pàgines, introdueix de manera entenedora la probabilitat condicional, els esdeveniments independents, el teorema de Bayes i la «paradoxa dels aniversaris».

Els capítols 6, 7, 8 i 9 conformen una unitat dedicada als sistemes de clau pública. Els capítols 6 i 8 analitzen la dificultat de factoritzar un enter extremadament gran. Hi apareixen els patològics nombres de Carmichael i els tests de Fermat i Miller-Rabin, que ens permeten afirmar, amb probabilitat alta, que un enter donat és primer. Els capítols 7 i 9 estan dedicats a la descripció dels dos sistemes de clau pública més importants: RSA i ElGamal. I també a la del protocol d'intercanvi de claus de Diffie-Hellman. De tots aquests algorismes, se n'avalua la seguretat i se'n compara l'eficiència. Aquí l'autor també juga fort i ens trobem amb aquesta perla: «it may very well be that someone already knows an efficient factoring algorithm and that RSA is insecure.»

Els capítols 10 i 11 introdueixen les funcions de compressió, la necessitat d'evitar la suplantació de personalitat mitjançant la signatura electrònica, i la implementació de l'algorisme DSA de signatura digital.

Finalment, s'agraeix especialment el contingut dels capítols 12, 13 i 14, que tracten, encara que breument, temes que habitualment es deixen de banda en els textos clàssics de criptografia elemental: construcció de grups finits en els quals és difícil resoldre el problema del logaritme discret, identificació i gestió de *passwords*, autoritats certificadores.

Cada capítol consta d'una extensa llista de problemes de tota mena: fàcils, difícils, divertits, de programació, purament matemàtics. La meitat dels exercicis proposats estan resolts en un apèndix final.

David Juher
Universitat de Girona

Problemes

Abans de parlar dels problemes, permeteu-me que em presenti. Sóc en Carles Romero, i, a partir d'aquest número del *Notícies*, em faig càrrec d'aquesta secció. He rebut tots els protocols, arxius i benediccions d'en Pelegrí Viader, qui se n'encarregava fins ara, i em llenço a l'aventura de seguir oferint-vos aquestes racions de *tapes*, que, espero, trobareu prou saboroses.

Bé, parlem de problemes de matemàtiques: del problema A46, no n'hem rebut cap solució. Un acostament naïf porta a quatre pesades com a mínim, però no és gaire arriscat sospitar (i el proposant ho creu) que es pot fer en tres. Així doncs, el tornem a proposar tot animant-vos a rerumiar-lo.

I, com ja es feia abans, preguem als nostres lectors que, si fan servir TEX o LATEX per escriure les seves solucions, les enviïn per correu electrònic a: (cromero@pie.xtec.es) així com qualsevol proposta o suggeriment. (Sí, és clar, *abans* s'enviava a *una altra* adreça!)

Problemes proposats

A46. (Proposat per Jordi Ramoneda, Valldoreix.) Tenim 12 boles iguals i indistingibles en tot llevat del pes, ja que una d'aquestes pesa diferent de les altres, no sabem si més o menys. Disposem d'una balança de dos plats. Quin és el mínim nombre de pesades que ens cal fer per tal de trobar la bola diferent?

A50. (Proposat per Pelegrí Viader, UPF.) Inspirat en l'article de G. Polya «On the Harmonic Mean of Two Numbers», *The American Mathematical Monthly*, vol. 57, núm. 1, gener 1950, p. 26–28.) En Joan fa la següent juguesca amb la Joana: «tria un nombre real qualsevol entre 9 i 11 (extrems inclosos); si t'equivoques en més del 10%

del que hi ha escrit en aquest paper que jo no he vist, em pagues un cafè. Si no, te'l pago jo». La Joana, que és una excel·lent alumna de matemàtiques, s'ho pensa una mica, fa uns quants càlculs i li diu un nombre al Joan. Aquest, sense ni tan sols consultar el paper, li paga el cafè. Quin número havia triat la Joana?

A51. (De *Teaching Mathematics and its Applications*, vol. 12, núm. 1, 1993, p. 45.) És ben conegut que, per tal de generar solucions enteres de $a^2+b^2=c^2$, cal prendre p i q enters qualssevol i fer $a=p^2-q^2$, $b=2pq$ i $c=p^2+q^2$. Hi ha algun mecanisme similar per tal de generar solucions enteres de $a^2+b^2=c^3$?

