Problemes de teoria de nombres

11. (OI 1969) Demostreu que, per a tot $n > 1$, $n^4 + 4$ és sempre un nombre compost.

Solució

$$n^4 + 4 = n^4 - 4n^2 + 4 - 4n^2 = (n^2 - 2)^2 - 4n^2 = (n^2 - 2 + 2n)\,(n^2 - 2 - 2n).$$

12. (OI 1959) Demostreu que, per a tot nombre natural n, la fracció $\dfrac{21n + 4}{14n + 3}$ és irreductible.

Solució

Si d és un divisor de $21n + 4$ i de $14n + 3$, llavors d divideix també

$$2(21n + 4) = 42n + 8 \quad \text{i} \quad 3(14n + 3) = 42n + 9.$$

Per tant divideix la diferència que és 1.

13. (OI 1964) (a) Trobeu tots els enters positius m pels quals $2^n - 1$ és divisible per 7.

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

Solució

(a) A $\mathbb{Z}_7$ es compleix que $2^0 = 1, 2^1 = 2, 2^2 = 4$ i $2^3 = 1$ de forma que l'ordre de 2 a $\mathbb{Z}_7$ és 3. Per tant $2^n - 1$ és divisible per 7 si, i només si, n és múltiple de 3.

(b) De la mateixa manera, $2^n + 1$ serà divisible per 7 si, i només si, $2^n = -1 = 6$ a $\mathbb{Z}_7$ la qual cosa és impossible.

14. (OI 1972) Siguin m i n enters no negatius qualssevol. Demostreu que

$$\frac{(2m)!\,(2n)!}{m!\,n!\,(m+n)!} \quad \text{és un enter.} \qquad (0! = 1).$$

Primera solució

En primer lloc recodem que s'anomena *valoració p–àdica* d'un enter $a \neq 0$, i s'indica $v_p(a)$, l'exponent amb el que el primer p figura a la descomposició d'a en factors primers.

De la mateixa definició en resulta fàcilment que $v_p(a) \geq 0$, que $v_p(1) = 0$, i que, si a, b són enters no nuls, $v_p(a \cdot b) = v_p(a) + v_p(b)$. Si $\frac{m}{n}$ és un nombre racional no nul, es defineix $v_p\left(\frac{m}{n}\right) = v_p(m) - v_p(n)$.

El nombre racional $\frac{m}{n}$ serà enter ssi, per a tot nombre primer p, $v_p(m) \geq v_p(n)$.

Per tant resoldre la qüestió plantejada és equivalent a demostrar que

$$(1) \qquad \begin{cases} v_p\left((2m)!\,(2n)!\right) - v_p\left(m!\,n!\,(m+n)!\right) = \\ = v_p\left((2m)!\right) + v_p\left((2n)!\right) - v_p\left(m!\right) - v_p\left(n!\right) - v_p\left((m+n)!\right) \geq 0, \end{cases}$$

per a tot nombre primer p.

És sabut que $v_p(m!) = \sum_{i=1}^{\infty} \left[\frac{m}{p^i}\right]$, on $\left[\frac{m}{p^i}\right]$ representa la part entera del nombre racional $\frac{m}{p^i}$, És clar que aquesta suma és finita ja que, si $p^r \leq m < p^{r+1}$, $\left[\frac{m}{p^i}\right] = 0$ per a $i \geq r+1$. Per demsotrar-ho primer es comprova que és cert per a $m = 0$, i després es pot procedir o bé per inducció sobre m o bé simplement comptant quantes vegades apareix el factor p a $m!$ amb exponent igual almenys a 1, quantes amb exponent igual almenys a 2, quantes amb exponent almenys igual a 3, etc.

