

que és el que volíem 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. Repasseu-la a veure si ho trobeu. Podríem 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 $\text{mcd}(a, m) = 1$ 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 sí que sigui vàlida. Fixem-nos que si p és primer, els nombres $1, 2, 3, \dots, p-1$ 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 $b_1, b_2, \dots, b_{\phi(m)}$ 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 incongrus dos a dos segons el mòdul m . Com que $\text{mcd}(a, m) = 1$, els nombres $a \cdot b_1, a \cdot b_2, \dots, a \cdot b_{\phi(m)}$ seran també incongrus dos a dos i cadascun d'ells congru amb un i només un dels $b_1, b_2, \dots, b_{\phi(m)}$. 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 volíem 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 $18 = 3 \cdot 6 = 2 \cdot 9$; si l'indicador del producte fos 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 $\text{mcd}(k, l) = 1$, 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 $\text{mcd}(p_i^{a_i}, p_j^{a_j}) = 1$ per $i, j = 1, 2, \dots, r$, 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 fraccionària 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 $\left(\frac{p}{q}\right)^2 = 7$. 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 implícitament la afirmació que de nombres primers n'hi ha infinits, i això per ara no ho sabem, ja que podria ocórrer 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 sèrie 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 $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p$ de tots els nombres primers i considerem el nombre

$$N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p + 1$$

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 $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p$ 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 $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p$ conté tots els nombres primers, q ha de ser un d'ells. Per tant com que q divideix N i divideix $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p$, 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 enunciat una proposició i hem omès la demostració, 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 podríem 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 $4n - 1$, $n = 1, 2, \dots$

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

$$N = 4 \cdot 3 \cdot 5 \cdots p - 1$$

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 $4 \cdot 3 \cdots p - 1$ 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 $\text{mcd}(a, r) = 1$ la progressió aritmètica $a + rn$ $n = 1, 2, \dots$ 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 membres per Z^2 i s'obté l'equació

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

y posant $\frac{X}{Z} = x$, $\frac{Y}{Z} = y$ 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 $Z \neq 0$, $\frac{X}{Z}$, $\frac{Y}{Z}$ seran nombres racionals, i per tant a les solucions del nostre problema els corresponen punts racionals de la circumferència. Intentem doncs de resoldre aquest altre

Problema 18. Trobeu tots els punts de coordenades racionals de la circumferència d'equació $x^2 + y^2 = 1$.

Observeu 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 $x^2 - 1 + t^2(x + 1)^2 = 0$ 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 $x(1 + t^2) = 1 - t^2$ 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'havíem trobat abans, un valor real de t .

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

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

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

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 havíem posat $\frac{X}{Z} = x$, $\frac{Y}{Z} = y$ 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 havíem suposat que $\text{mcd}(X, Z) = 1$, $\text{mcd}(Y, Z) = 1$ ha de ser

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

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 ambdós 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 longituds 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 19. Trobeu totes les solucions amb nombres naturals de l'equació

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

Si mireu un xic detingudament el nombre 1729, observareu 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

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

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

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

$$\left. \begin{array}{l} x + y = a \\ x^2 - xy + y^2 = b \end{array} \right\} \quad \text{amb} \quad ab = 1729 = 7 \cdot 13 \cdot 19$$

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 havíem 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.

Aritmètica

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 desenes és doble de la de les unitats, i la diferència entre el nombre i el que resulta d'invertir les xifres és 297. Determineu aquest nombre.

Discuti 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 $\pi(n) \geq \frac{\log n}{\log 4}$, 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.

Aritmètica

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 $1^{1983} + 2^{1983} + \dots + 1986^{1983} \equiv 0 \pmod{1987}$.

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

$$\begin{cases} a^3 - b^3 - c^3 = 3abc \\ a^2 = 2(b + c) \end{cases}$$

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

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

En ser tots els termes no negatius, només s'anulla 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 $a^{a(1+\frac{p}{q})} = (a(1+\frac{p}{q}))^a$ i substituint 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

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

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 $2, 3, \dots, p_{\pi(n)}$ 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 $2^{2^n} = (2^{2^{n-1}})^2$ 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

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

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.

ANÀLISI COMBINATÒRIA

Josep Pla i Carrera

Dos principis bàsics de càlcul d'elements de conjunts

El principi additiu [PA]

Suposem que dues experiències excloents E_1 i E_2 tenen respectivament n_1 i n_2 resultats possibles. L'experiència $E_1 \oplus E_2$ que consisteix en el fet que s'hagi produït una d'ambdues experiències té $n_1 + n_2$ resultats possibles.

En termes conjuntistes diríem: tenim dos conjunts disjunts finits A_1 , A_2 , on $A_1 \cap A_2 = \emptyset$. Es tracta de calcular la quantitat d'elements —el *cardinal*— del conjunt $A_1 \cup A_2$, en el supòsit que coneixem els cardinals dels conjunts A_1 i A_2 . El PA estableix que

$$|A_1 \cup A_2| = |A_1| + |A_2|, \text{ sempre que } A_1 \cap A_2 = \emptyset.$$

El principi multiplicatiu [PM]

Suposem que dues experiències E_1 i E_2 tenen, respectivament, n_1 i n_2 resultats possibles. Considerem l'experiència E formada per totes les *parelles ordenades* de resultats de les experiències E_1, E_2 . L'experiència E consta de $n_1 \times n_2$ resultats possibles.

En termes conjuntistes diríem: tenim dos conjunts finits A_1 i A_2 tals que $|A_1| = n_1$, $|A_2| = n_2$. Considerem el *producte cartesià*

$$A_1 \times A_2 = \{(a_1, a_2) : a_1 \in A_1, a_2 \in A_2\}$$

dels conjunts A_1 i A_2 . El PM estableix que $|A_1 \times A_2| = n_1 \times n_2$.

