema d'equacions aïllant x a la primera i substituint a la segona; després de fer operacions arribem a l'equació de segon grau

$$3x^2 - 3ax + a^2 - b = 0.$$

Per tant

$$x = \frac{3a \pm \sqrt{12b - 3a^2}}{6}$$

Mirem totes les condicions que han de satisfer a i b. Recordem que $a \cdot b = 7 \cdot 13 \cdot 19$; a més a més ha de ser $a > 1$, $12b - 3a^2 \geq 0$ i quadrat d'un nombre enter. Amb aquestes condicions veureu tot seguit que els únics valors de a i b són $a = 13$, $b = 7 \cdot 19$; $a = 19$, $b = 7 \cdot 13$; a aquests valors corresponen els valors de x, y que haviem obtingut al principi. Per tant aquelles són les úniques solucions

Problemes

AR1.–Proveu que si els tres costats d'un triangle rectangle vénen expressats per tres nombres naturals en progressió aritmètica llavors el seu perímetre és múltiple de 12.

AR2.–Els tres nombres naturals $1652_{(n}$, $2012_{(n}$, $2042_{(n}$ (escrits en base n) estan en progressió aritmètica. Determineu la base n de numeració i la raó de la progressió.

AR3.–Un nombre de tres xifres en base 10 s'escriu xyz en el sistema de base 7 i zyx en el sistema de base 9. Determineu aquest nombre escrit en base 10.

AR4.–Proveu que l'única parella d'enters positius (a, b) per a la qual la suma coincideix amb el producte és la $(2, 2)$.

AR5.–Proveu que només hi ha una parella d'enters positius (a, b) tal que $a^b = b^a$ i trobeu-la.

AR6.–Resoleu en el conjunt dels nombres naturals l'equació

$$\frac{x}{2} + \frac{y}{4} + \frac{z}{16} = 1.4375 \, .$$

AR7.–En un nombre de tres xifres, la suma d'elles és 15, la xifra de les unitats és doble de la de les desenes, i la diferència entre el nombre i el que resulta d'invertir les xifres és 297. Determineu aquest nombre.
Discutiu el problema en el cas general, és a dir si la suma de les xifres és s i la diferència que s'obté en invertir l'ordre de les seves xifres és d.

AR8.–Trobeu els valors naturals de x per als quals $x^2 + 5x + 160$ és un quadrat perfecte.

AR9.–Determineu 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.

AR10.–Un nombre té 216 divisors, el seu doble té 270 divisors, la seva tercera part té 180 divisors i la seva cinquena part té 144 divisors. Trobeu aquest nombre amb la condició que sigui el més petit possible.

AR11.–Trobeu un nombre de quatre xifres, quadrat perfecte, sabent que la suma de les seves xifres és igual a la suma de les xifres de la seva arrel quadrada. Determineu totes les solucions.

AR12.–Demostreu que per a tot valor natural de n,

$$3^{2n+2} + 2^{6n+1}$$

és múltiple de 11.

AR13.–Una pila de boles de base rectangular té a la base $m \cdot n$ boles i les altres capes es formen col·locant una bola en el forat que deixen les quatre boles de la capa anterior, i així successivament fins que s'arriba a una capa formada per una sola fila. Calculeu quantes boles té la pila sabent que m és el nombre de diagonals que té un decàgon i n és el menor nombre que dividit per 4 dóna residu 3, dividit per 5 dóna residu 4 i dividit per 6 dóna residu 5.

AR14.–Determineu en quants zeros acaba 1000!

AR15.–Proveu que $\pi(n) \geq \frac{\log n}{log4}$, on $\pi(n)$ és el nombre de primers que no sobrepassen el nombre natural n. (*Teorema de* Wacław Sierpinski).

AR16.–Determineu x, y i z per tal que el nombre $33xy49z$ (escrit en base 10) sigui múltiple de 693.

AR17.–Calculeu dos nombres de la forma aa, $bbcc$ tals que

$$aa = \sqrt{bbcc}.$$

AR18.–Calculeu l'enter més petit x pel qual $x^2 + x + 41$ és compost.

AR19.–Demostreu que si dos nombres enters són de la mateixa paritat, la meitat de la suma dels seus quadrats és una suma de dos quadrats.

AR20.–a) Trobeu tots els enters positius n tals que $2^n - 1$ és divisible per 7.

b) Demostreu que no existeix cap enter positiu tal que $2^n + 1$ és divisible per 7.

AR21.–Demostreu que si $2^n - 1$ és primer, llavors n és primer.

AR22.–Demostreu

a) Per tot n existeixen n nombres consecutius compostos.

b) Per tot n existeixen n nombres consecutius tals que cap d'ells és la potència d'un primer.