Tenint això en compte, provar (1) és equivalent a provar que, per a tot primer p,

$$\sum_{i=1}^{\infty} \left[\frac{2m}{p^i}\right] + \sum_{i=1}^{\infty} \left[\frac{2n}{p^i}\right] - \sum_{i=1}^{\infty} \left[\frac{m}{p^i}\right] - \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] - \sum_{i=1}^{\infty} \left[\frac{m+n}{p^i}\right] \geq 0.$$

Com que totes les sumes són finites aquesta condició es pot escriure en la forma

$$\sum_{i=1}^{\infty} \left(\left[\frac{2m}{p^i}\right] + \left[\frac{2n}{p^i}\right] - \left[\frac{m}{p^i}\right] - \left[\frac{n}{p^i}\right] - \left[\frac{m+n}{p^i}\right] \right) \geq 0$$

per tant basta provar que

$$\left[\frac{2m}{p^i}\right] + \left[\frac{2n}{p^i}\right] - \left[\frac{m}{p^i}\right] - \left[\frac{n}{p^i}\right] - \left[\frac{m+n}{p^i}\right] \geq 0$$

per a tot primer p i tot $i \geq 1$.

Si posem

$$\frac{m}{p^i} = \left[\frac{m}{p^i}\right] + \alpha, \quad 0 \leq \alpha < 1, \qquad \frac{n}{p^i} = \left[\frac{n}{p^i}\right] + \beta, \quad 0 \leq \beta < 1,$$

es té

$$\left[\frac{2m}{p^i}\right] = 2\left[\frac{m}{p^i}\right] + [2\alpha], \quad \left[\frac{2n}{p^i}\right] = 2\left[\frac{n}{p^i}\right] + [2\beta], \quad \left[\frac{m+n}{p^i}\right] = \left[\frac{m}{p^i}\right] + \left[\frac{m}{p^i}\right] + [\alpha+\beta].$$

Per tant,

$$\left[\frac{2m}{p^i}\right] + \left[\frac{2n}{p^i}\right] - \left[\frac{m}{p^i}\right] - \left[\frac{n}{p^i}\right] - \left[\frac{m+n}{p^i}\right] = [2\alpha] + [2\beta] - [\alpha+\beta]$$

que pot ser 0 o 1 segons els valors d'α i β.

Exemple

$$\frac{14!\,30!}{7!\,15!\,22!} = 2^3 \cdot 3^2 \cdot 5 \cdot 13 \cdot 23 \cdot 29 = 3\,121\,560.$$

Anàlisi del problema

Comentari: Aquest problema es podria classificar com un problema d'ofici matemàtic: és prou difícil com perquè no surti en una primera aproximació "naïf" però, si se n'ha vist algun altre de semblant, és força rutinari. En tot cas, és prou instructiu.

Solució: En un primer intent es pot abordar el problema per inducció, per exemple sobre n, tot mantenint m fix. Però el cas $n = 0$ ja ens presenta problemes. Si anomenem $f(m,n)$ a l'expressió en qüestió, el cas $f(m,0)$ és

$$f(m,0) = \frac{(2m)!}{m!\,m!}$$

que sabem que és un sencer perquè $\dfrac{(2m)!}{m!\,m!} = \binom{2m}{m} = C_{2m}^{m}$ són les combinacions de $2m$ elements agafats d'm en m. Arribats a aquest punt ens podem plantejar ja una pregunta rellevant: com es demostra que $\binom{m}{n} = \dfrac{m!}{n!(m-n)!}$ és un nombre sencer sense fer servir el fet que aquest número representa el nombre de combinacions d'm elements agafats d'n en n?

De moment deixem la pregunta a l'aire i seguim els nostres intents de demostrar el resultat inicial per inducció sobre n. Ja sabem que $f(m,0)$ és un sencer. Ara suposem que $f(m,n)$ també ho és i intentem de demostrar que $f(m,n+1)$ també ho és:

$$f(m,n+1) = \frac{(2m)!(2n+2)!}{m!(n+1)!(m+n+1)!} = \frac{(2m)!(2n+2)(2n+1)(2n)!}{m!(n+1)n!(m+n+1)(m+n)!} =$$
$$= \frac{(2m)!(2n)!}{m!n!(m+n)!} \cdot \frac{2(n+1)(2n+1)}{(n+1)(m+n+1)} = f(m,n) \cdot \frac{2(2n+1)}{m+n+1}.$$

Per desgràcia el fet que $f(m,n)$ sigui sencer no ens ajuda pas gaire a l'hora de demostrar que $f(m,n+1) \in \mathbb{N}$. Si haguessim aconseguit trobar una relació similar però sumant en comptes de multiplcant, llavors hi hauria més possibilitats d'èxit.