Un principi bàsic del conjunt $\mathbb{N}$ dels nombres naturals [PI]

Els nombres naturals es caracteritzen per dos fets notables:

- Tenen un primer element 1.
- Cada element $n \in \mathbb{N}$ té un únic següent $n + 1$.

Però, a més, el conjunt $\mathbb{N}$ compleix el *principi d'inducció* [PI], que estableix el següent:

Sigui $A \subseteq \mathbb{N}$, no buit, tal que

- (1) $1 \in A$, i
- (2) per a cada $n \in A$, podem provar que $n + 1 \in A$.

Aleshores $A = \mathbb{N}$.

Aquest principi el podem reescriure en els termes següents:

Sigui $P(n)$ una propietat relativa als nombres naturals tal que

- (1) $P(1)$ és certa, i
- (2) quan $P(n)$ és certa, podem provar que $P(n + 1)$ també ho és.

Aleshores $P(n)$ és certa per a tot $n \in \mathbb{N}$.

La hipòtesi que fem quan suposem que la propietat P és certa per a un valor n és la *hipòtesi d'inducció*.

Nota. A vegades el primer element de la inducció és zero. Aleshores cal suposar que $\mathbb{N}$ conté el zero. De vegades, la propietat $P(n)$ és certa a partir d'un cert valor n_0 . En aquests casos, hem de provar que

- (1) $P(n_0)$ és certa,
- (2) per a cada $n > n_0$, si $P(n)$ és certa, aleshores $P(n + 1)$ també.

Aquesta mena de principis permeten establir molts i molts resultats importants, i són unes eines indispensables en l'anàlisi combinatòria. Abans, però de ficar-nos de ple en aquesta mena de qüestions, donarem sis exemples il·lustratius.

Problema 1. Per anar de Barcelona a Hostalric podem fer-ho amb tren o bé amb autobús. Supposem que solament hi ha tres maneres d'anar-hi amb tren i dues amb autobús. De quantes maneres diferents és possible anar de Barcelona a Hostalric?

D'acord amb el PA, tenim que

$$|A_1 \cup A_2| = |A_1| + |A_2| = n_1 + n_2 = 3 + 2 = 5,$$

on A_1 és el conjunt d'itineraris de tren i A_2 és el conjunt d'itineraris d'autobús.

Problema 2. Hem d'anar d'Hostalric a Barcelona i, per obres, és necessari fer un tros amb tren i un tros amb autobús. Hi ha tres itineraris possibles de tren i dos d'autobús. Quantes maneres diferents tenim per arribar a Barcelona?

D'acord amb el PM: $|A_1 \times A_2| = 3 \cdot 2 = 6$.

Problema 3. Si $A_1, A_2, \dots, A_k$ són k conjunts disjunts dos a dos i $|A_i| = n_i, i = 1, \dots, k$, aleshores

$$|A_1 \cup A_2 \cup \dots \cup A_{k-1} \cup A_k| = n_1 + n_2 + \dots + n_{k-1} + n_k.$$

D'acord amb el PI hem d'establir:

- (1) La fórmula és vertadera per a $k = 2$, que és el PA.
- (2) Suposem que, si $A_1, A_2, \dots, A_{k-1}, A_k$ són k conjunts disjunts dos a dos i $|A_i| = n_i, i = 1, \dots, k$, aleshores

$$|A_1 \cup A_2 \cup \dots \cup A_{k-1} \cup A_k| = n_1 + n_2 + \dots + n_{k-1} + n_k.$$

És a dir, suposem que la propietat $P(n)$ és certa per a $n = k$. Ara hem de demostrar que, si $A_1, A_2, \dots, A_k, A_{k+1}$ són $k+1$ conjunts disjunts dos a dos i $|A_i| = n_i, i = 1, \dots, k+1$, aleshores

$$|A_1 \cup A_2 \cup \dots \cup A_k \cup A_{k+1}| = n_1 + n_2 + \dots + n_k + n_{k+1}.$$

Per provar-ho, fem $B_1 = A_1 \cup A_2 \cup \dots \cup A_k$ i $B_2 = A_{k+1}$. Els conjunts B_1, B_2 són disjunts:

$$\begin{aligned} B_1 \cap B_2 &= (A_1 \cup A_2 \cup \dots \cup A_k) \cap A_{k+1} = \\ &= (A_1 \cap A_{k+1}) \cup \dots \cup (A_k \cap A_{k+1}) = \emptyset, \end{aligned}$$

atès que els conjunts $A_i, i = 1, \dots, k, k+1$, són disjunts dos a dos.

Ara podem aplicar el PA als conjunts B_1 i B_2 :

$$|B_1 \cup B_2| = |B_1| + |B_2| = (n_1 + \dots + n_k) + n_{k+1}.$$

Per a determinar el cardinal $|B_1|$ hem aplicat la hipòtesi d'inducció.

Problema 4. Quantes parelles ordenades (x, y) de nombres enters hi ha que compleixin la propietat $x^2 + y^2 \leq 5$?

Segui $A = \{(x, y) \in \mathbb{Z}^2 : x^2 + y^2 \leq 5\}$. Fem $A_i = \{(x, y) : x^2 + y^2 = i\}, i = 0, 1, 2, 3, 4, 5$. Aleshores $A_0 = \{(0, 0)\}, A_1 = \{(-1, 0), (1, 0), (0, 1), (0, -1)\}$, etc. Un cop ben caracteritzats els conjunts $A_i, i = 0, 1, 2, 3, 4, 5$, calculem $|A_i|$. Llavors podem aplicar el PA, atès que $A = A_0 \cup A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$, i que els conjunts $A_i, i = 0, 1, 2, 3, 4, 5$, són disjunts dos a dos. Per tant,

$$|A| = |A_0| + |A_1| + |A_2| + |A_3| + |A_4| + |A_5| = 1 + 4 + 4 + 0 + 4 + 8 = 21.$$

Problema 5. Trobeu tots els divisors positius possibles de 600, incloent-hi l'1 i el 600.