AR23.–Determineu quina condició han de complir les xifres de les desenes de dos nombres acabats en 6 per tal que el seu producte acabi en 36.

AR24.–Trobeu els nombres de quatre xifres que són iguals al quadrat de la suma del nombre format per les dues primeres xifres i el format per les dues darreres xifres.

AR25.–Proveu que $2^{2^n} + 2^{2^{n-1}} + 1$ no pot ser expressat com a producte de menys de n primers (no necessàriament diferents).

AR26.–El nombre natural

$$3^n + 2 \cdot 17^n$$

no és quadrat perfecte per cap natural n.

AR27.–La suma dels dígits de $N = 4444^{4444}$ (escrit en notació decimal) és A. La suma dels dígits de A és B i la suma dels dígits de B és C. Calculeu C.

AR28.–Siguin n, m nombres naturals qualssevol. Demostreu que

$$\frac{(2m)!\,(2n)!}{m!\,n!\,(m+n)!}$$

és un enter.

AR29.–Demostreu que si a i b són enters positius, llavors, si

$$\frac{a^2 + b^2}{ab + 1}$$

és un enter, és un quadrat perfecte.

AR30.–Un nombre natural és perfecte si és igual a la suma dels seus divisors menors que ell. Demostreu que si $2^n - 1$ és primer llavors $2^{n-1}(2^n - 1)$ és perfecte.

AR31.–Proveu que si p és un nombre primer diferent de 2 i 5, p divideix infinits termes de la successió 9, 99, 999, 9999,...Proveu el mateix per la successió 1, 11, 111, 1111,...

AR32.–Proveu que $n^2 + 3n + 5$ no és mai divisible per 121.

AR33.–Proveu que $2222^{5555} + 5555^{2222}$ és divisible per 7.

AR34.–Proveu que si tots els coeficients de l'equació $ax^2 + bx + c = 0$ són imparells, les arrels d'aquesta equació no poden ser racionals.

AR35.–Proveu que tots els nombres de la forma 10001, 100010001, 1000100010001,...són compostos.

AR36.–Trobeu totes les solucions en nombres enters de l'equació

$$x^2y^2 = 5x^2y + 20x + 16.$$

AR37.–Si $T_0 = 2$, $T_{n+1} = {T_n}^2 - T_n + 1$, proveu que $\text{mcd}(T_n, T_m) = 1$, $m \neq n$.

AR38.–Proveu que $1^{1983} + 2^{1983} + \cdots + 1986^{1983} \equiv 0 \pmod{1987}$.

AR39.–Si a, b, x, y són nombres naturals, $\text{mcd}(a, b) = 1$ i $x^a = y^b$, proveu que existeix un nombre natural n tal que $x = n^b$, $y = n^a$.

AR40.–Trobeu totes les solucions en nombres naturals del sistema d'equacions

$$\left.\begin{array}{c} a^3 - b^3 - c^3 = 3abc \\ a^2 = 2(b + c) \end{array}\right\}$$

AR41.–Proveu que l'equació $x^2 + y^2 = 3z^2$ només té en nombres enters la solució $x = 0$, $y = 0$, $z = 0$. Com a conseqüència proveu que la circumferència $x^2 + y^2 = 3$ no té cap punt de coordenades racionals.

AR42.–Trobeu tots els punts de coordenades racionals de la circumferència $x^2 + y^2 = 2$.

AR43.–Trobeu totes les solucions amb nombres enters de l'equació $x^3 + y^3 = 793$.

AR44.–Proveu que si p és un nombre primer imparell, l'equació $x^3 + y^3 = p$ o bé no té cap solució en nombres enters, o bé p és de la forma $3n^2 + 3n + 1$.

Mostra de solucions

Solució del problema AR4

La condició $ab = a + b$ es pot escriure $(a-1)(b-1) = 1$ que només té les solucions enteres $a-1 = 1, b-1 = 1$ o bé $a-1 = -1, b-1 = -1$. La segona parella queda exclosa perquè dóna $a = 0, b = 0$. La primera dóna $a = 2, b = 2$.

Si a, b fossin racionals (o reals), l'equació tindria una infinitat de solucions

$$a = \frac{b}{b-1}$$

on b és un racional (real) arbitrari diferent de 1.