A52. («59th Annual William Lowell Putnam Mathematical Competition») Sigui s un arc qualsevol del cercle unitat, situat tot ell al primer quadrant. Siguin A l'àrea de la regió trapezoidal compresa entre l'arc i l'eix "x" i B l'àrea de la regió trapezoidal compresa entre l'arc i l'eix "y". Demostreu que $A+B$ només depèn de la longitud de l'arc s i no de la seva posició.

Solucions

Problemes proposats a SCM/Notícies 15

A47. (Proposat per Edgar Güeto, UPC.) Proveu que, per qualssevol $p,n\in\mathbb{N}$,

$$\frac{p^{2\cdot 5^n}+p^{5^n}+1}{p^2+p+1}\in\mathbb{N}\,.$$

Solució: (Esteve Casas, Sant Celoni.) Si considerem el numerador i el denominador com a polinomis (com si p fos una variable), la idea serà demostrar que el numerador és múltiple del denominador i, per tant, que l'expressió és, en realitat, un element de $\mathbb{Z}[p]$. A partir d'aquí, la conclusió és òbvia.

Les arrels de $p^2+p+1=\dfrac{p^3-1}{p-1}$ són les arrels cúbiques de la unitat diferents de 1. Anomenem-les ξ i $\xi^2=\xi^{-1}$.

Si analitzem $5^n\equiv\ \pmod 3$ podem veure que, en ser $5\equiv -1\pmod 3$, resulta $5^n\equiv\pm 1\pmod 3$.

Si, per exemple, $5^n\equiv -1\pmod 3$, aleshores

$$\xi^{2\cdot 5^n}+\xi^{5^n}+1=\xi+\xi^{-1}+1=0\,.$$

De manera similar es tractaria el cas $5^n\equiv 1\pmod 3$.

Les dues arrels del polinomi del denominador les té el polinomi del numerador, la qual cosa ens permet afirmar que:

$$\frac{p^{2\cdot 5^n}+p^{5^n}+1}{p^2+p+1}=P(p)\in\mathbb{Q}[p]\,.$$

Ara només ens cal demostrar que, de fet, $P(p)\in\mathbb{Z}[p]$, la qual cosa és directa ja que, si descomponem $p^{2\cdot 5^n}+p^{5^n}+1$ en factors de primer grau i traiem els factors conjugats $(x-\xi)$ i $(x-\xi^{-1})$, la qual cosa equival a dividir per p^2+p+1, obtenim un polinomi a coeficients enters.

De fet, és una propietat coneguda que si tenim un polinomi mònic de coeficients enters expressat com a producte d'altres dos, aquests també hauran de ser de coeficients enters.

Solució del proposant. Per divisió directa veiem que $p^{10}+p^5+1$ és divisible per p^2+p+1 i resulta $p^8-p^7+p^5-p^4+p^3-p+1$. Fixem p i definim $a(p)=p^2+p+1$ i $v(n)=a(p^{5^n})$. Llavors considerem $u(n)=v(n+1)/v(n)$. Tenim

$$u(n)=\frac{v(n+1)}{v(n)}=\frac{v(n+1)}{v(n-1)}\cdot\frac{v(n-1)}{v(n)}=$$
$$=\frac{v(n+1)}{v(n-1)}\cdot\frac{1}{u(n-1)}\,.$$

Repetint els càlculs, arribem a

$$u(n)=\frac{v(n+1)}{v(0)}\cdot\frac{1}{u(n-1)}\cdot\frac{1}{u(n-2)}\cdots\frac{1}{u(0)}\,.$$

Per tant, fent les substitucions pertinents,

$$\frac{p^{2\cdot 5^{n+1}}+p^{5^{n+1}}+1}{p^2+p+1}=$$
$$=u(n)\cdot u(n-1)\cdots u(1)\cdot u(0)\,. \qquad (*)$$

Ara bé, hem vist que $a(p^5)/a(p)\in\mathbb{N},\ \forall p\in\mathbb{N}$, és a dir, $a(p^{5^{n+1}})/a(p^{5^n})\in\mathbb{N},\ \forall n,p\in\mathbb{N}$ i, per tant, $u(n)=v(n+1)/v(n)\in\mathbb{N}\forall n\in\mathbb{N}$. Llavors veiem que l'expressió $(*)$ és un nombre natural per qualssevol n i p naturals.