Sabem que $600 = 2^3 \cdot 3 \cdot 5^2$. Els seus divisors són de la forma

$$d = 2^i \cdot 3^j \cdot 5^k, \text{ on } 0 \leq i \leq 3, 0 \leq j \leq 1, 0 \leq k \leq 2.$$

Per tant hem de calcular $|D|$, on $D = \{d \in \mathbb{N} : d \mid 600\}$. Cal, doncs, trobar el nombre de ternes ordenades (i, j, k) que podem fer amb $i \in \{0, 1, 2, 3\}$, $j \in \{0, 1\}$, $k \in \{0, 1, 2\}$. Pel PM resulta que $|D| = 4 \cdot 2 \cdot 3 = 24$.

Problema 6. Sabem que el valor Q_n de la suma $1^2 + 2^2 + \dots + (n-1)^2 + n^2$ dels quadrats dels n primers nombres naturals val $\frac{(2n+1)n(n+1)}{6}$.

Una manera de provar-ho és aplicant el principi d'inducció. D'entrada hem de calcular

$$Q_1 = 1^2 = 1 \text{ i } \frac{(2 \cdot 1 + 1) \cdot 1 \cdot (1 + 1)}{6} = 1.$$

Coincideixen.

Seguidament, suposem que $Q_n = 1^2 + \dots + n^2 = \frac{(2n+1)n(n+1)}{6}$. És la hipòtesi d'inducció.

Ara hem de demostrar, basant-nos en la hipòtesi d'inducció, que

$$Q_{n+1} = \frac{(2(n+1)+1)(n+1)((n+1)+1)}{6}.$$

Però,

$$Q_{n+1} = Q_n + (n+1)^2 = \frac{(2n+1)n(n+1)}{6} + (n+1)^2.$$

Només cal fer els càlculs pertinents.

Figures combinatòries

Nombre de parts d'un conjunt A

Sigui A un conjunt amb m elements. El nombre de parts o de subconjunts de A , és a dir, el nombre d'elements del conjunt $\mathcal{P}(A)$, és 2^m . (Indicació: Recordem que $\emptyset$ i A són subconjunts del conjunt A .)

Permutacions de m elements

Una permutació de m objectes és el resultat de col·locar els m objectes en m llocs (o cel·les o també caselles) de manera que cada lloc contingui solament un objecte.

Tenim, doncs, m objectes $\{a_1, a_2, \dots, a_m\}$ en m cel·les. A la primera cel·la n'hi podem col·locar m , a la segona, només $m - 1$, atès que ja n'hi ha un a la primera cel·la i no el podem repetir, etc. Pel PM, resulta que el nombre P_m de permutacions de m objectes és

$$P_m = m(m-1) \cdots 2 \cdot 1 = m!$$

Nota. $m!$ es llegeix *factorial* de m , o bé *m factorial*. Per conveni, $0! = 1$.

Fixem-nos que una *permutació* de m elements és una *filera* o *paraula* feta amb els m objectes sense repetir-ne cap.

Variacions de m elements presos de k en k

Suposem ara que tenim m objectes, però solament disposem de k cel·les, amb $k \leq m$. Cada una de les diferents maneres de col·locar k dels m objectes, sense repetir-ne cap, en les k cel·les és una *variació de m elements presos de k en k*. Dues variacions amb els mateixos objectes però col·locats de maneres diferents, són diferents.

Com abans, és clar que el nombre V_m^k de variacions de m elements presos de k en k és

$$V_m^k = m(m-1) \cdots (m-k+1) = \frac{m!}{(m-k)!}.$$

És clar que $V_m^m = P_m$ i $V_m^0 = 1$, atès que $0! = 1$.

Una *variació de m elements presos de k en k* és una *filera* o *paraula* feta amb k objectes diferents dels m de què disposem.

Combinacions de m elements presos de k en k

Una *combinació de m elements presos de k en k* és una tria de k elements dels m donats.

És evident que ha de ser $k \leq m$.

Això fa que dues variacions de m objectes presos de k en k , amb els mateixos k elements, però col·locats de manera diferent, donin la mateixa combinació. I de variacions diferents que donen una mateixa combinació n'hi ha exactament $k!$. Per tant,

$$C_m^k = \binom{m}{k} = \frac{1}{k!} V_m^k = \frac{m!}{k!(m-k)!}.$$

Els nombres $\binom{n}{k}$ s'anomenen *nombres combinatoris* i tenen propietats molt notables. A tall d'exemple en posem algunes.

$$\binom{n}{k} = \binom{n}{n-k}$$

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

$$\binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1}$$

$$\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

El desenvolupament del *binomi de Newton* conté nombres combinatoris.

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \dots + \binom{n}{n-2}a^2b^{n-2} + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

Podem escriure aquesta fórmula en forma abreujada

$$(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i.$$

Variacions circulars relatives

Una *variació circular relativa* de m objectes presos de k en k és una col·locació arbitrària al voltant d'una taula rodona de k objectes triats d'entre m , tenint en compte que només cal fixar-se en la posició relativa del objectes entre ells, però no en relació a la taula.

Per veure-ho, suposem que $A = \{\alpha, \beta, \gamma, \delta\}$ és un conjunt de $m = 4$ elements i que $k = 3$. Aleshores $V_4^3 = 24$. Ara bé, aquestes vint-i-quatre variacions les podem dividir en 8 grups que són indistingibles per *rotació circular*.