Solució del problema AR5

Suposem $a^b = b^a$ amb $1 < a < b$ enters positius. Podem escriure $b = a + n$ amb $n \geq 1$ i queda $b^a = a^b = a^{a+n} = a^a a^n$ d'on surt $a^n = (b/a)^a$. Si fem $\lambda = b/a > 1$ queda $b = \lambda a$ i $n = b - a = a(\lambda - 1)$. Substituint, $a^{a(\lambda-1)} = \lambda^a$ o bé $a^{\lambda-1} = \lambda$, d'on, fent $a = 1 + k$, queda $\lambda = (1+k)^{\lambda-1}$ o bé

$$(\lambda - 1)(k-1) + \binom{\lambda-1}{2} k^2 + \cdots + \binom{\lambda-1}{\lambda-1} k^{\lambda-1} = 0.$$

En ser tots els termes no negatius, només s'anul·la l'expressió si tots són nuls. Tenim, doncs, que ha de ser $k = 1$ o bé $\lambda = 1$. Aquest darrer cas ens dóna el cas trivial $a = b$. Si $k = 1$ queda $a = 2$ i $2^{\lambda-1} = \lambda$ que només es compleix per $\lambda = 2$, d'on $b = 4$.

Si suposem que a i b són racionals amb $b > a$ podem posar

$$\frac{b}{a} = 1 + \frac{p}{q}$$

i la igualtat $a^b = b^a$ queda $a^{a(1+\frac{p}{q})} = \left(a(1+\frac{p}{q})\right)^a$ i susbstituint dóna lloc a

$$a = \left(1 + \frac{p}{q}\right)^{\frac{q}{p}} \quad b = \left(1 + \frac{p}{q}\right)^{\frac{p+q}{p}}.$$

Per tal que a i b siguin racionals cal que tant q com $p+q$ siguin, simultàniament, arrels p-èsimes exactes. Però això és impossible si $p \neq 1$. En efecte, si q no és arrel exacta, ja hem acabat. Si ho és, serà $q = r^p$, $r > 1$. Queda

$$(r+1)^p = r^p + pr^{p-1} + \frac{p(p-1)}{2} r^{p-2} + \cdots,$$

i com que $r^p = q$, $pr^{p-1} > p$ i els altres termes són no negatius, queda $(r+1)^p > p+q$, de forma que $p+q$ queda entre dues potències consecutives d'exponent p i no pot ser potència entera exacta. En conclusió, $p = 1$ i finalment

$$a = \left(1 + \frac{1}{q}\right)^q \quad b = \left(1 + \frac{1}{q}\right)^{q+1}.$$

Una simple comprovació demostra que aquests nombres compleixen l'equació.

Solució del problema AR15

Siguin $2, 3, \ldots, p_{\pi(n)}$ els nombres primers que són més petits o iguals que n. Qualsevol natural $m \leq n$ el podrem escriure en la forma

$$m = m_1^2 \cdot 2^{a_1} \cdot 3^{a_2} \cdots p_{\pi(n)}^{a_{\pi(n)}}$$

on els a_i només poden prendre valors 0,1. Si donem valors 0,1 de totes les maneres possibles als a_i obtindrem tots els nombres més petits o iguals a n que són *lliures de quadrats*; el nombre total obtingut serà $2^{\pi(n)}$. Com que $m_1^2 \leq m \leq n$, serà $m_1 \leq \sqrt{m} \leq \sqrt{n}$. Si volem obtenir tots els nombres menors o iguals a n haurem de multiplicar els $2^{\pi(n)}$ lliures de quadrats per tots els m_1 que compleixin la condició $m_1 \leq \sqrt{n}$. Per tant, el nombre total de nombres més petits o iguals que n , que és n, ha de complir $n \leq \sqrt{n}\, 2^{\pi(n)}$. Fent operacions queda $\sqrt{n} \leq 2^{\pi(n)}$ o bé, prenent logaritmes, $\log n \leq \pi(n) \log 4$, i d'aquí el resultat.

Observació: Com que el logaritme tendeix a infinit, deduïm que $\pi(n)$ també ho fa, i demostrem altra vegada la infinitud dels primers. Però la fita inferior de l'enunciat és molt poc fina: per exemple, $\pi(1000) = 168$ i $\log 1000/\log 4 = 4.983$.

Solució del problema AR25

Usarem la igualtat $2^{2^n} = \left(2^{2^{n-1}}\right)^2$ i la identitat $(x^2+x+1)(x^2-x+1) = x^4+x^2+1$. Procedirem per inducció sobre n. Per a $n=1$ no hi ha res a demostrar. Suposant-ho cert per a n, tenim

$$2^{2^{n+1}} + 2^{2^n} + 1 = \left(2^{2^n} + 2^{2^{n-1}} + 1\right)\left(2^{2^n} - 2^{2^{n-1}} + 1\right)$$

i com que el primer factor s'expressa, per hipòtesi d'inducció, com a producte de n primers com a mínim, i el segon en té un com a mínim, resulta que en total n'hi ha $n+1$ com a mínim.