A48.(Proposat per Edgar Güeto, UPC.) Considereu la seqüència $4, 6, 9, 10, 14, 15, 21, 22, 25, 26, \ldots$ Proveu que no hi ha quatre termes de la sèrie que siguin naturals consecutius.

Solució: (Esteve Casas, Sant Celoni.) La primera cosa que cal notar és que la successió és estrictament creixent i formada per **tots** els enters que són productes de dos primers, no necessàriament diferents.

Vegem-ho: $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $9 = 3 \cdot 3$, $10 = 5 \cdot 2$, $14 = 2 \cdot 7$, etc. i entremig no ens en deixem cap amb aquestes característiques. Si continuéssim els termes de la successió, els tres següents serien $11 \cdot 3 = 33$, $17 \cdot 2 = 34$ i $7 \cdot 5 = 35$ (de passada veiem que hi pot haver tres naturals consecutius i que la quantitat demanada en el problema és mínima).

Fets aquests aclariments, ens adonarem que, si hi hagués quatre naturals consecutius en la nostra successió, dos serien parells i de la manera $2p$ i $2q$, amb p i q primers i, si suposem que $2p < 2q$, aleshores tindríem $2p + 2 = 2q$ i, per tant, que $p + 1 = q$, la qual cosa és impossible ja que, tant p com q han de ser senars (si no, $p = 2$ i $q = 3$, que tampoc compleixen els requisits).

Solució del proposant. És clar que hem de començar per veure quina llei segueixen els nombres de la sèrie. Si experimentem una mica, veurem que no és ni aritmètica ni geomètrica. No hi ha un mètode general que ens permeti trobar la llei de formació d'una seqüència de naturals, així que, senzillament, ens haurem d'adonar que els nombres de la sèrie són els que són producte de dos primers (iguals o diferents). Podríem dir que són els nombres de grau 2 (perquè la suma dels exponents dels primers de la descomposició en factors primers sumen 2).

Suposem, doncs, que hi ha quatre termes de la sèrie que són naturals consecutius. Llavors, i aquest és el fet clau, n'hi ha un que és divisible per 4. Ara bé, 4 és un nombre de grau 2, per tant, el nombre que és múltiple de quatre ha de ser precisament 4, ja que altrament seria de major grau i no seria a la sèrie. Això significa que el 3 o el 5 han de ser a la sèrie, però cap dels dos no hi pertany. Per tant, no pot haver quatre termes de la sèrie que siguin naturals consecutius.

B49. (Proposat per José Luís Díaz, UPC, Terrassa.) Donats els nombres $a, b, c \in \mathbb{C}$ tots diferents i no nuls, proveu que

$$\frac{2a+b+c}{a(a-b)(a-c)} + \frac{a+2b+c}{b(b-a)(b-c)} + \\ + \frac{a+b+2c}{c(c-a)(c-b)} = \frac{1}{ab} + \frac{1}{bc} + \frac{1}{ca}\,.$$

Solució: (Esteve Casas, Sant Celoni.) Anem a pams:

$$\frac{2a+b+c}{a(a-b)(a-c)} + \frac{a+2b+c}{b(b-a)(b-c)} + \\ + \frac{a+b+2c}{c(c-a)(c-b)} = \\ = \frac{1}{(a-b)(a-c)} + \frac{1}{(b-a)(b-c)} + \\ + \frac{1}{(c-a)(c-b)} + \left(\frac{a+b+c}{a(a-b)(a-c)} + \right. \\ \left. + \frac{a+b+c}{b(b-a)(b-c)} + \frac{a+b+c}{c(c-a)(c-b)} \right)\,.$$

Analitzem en primer lloc el fragment

$$\frac{1}{(a-b)(a-c)} + \frac{1}{(b-a)(b-c)} + \\ + \frac{1}{(c-a)(c-b)} = 0$$

per tal de veure que val zero. En efecte, si sumem els dos primers sumands obtindrem el tercer canviat de signe. Vegem-ho:

$$\frac{1}{(a-b)(a-c)} + \frac{1}{(b-a)(b-c)} = \\ = \frac{(b-c)-(a-c)}{(a-b)(a-c)(b-c)} = \frac{-1}{(c-a)(c-b)}\,.$$