I	II	III	IV	V	VI	VII	VIII
$\alpha\beta\gamma$	$\alpha\beta\delta$	$\alpha\gamma\delta$	$\beta\gamma\delta$	$\alpha\gamma\beta$	$\alpha\delta\beta$	$\alpha\delta\gamma$	$\beta\delta\gamma$
$\gamma\alpha\beta$	$\delta\alpha\beta$	$\delta\alpha\gamma$	$\delta\beta\gamma$	$\beta\alpha\gamma$	$\beta\alpha\delta$	$\gamma\alpha\delta$	$\gamma\beta\delta$
$\beta\gamma\alpha$	$\beta\delta\alpha$	$\gamma\delta\alpha$	$\gamma\delta\beta$	$\gamma\beta\alpha$	$\delta\beta\alpha$	$\delta\gamma\alpha$	$\delta\gamma\beta$

És a dir, cada tres variacions dels elements de A presos de tres en tres donen una mateixa variació circular. Per tant, $Q_4^3 = \frac{1}{3}V_4^3 = 8$.

En general, doncs: $Q_m^k = \frac{1}{k}V_m^k$.

Variacions amb repetició de m objectes presos de k en k

Ara, a diferència de les variacions introduïdes abans en les quals un cop col·locat un objecte en un lloc no era possible col·locar-lo en cap altre lloc, això ho podem fer. Cal, és clar, que disposem de prou còpies de cada objecte. Això fa que, a l'hora de col·locar l'objecte següent, estiguem en les mateixes condicions que abans de col·locar-lo. Hi ha independència de les accions efectuades.

Una *variació amb repetició de m objectes presos de k en k* s'obté quan es col·loquen k còpies d'alguns dels objectes d'un conjunt de m objectes diferents, en k cel·les de manera que cada cel·la només contingui un objecte.

És clar que el nombre VR_m^k de variacions amb repetició de m objectes presos de k en k és $VR_m^k = m^k$.

Permutacions amb repetició de m objectes

Disposem de m objectes dels quals k són iguals entre si i $(m - k)$ també són iguals entre si. Si els permutem de totes les maneres possibles, tindrem $m!$ casos, però no pas tots seran diferents, atès que les permutacions entre si dels k objectes que són indistingibles dona una mateixa permutació. Això fa que, de fet, només en poguem distingir, com a màxim, $\frac{m!}{k!}$. Ara bé, el mateix passa amb les permutacions dels $(m - k)$ objectes indistingibles. Per tant, en total

$$PR_m^k = \frac{m!}{k! (m - k)!} = \binom{m}{k} = C_m^k.$$

En general, si tenim m objectes, però n'hi ha k_1 d'indistingibles, k_2 d'indistingibles, ..., k_r d'indistingibles, amb $k_1 + k_2 + \dots + k_r = m$, aleshores, quan els permutem, tenim les *permutacions amb repetició de m objectes amb $k_1, k_2, \dots, k_r$ de repetits*. El nombre $PR_m^{k_1, \dots, k_r}$ de permutacions amb repetició de m objectes amb $k_1, k_2, \dots, k_r$ de repetits és:

$$PR_m^{k_1, \dots, k_r} = \frac{m!}{k_1! \dots k_r!}.$$

Combinacions amb repetició de m objectes

Donats m objectes dels quals en tenim tantes còpies com faci falta, una *combinació amb repetició de m objectes presos de k en k* és qualsevol tria de k còpies d'entre els m tipus d'objectes diferents.

Per tal de calcular el nombre CR_m^k analitzarem un cas particular. Tenim una pila d'objectes de 4 tipus. Cada objecte pot ser de tipus 1, 2, 3, 4 i en volem triar 3. En

Anàlisi combinatòria

aquest cas, $m = 4, k = 3$. Per representar cada tria disposem de *quatre cel·les* o *caselles* separades entre elles per una paret i numerades de 1 a 4, i 3 boles iguals. Colloquem a cada cel·la tantes boles com objectes d'aquell tipus hi hagi a la tria feta. És a dir,

tries		cel·les				representació	
		1	2	3	4		
111	→	•••				→	•••
112	→	••	•			→	•• •
113	→	••		•		→	•• •
114	→	••			•	→	•• •
122	→	•	••			→	• ••
123	→	•	•	•		→	• • •
124	→	•	•		•	→	• • •
133	→	•		••		→	• ••
134	→	•		•	•	→	• • •
144	→	•			••	→	• ••
222	→		•••			→	•••
223	→		••	•		→	•• •
224	→		••		•	→	•• •
233	→		•	••		→	• ••
234	→		•	•	•	→	• • •
244	→		•		••	→	• ••
333	→			•••		→	•••
334	→			••	•	→	•• •
344	→			•	••	→	• ••
444	→				•••	→	•••

Tal com indica la darrera columna de la taula, podem identificar cada tria amb una seqüència de tres boles i tres barres, corresponents a les boles i als separadors, i fet de totes les maneres possibles; i d'aquestes n'hi ha tantes com les permutacions amb repetició de 6 elements amb 3 i 3 repetits. És a dir,

$$CR_4^3 = PR_{(4-1)+3}^3 = C_6^3 = \binom{6}{3}.$$

En general, tindrem un conjunt prou gran d'objectes, cada un de tipus de 1 a m i n'haurem de triar k ; seguint amb l'exemple anterior, necessitariem m cel·les (per tant, amb $m - 1$ separadors) per a col·locar-hi k boles, posant a cada cel·la tantes boles com objectes d'aquell

tipus hi hagi a la tria. D'aquesta manera podem identificar cada tria amb una successió de k boles i $m - 1$ separadors. Per tant,

$$CR_m^k = PR_{m+k-1}^k = C_{m-1+k}^k = \binom{m+k-1}{k}.$$

Distribucions de k objectes diferents en n capsos diferents

(1) Cada capsa pot contenir, *com a màxim*, un objecte. Aleshores ha de ser $k \leq n$. Com que tots els objectes s'han de col·locar, el nombre de maneres de distribuir-los és el de variacions de n caixes preses de k en k , és a dir, V_n^k .

(2) Cada capsa pot contenir *qualsevol nombre* d'objectes. Aleshores el nombre de maneres de distribuir-los és el de variacions amb repetició de n capsos preses de k en k , és a dir, VR_n^k .

(3) Cada capsa pot contenir qualsevol nombre d'objectes, però l'ordre dins de cada capsa és rellevant. Aleshores el nombre de casos és $\frac{(n-1+k)!}{(n-1)!}$.

Distribucions de k objectes idèntics en n capsos diferents

(1) Si cada capsa pot contenir, *com a màxim*, un objecte, aleshores ha de ser $k \leq n$ i el nombre de maneres de distribuir-los és el de combinacions de n capsos preses de k en k , és a dir, $\binom{n}{k}$.

(2) Si cada capsa pot contenir qualsevol nombre d'objectes, aleshores el nombre de maneres de distribuir-los és el de combinacions amb repetició de n capsos preses de k en k , és a dir CR_n^k .

Problemes

AC1. Sigui $N = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, on $p_1, p_2, \dots, p_r$ són nombres primers, i D el conjunt dels divisors positius de N . Llavors $|D| = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$.
(És un simple exercici d'aplicació del principi multiplicatiu).

AC2. Proveu, per inducció, que el nombre de subconjunts d'un conjunt A , de cardinal m , inclosos el conjunt buit i A , té cardinal 2^m .

Anàlisi combinatòria

AC3. Proveu, per inducció, que si un conjunt A té m elements, el conjunt d'aplicacions de A en el conjunt $2 = \{0, 1\}$, en té 2^m .

Sabríeu provar-ho d'una altra manera?

AC4. Useu el PM per provar que el nombre de tirallongues de n nombres naturals agafats del conjunt $A = \{1, 2, \dots, k\}$ és igual a k^n .

AC5. El menú turístic d'un restaurant és:

Elegiu un dels entrants:

Sopa, Suc de fruita, Cocktail de marisc.

Elegiu un dels següents plats de vianda:

Bistec

Roast Beaf

Pollastre rostit

Mandonguilles amb espagueti

Elegiu un dels següents acompanyaments:

Patates fregides

Tomàquet a la grega

Pèsols saltejats

Elegiu una d'aquestes postres:

Fruita, Gelat, Formatge.

Elegiu:

Café o Té.

Quants menjars diferents hi pot fer un turista? Quin dia podrà tornar a casa seva si el primer dinar el fa el 28 de febrer de 1993, suposant que els vol tastar tots i només hi dina?

AC6. Llançem 6 daus indistingibles. Quants resultats diferents podem observar? I si els daus són distingibles?

AC7. Considerem totes les VR_4^2 del conjunt $\{1, 2, 3, 4\}$ i totes les V_4^2 . Quants elements cal eliminar de les primeres per tal d'aconseguir CR_4^2 ? I quines hem d'eliminar de les segones per obtenir C_4^2 ?

AC8. (i) Quatre persones volen jugar simultàniament partits individuals de tennis i disposen de dues pistes. De quantes maneres podem distribuir-los, si no tenim en compte l'elecció de pista? De quantes maneres, si es té en compte la pista on juga cada parella?

(ii) De quantes maneres podem situar m persones en r llocs diferents si volem que $m_1, m_2, \dots, m_r$ es colloquin respectivament al lloc $1, 2, \dots, r$? ($m_1 + m_2 + \dots + m_r = m$).

AC9. Sis muntanyencs s'han de dividir en 3 grups de dos cada un per tal de fer l'assalt final. De quantes maneres poden fer-ho? I si els grups consten d'1, 2 i 3 persones?

Si ara cal ordenar-los en primer, segon i tercer grup d'assalt, de quantes maneres ho podrem fer?

AC10. Proveu que

$$\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n};$$

$$\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-2}{n-1} + \dots + \binom{n}{n-1} + \binom{n-1}{n-1}.$$

AC11. Proveu que

$$\binom{m}{n} = \sum_{j=0}^k \binom{k}{j} \cdot \binom{m-k}{n-j}$$

i calculeu $\binom{7}{3}$ i $\binom{7}{5}$ fent servir el triangle aritmètic fins a la fila 5.

AC12. De quantes maneres podem posar n boles en n capsos numerades de forma que quedi buida exactament una capsa? (Indicació: Separeu el cas distingible del cas indistingible.)

AC13. Una noia vol regalar al seu xicot una camisa o una corbata pel seu aniversari. Però solament pot triar entre 3 camises i 2 corbates. Quantes tries diferents pot fer? I si vol comprar alhora una camisa i una corbata?

AC14. En una botiga hi ha tres menes de camises per vendre

(a) Si dos homes compren una camisa cada un, de quantes maneres diferents poden fer-ho?

(b) Si un home compra dues camises, de quantes maneres pot triar-les?

Anàlisi combinatòria

AC15. Quantes inicials diferents podem fer amb dues o tres lletres de l'alfabet? Quantes lletres hauria de tenir un alfabet per tal que un milió de persones diferents es pogués identificar amb inicials de dues o tres lletres?

AC16. De quantes maneres es poden aparellar 4 nois i 4 noies? De quantes maneres es poden col·locar en una fila de manera que s'alternin persones de sexe diferent?

AC17. De quantes maneres podem triar un comitè de tres persones d'un grup de 20? I de quantes si cal que una sigui el president, l'altre el vicepresident i la tercera secretari?

AC18. Si tenim dues monedes de 50 pta, dues de 25 pta i tres duros, quantes sumes diferents podem aconseguir? Si canviem una de les monedes de 25 pta en duros, quantes sumes diferents podrem aconseguir?

AC19. Deu llibres es col·loquen en dues piles. De quantes maneres podem fer-ho si els llibres són indistingibles? I si són distingibles? I si les piles són distingibles o indistingibles? Analitzeu els 4 casos.