Passem ara a estudiar el factor que ens queda, analitzant-ne en primer lloc el terme:

$$\frac{1}{a(a-b)(a-c)} + \frac{1}{b(b-a)(b-c)} + \\ + \frac{1}{c(c-a)(c-b)} = \\ = \frac{b^2-a^2-bc+ac}{ab(a-b)(a-c)(b-c)} + \frac{1}{c(c-a)(c-b)} = \\ = \frac{(b-a)(a+b)+c(a-b)}{ab(a-b)(a-c)(b-c)} + \frac{1}{c(c-a)(c-b)} = \\ = \frac{-a-b+c}{ab(a-c)(b-c)} + \frac{1}{c(c-a)(c-b)} =$$

$$= \frac{c(c-a-b)+ab}{abc(a-c)(b-c)} = \frac{c^2-ac-cb+ab}{abc(a-c)(b-c)} =$$
$$= \frac{a(b-c)+c(c-b)}{abc(a-c)(b-c)} = \frac{(b-c)(a-c)}{abc(a-c)(b-c)} =$$
$$= \frac{1}{abc}\,.$$

Si ara multipliquem pel terme $(a+b+c)$ obtenim

$$\frac{a+b+c}{abc}$$

i, en separar en tres termes i simplificar cada fracció, ens dóna el resultat buscat

$$\frac{1}{ab}+\frac{1}{bc}+\frac{1}{ca}\,.$$

Solució del proposant. És ben conegut en la teoria de les diferències finites [∗] que

$$f(z_0,z_1,\ldots,z_n) = \sum_{j=0}^{n} f(z_j) \prod_{\substack{k=0\\k\neq j}}^{n} \frac{1}{z_j-z_k}\,. \quad (*)$$

En aplicar el resultat anterior a la funció $f(z) = 1+\dfrac{a+b+c}{z}$, el primer membre de l'equació $(*)$ és igual a

$$f(a,b,c) = \frac{f(b,c)-f(a,b)}{c-a} =$$
$$= \frac{1}{c-a}\left(\frac{a+b+c}{ab} - \frac{a+b+c}{bc}\right) =$$
$$= \frac{a+b+c}{abc} = \frac{1}{ab}+\frac{1}{bc}+\frac{1}{ca}\,.$$

D'altra banda, el segon membre de (*) és

$$\frac{f(a)}{(a-b)(a-c)} + \frac{f(b)}{(b-a)(b-c)} + \frac{f(c)}{(c-a)(c-b)} =$$
$$= \frac{2a+b+c}{a(a-b)(a-c)} + \frac{a+2b+c}{b(b-a)(b-c)} + \frac{a+b+2c}{c(c-a)(c-b)}$$

i la identitat queda provada.

[∗] E. Isaacson, H. B. Keller, *Analysis of Numerical Methods*, Dover, 1994, p. 247.

Carles Romero
IES Manuel Blancafort, la Garriga

Tesis

- Maria Alberich i Carramiñana va llegir la seva tesi, dirigida per Eduard Casas Alvero, titulada *Geometria de les transformacions biracionals del pla*, el dia 31 de gener de 2000. La tesi correspon al Departament d'Àlgebra i Geometria de la Universitat de Barcelona.

A una transformació biracional del pla (també coneguda amb el nom de *transformació de Cremona del pla*) $f\colon P \to P'$, se li associa el sistema lineal (xarxa), sense part fixa, H en el pla P que és la imatge inversa de la xarxa de rectes en P'. La xarxa H determina la transformació f llevat d'una projectivitat de P'. Aleshores un punt x de P és fonamental per f (és a dir, x pertany al subconjunt tancat de P on f no es pot definir com a morfisme) si, i només si, x és un punt base de la xarxa H. Es considera el conjunt dels punts base de H: no tan sols els punts fonamentals de f, que són punts propis en el pla P, sinó també els punts base infinitament propers, que són punts propis en una superfície obtinguda a partir del pla per successives explosions de punts. Els punts base formen un clúster ponderat $K = (K, m)$, on K són els punts base de H i m assigna a cada punt p de K la multiplicitat en p de corbes genèriques de H. Aquesta tesi estudia les transformacions de Cremona del pla des del punt de vista de la geometria dels seus clústers ponderats de punts base.

En primer lloc, s'han revisat els resultats clàssics, que només estaven ben establerts per al cas en què els punts base de la transformació directa i inversa són propis, i s'han estès a una transformació arbitrària. En aquest sentit