AC20. Repartim deu llibres diferents entre en Daniel, en Felip, en Pau i en Joan de manera que s'enduen respectivament lots de 3, 3, 2 i 2 llibres. De quantes maneres podem fer-ho?

En Pau i en Joan no estan d'acord amb aquest repartiment i es decideix repartir els lots entre ells de manera que cada un tingui un lot. De quantes maneres podem fer ara el repartiment? Ara la Maria i la Cori volen també tenir dret a aconseguir llibres. Es decideix repartir els lots entre tots sis de forma que hi haurà dues persones que no obtindran cap lot. De quantes maneres podem fer això?

AC21. Considereu el conjunt $A = \{1, 2, \dots, 100\}$ i sigui

$$S = \{(a, b, c) : a, b, c \in A, a < b \text{ i } a < c\}.$$

Trobeu $|S|$.

AC22. Proveu, per inducció, que $1^3 + 2^3 + \dots + n^3 = \frac{n^2(n+1)^2}{4}$. Sabríeu demostrar-ho d'alguna altra manera?

AC23. Trobeu les identitats que expressen, en funció de n , els valors de
(a) $1 + 2 + \dots + n$, (b) $1^2 + 2^2 + \dots + n^2$, i (c) $1^3 + 2^3 + \dots + n^3$.

Fixeu-vos en la diferència que hi ha entre trobar una expressió i provar-ne la validesa, un cop trobada.

AC24. De quantes maneres podem fer la tria d'una parella $\{a, b\}$ de nombres diferents del conjunt $A = \{1, 2, \dots, 50\}$, si volem que

(a) $|a - b| = 5$,

(b) $|a - b| \leq 5$.

AC25. *Principi additiu general* [PAG]: Si A, B són dos conjunts finits, aleshores $|A \cup B| = |A| + |B| - |A \cap B|$. Proveu-ho.

AC26. Proveu que el nombre de *bijeccions* que podem fer entre el conjunt $m = \{1, 2, \dots, m\}$ i un conjunt A amb m elements coincideix amb el nombre de permutacions de m elements.

AC27. Suposem que volem col·locar m objectes en m cadires que es troben al voltant d'una taula rodona i que les cadires estan numerades amb els números $1, 2, \dots, m-1, m$.

Proveu que les maneres de fer-ho és $m!$. *Nota:* Les cadires són distingibles.

Què passaria, si les cadires no fossin distingibles?

AC28. Sigui A, B dos conjunts i suposem que $|A| = k, |B| = m, k \leq m$. Quantes *injeccions* podem fer de A en B ?

AC29. (a) Tenim 4 fitxes marcades amb les lletres a, b, c, d . Quantes paraules de tres lletres podem fer?

(b) Quantes paraules de tres lletres podem fer amb les lletres a, b, c, d ?

(c) Tenim 9 fitxes numerades de l'1 al 9. Quants nombres de 4 xifres podem fer?

(d) Quants nombres de 4 xifres podem fer usant només els nombres $1, 2, 3, 4, 5, 6, 7, 8, 9$?

AC30. Sigui $A = \{a, b, c, \dots, x, y, z\}$ el conjunt de les 26 lletres de l'alfabet català. Quin és el nombre de paraules de 5 lletres que podem fer amb les lletres de A , si volem que la primera i la darrera siguin vocals i les altres tres consonants?

Anàlisi combinatòria

AC31. En una festa hi ha 7 nois i 3 noies. De quantes maneres podem posar-los en fila, si volem que

(a) les noies formin un bloc, (b) les dues posicions finals estiguin ocupades per nois i que cap noia no estigui al costat d'una altra noia?

AC32. Entre 20.000 i 70.000, quants nombres parells hi ha que no tinguin cap dígit repetit?

AC33. Sigui A el conjunt dels nombres naturals els díigits dels quals són $\{1, 3, 5, 7\}$ sense que n'hi hagi cap de repetit. Calculeu:

(a) el cardinal del conjunt A ;

(b) el nombre $S = \sum_{m \in A} m$.

AC34. (a) Proveu que tot nombre combinatori és un nombre natural. Sabríeu demostrar-ho per inducció?

(b) Proveu que, si p és un nombre primer i $1 \leq k < p$, aleshores $\binom{p}{k}$ és un múltiple de p .

(c) Què passa quan p no és un nombre primer? [Indicació: Feu unes quantes fileres del triangle aritmètic.]

AC35. Proveu que $\binom{m}{k}$ és el nombre de subconjunts de k elements d'un conjunt A de m elements. Deduïu-ne que

$$\binom{m}{0} + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{m-1} + \binom{m}{m} = 2^m.$$

AC36. Fem tirallongues de 0 i 1 de llargada 7. Quantes n'hi ha que tinguin 3 zeros i 4 uns? Deduïu-ne que $\binom{m}{k} = \binom{m}{m-k}$.

AC37. De quantes maneres podem fer un comitè de 5 persones d'un col·lectiu de 11 de les quals 4 són noies i 7 són nois, si volem que

(a) el comitè tingui exactament dues noies?

(b) el comitè tingui almenys 3 noies?

(c) el comitè contingui una noia i un noi concrets?

AC38. (a) De quantes maneres diferents podem formar tres equips de futbol amb 33 nois?

(b) Si $|A| = 2n, n \geq 1$, quantes parelles d'elements de A podem fer?

(c) Generalitzeu aquest problema. Proveu que el nombre de k -agrupacions diferents d'elements de A , amb $|A| = nk$ és precisament $\frac{(nk)!}{n! (k!)^n}$.

Mostra de solucions

Solució del problema AC14

Suposem que dos homes compren una camisa cada un. El primer home pot comprar una camisa d'un dels tres tipus que hi ha. El segon home també. Per tant hi ha $3 \times 3 = 9$ maneres de fer-ho. També es pot interpretar que es tracta de VR_3^2 .

Si un home compra dues camises, l'ordre com les tria no és rellevant per al resultat final de la compra. Com que els tipus de camises es poden repetir, tindrem $CR_3^2 = \binom{3+2-1}{2} = 6$ maneres de fer-ho.

Solució del problema AC18

És un problema de comptes de la vella, és a dir, cal comptar sense equivocar-se ni deixar-se cap cas, ni repetir-ne cap.

D (duros)	$D+25$	$D+2 \cdot 25$ $(D+50)$	$D+25+50$	$D+2 \cdot 25+50$ $(D+2 \cdot 50)$	$D+2 \cdot 50$ $+25$	$D+2 \cdot 50$ $+2 \cdot 25$
	25	50	75	100	125	150
5	30	55	80	105	130	155
10	35	60	85	110	135	160
15	40	65	90	115	140	165.

L'altre cas es deixa per al lector.

Solució del problema AC19

a) Llibres indistingibles i piles distingibles. Els deu llibres es poden col·locar a les piles en les formes $(0, 10), (1, 9), \dots, (9, 1)$ i $(10, 0)$. En total hi ha 11 maneres de fer-ho.

b) Llibres indistingibles i piles indistingibles. Les piles dels cas anterior $(0, 10)$ i $(10, 0)$ són indistingibles. També ho són les $(1, 9)$ i $(9, 1)$, etc. fins a les $(4, 6)$ i $(6, 4)$. L'apilament $(5, 5)$ no té parella. En total els apilaments es poden fer de 6 maneres.

Anàlisi combinatòria

c) Llibres distingibles i piles distingibles. Primer permutem els llibres de totes les maneres possibles, que seran $10!$. Fixada una permutació concreta dels llibres, apilem-los tal com hem fet al cas a). Tindrem en total $11 \times 10!$ maneres en total.

d) Llibres distingibles i piles indistingibles. Es raona com al cas anterior formant les $10!$ permutacions de llibres, i apilant-los després segons b). En total hi haurà $6 \times 10!$ casos.

Solució del problema AC30

A l'alfabet de 26 lletres hi ha 5 vocals i 21 consonants. Podem fixar les vocals de $VR_5^2 = 5^2$ maneres diferents, i les consonants de $VR_{21}^3 = 21^3$ maneres diferents. En total tindrem $5^2 21^3$ paraules.

Solució del problema AC31

a) Considerem les tres noies com un bloc. Les noies, en aquest bloc, poden col·locar-se de $3!$ maneres diferents. Si marquem amb números les posicions dels nois, i amb $\bullet$ els llocs inicial, final i intermedis, tindrem

$$\bullet 1 \bullet 2 \bullet 3 \bullet 4 \bullet 5 \bullet 6 \bullet 7 \bullet$$

i el bloc de noies ha d'ocupar una de les posicions marcades per $\bullet$. En total tindrem, doncs, $8 \times 3! 7!$ col·locacions possibles.

b) Si marquem, com abans, les posicions dels nois amb números, cada una de les noies pot ocupar una posició $\bullet$ a

$$1 \bullet 2 \bullet 3 \bullet 4 \bullet 5 \bullet 6 \bullet 7$$

i haurem de triar 3 $\bullet$ d'entre els 6 que hi ha. Com que les noies es poden permutar i els nois també, tindrem $C_6^3 P_3 P_7 = V_6^3 P_7$ possibilitats.

EL PRINCIPI DE LES CASELLES

Josep Pla i Carrera

El principi de Dirichlet

La idea del principi és molt senzilla: si hem de col·locar tres coloms en dues caselles, necessàriament dos coloms han de compartir una mateixa casella.

El principi de les caselles (o del colomar) [PC]

Enunciat 1:

Siguin k i n dos enters positius. Si almenys $kn + 1$ objectes es distribueixen entre n compartiments, aleshores almenys un dels compartiments contindrà $k + 1$ objectes.

Enunciat 2:

Si N objectes s'han de distribuir entre k cel·les o caselles, aleshores una almenys de les cel·les conté un nombre d'objectes que és més gran o igual que $\left\lceil \frac{N}{k} \right\rceil + 1$, en el cas que k no divideixi N . Si k divideix N , el nombre d'objectes és més gran o igual que $\frac{N}{k}$.

En particular, si $n + 1$ objectes es reparteixen entre n cel·les o caselles, aleshores una almenys conté dos objectes.

Aquest principi es coneix també amb el nom de *principi de Dirichlet* [DIRICHLET, P. G. LEJEUNE [1805–1859]]. En anglès es parla habitualment del *drawer principle* o, molt més sovint, del *pigeon-hole principle*, on el mot “pigeon-hole” equival a una casella d'un moble subdividit en cel·les per tal de col·locar-hi cartes, documents o altres objectes, i classificar-los (en castellà, “casillero”). Però l'ús reiterat porta a parlar de “pigeons i de “holes” separadament, fent-los servir com a primer exemple del principi. Tot això condueix a la denominació pintoresca de “colomar”.

El principi de les caselles

Problema 1. *Quantes persones cal reunir per tal d'assegurar que n'hi ha dues que tenen nom amb la mateixa inicial?*

El conjunt de "caselles" és el conjunt de lletres de l'alfabet, suposem que són 26. Si tenim 27 persones i les "colloquem" a les caselles, n'hi ha dues a la mateixa, i per tant tenen el nom amb la mateixa inicial. Si només hi hagués 26 persones, podria donar-se el cas que totes tinguessin inicials diferents.

Problema 2. *Quantes persones cal reunir per tal d'assegurar que n'hi ha sis que tenen nom amb la mateixa inicial?*

El conjunt de "caselles" és com abans el conjunt de les 26 lletres de l'alfabet. Si tenim $26 \times 5 + 1 = 131$ persones podem assegurar que al menys 6 d'elles tenen la mateixa inicial. Amb només 130 persones això no es podria assegurar, ja que podria haver-n'hi 5 de cada lletra.

Problema 3. *En una classe hi ha estudiants dels dos sexes, de tres pobles i que practiquen cinc esports. Quants n'hem de reunir per tal d'assegurar que n'hi ha dos del mateix sexe, del mateix poble i que practiquen el mateix esport?*

Assignem a cada estudiant una terna xyz on x pot ser H home o D dona, y pot ser P_1, P_2, P_3 , segons el poble d'origen, i z pot ser E_1, E_2, E_3, E_4, E_5 , segons l'esport practicat. El conjunt de totes les ternes possibles té $2 \times 3 \times 5 = 30$ elements. Si tenim 31 estudiants, és segur que n'hi ha 2 als quals els correspon la mateixa terna, és a dir, són del mateix sexe, del mateix poble i practiquen el mateix esport. Si només tinguéssim 30 estudiants, podria donar-se el cas que tots tinguessin ternes diferents, i dos a dos tindrien sempre algun atribut diferent.

Observació: Malgrat la seva aparença trivial, el principi de les caselles és un instrument molt potent per a demostrar, sota condicions que només afecten el nombre d'elements, l'existència de certs elements d'un conjunt que comparteixen les mateixes propietats.

Problemes

PC1. Proveu el principi del colomar.

PC2. Demostreu que entre els individus d'un grup de set persones, almenys n'hi ha quatre del mateix sexe.

PC3. Entre els individus d'un grup de 3000 persones, sempre n'hi ha 9 que tenen el mateix dia d'aniversari.

PC4. Entre els individus d'un grup de 2 o més persones, sempre n'hi ha dues amb el mateix nombre d'amics dins del grup. (Suposem que tot individu és sempre amic d'ell mateix i que l'amistat és una relació simètrica.)

PC5. Proveu que en tota elecció de 10 punts elegits en un quadrat de 3 unitats de costat, sempre hi ha 2 punts que disten com a màxim $\sqrt{2}$.

Nota. En aquest problema hom pot veure la importància en l'elecció de les cel·les. Si, per exemple, haguéssim elegit rectangles $\frac{1}{3} \times 3$, no hauríem pogut concloure allò que se'ns demanava.

PC6. Deu jugadors formen part d'un campionat d'escacs de tots contra tots; és a dir, cada jugador ha de jugar un joc amb cada un dels altres. Un jugador s'anota +1, quan guanya, 0, quan fa taules, i -1, quan perd. Quan el torneig s'acaba resulta que el 70 % dels jocs han estat taules. Proveu que hi ha dos jugadors amb el mateix nombre de punts.

PC7. *Olimpíada d'Israel, 1988*. Un grup de persones visita una exposició de 100 quadres. Cap no arriba a veure tots els quadres, però tots els quadres han estat vistos per algun dels visitants. Proveu que hi ha una parella de visitants (v_1, v_2) i una parella de quadres (α, β) tals que v_1 ha vist α però no ha vist β i v_2 ha vist β però no ha vist α .

PC8. *Putnam Competitions, 1953*. Distribuïm sis punts a l'espai sense que n'hi hagi tres d'alineats ni tampoc quatre de coplanaris. Ara tracem segments, en total quinze, que els uneixin dos a dos. Alguns els pintem de color blau i els altres de color vermell. Proveu que hi ha almenys un triangle que té tots els costats del mateix color.

Nota. Amb cinc vèrtexs no és possible de garantir un triangle del mateix color. Busqueu un contraexemple.

PC9. [*American Mathematical Monthly*, 65 (1958), 446, i resolt a 66 (1959), 141-142.] En una reunió de sis persones sempre n'hi ha tres que es coneixen mútuament o que es desconeixen totalment. Demostreu-ho.

El principi de les caselles

PC10. *Olimpiada Matemàtica Internacional, 1964/4.* Disset persones s'escriuen entre elles, cada una amb totes les altres. En les cartes només tracten tres temes. Cada parella de corresponsals, però, només tracta un dels temes. Proveu que almenys n'hi ha tres que escriuen sobre el mateix tema.

PC11. Donat un conjunt de 10 enters positius diferents i menors que 107, demostreu que hi ha dos subconjunts disjunts que tenen la mateixa suma.

PC12. Les persones d'una reunió han fet encaixades de mans en arribar. Suposem que ningú es dona la mà a ell mateix i cap parella de persones s'ha donat la mà més d'una vegada. Demostreu que hi ha dues persones a la reunió que han encaixat el mateix nombre de mans.

PC13. En un disc de radi 1 hi posem 8 punts (a l'interior o sobre la circumferència). Demostreu que n'hi ha dos que estan a distància estrictament inferior a la unitat.

PC14. Donat un conjunt de n enters positius qualssevol, hi ha un subconjunt tal que la suma dels seus elements és divisible per n . Demostreu-ho.

PC15. *P. Erdős.* Demostreu que donada una successió de més de $(r-1)(s-1)$ nombres diferents, hi ha una subsuccessió creixent de r termes, o hi ha una subsuccessió decreixent de s termes.

PC16. Suposem que el nombre màxim de llibres que pot tenir una persona és 50000. Demostreu que a Barcelona hi ha dues persones que tenen el mateix nombre de llibres. El nombre màxim de cabells per mm^2 és 5. Demostreu que a Espanya hi ha dues persones amb el mateix nombre de cabells.

PC17. Cada dia posem a una guardiola una moneda de 1 pta o una moneda de 2 pta i el total que tenim al cap de n dies és de m pta. Demostreu que per cada enter $0 \leq k \leq 2n - m$ hi ha un conjunt de dies consecutius durant els quals el contingut de la guardiola s'ha incrementat en k pta.