Ens veiem obligats a abandonar aquesta via que, malgrat el fracàs, ens ha deixat dos fets importants que cal retenir:

1. $\dfrac{(2m)!}{m!\,m!} = \binom{2m}{m} = \mathrm{C}_{2m}^{m}$, i per tant $\dfrac{(2m)!}{m!\,m!}$ és un sencer perquè respon a un problema combinatori.
2. La pregunta: com es demostra que $\binom{m}{n} = \dfrac{m!}{n!(m-n)!}$ és un enter sense fer servir el fet que aquest número representa el nombre de combinacions d'm elements agafats d'n en n?

El fet 1) ens condueix a reformular el nostre problema en el sentit indicat: podem trobar un problema combinatori la resolució del qual sigui precisament l'expressió $f(m,n)$?

Unes quantes manipulacionms porten l'expressió original d'$f(m,n)$ a una forma potser més engrescadora en aquesta línia:

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

Queda com a problema obert el trobar un enunciat en termes combinatoris, la solució del qual doni exactament aquesta expressió.

2) La resposta es pot trobar a qualsevol llibre d'anàlisi algebraica o de teoria de nombres elemental[1]:

Lema. *El nombre de vegades que un primer p divideix exactament $m!$ és igual a:*

$$\left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \left[\frac{m}{p^3}\right] + \cdots + \left[\frac{m}{p^k}\right] + \cdots,$$

on $[x]$ representa la part entera d'x.

[1] Veure per exemple *Introducción a la teoría elemental de números*. Niven y Zuckerman, Ed. Limusa, 88–89 o bé *La teoría de los números*. J. Cilleruelo y A. Córdoba. Ed. Biblioteca Mondadori, Madrid, 1992, 2–4.

La sèrie anterior de fet és finta ja que quan $p^k > m$, $\left[\frac{m}{p^k}\right] = 0$.

Amb aquest resultat és fàcil veure que tot primer que aparegui a la descomposició en factors primers d'$n!$ o d'$(m-n)!$ (suposant $n < m$) apareix a la descomposició en factors primers d'$m!$ i amb exponent més petit o igual i que, si un primer p apareix alhora a la descomposició d'$n!$ i d'$(m-n)!$,

$$\left[\frac{n}{p^k}\right] + \left[\frac{m-n}{p^k}\right] \leq \left[\frac{m}{p^k}\right].$$

En conseqüència, $\dfrac{m!}{n!(m-n)!}$ és un enter.

Això ens dóna la clau per trobar una demostració del nostre problema: estudiem la descomposició en factors primers del numerador i del denominador de l'expressió i intentem de demostrar que tots els factors primers del denominador apareixen a la descomposició del numerador amb exponent més petit o igual:

Si p és un factor primer del denominador, és un factor primer del numerador. En efecte, si p és un factor primer del denominador, p apareix a la descomposició d'$n!$ o d'$m!$ o d'$(m+n)!$. Lavors $p \leq \max(n, m, m+n)$ i per tant $p \leq \max(2n, 2m, m+n)$. D'ací en deduïm que p no pot ser alhora $> 2m$ i $> 2n$ [ja que, si $p \leq (m+n)$, aleshores $2p \leq 2(m+n)$].

Ara, si p^a és la contribució del factor primer p al denominador i p^b és la del numerador, anem a veure que $a \leq b$:

$$\begin{aligned} a &= \sum_j \left[\frac{m}{p^j}\right] + \sum_j \left[\frac{n}{p^j}\right] + \sum_j \left[\frac{m+n}{p^j}\right] = \sum_j \left(\left[\frac{m}{p^j}\right] + \left[\frac{n}{p^j}\right] + \left[\frac{m+n}{p^j}\right]\right) \\ b &= \sum_j \left[\frac{2m}{p^j}\right] + \sum_j \left[\frac{2n}{p^j}\right] = \sum_j \left(\left[\frac{2m}{p^j}\right] + \left[\frac{2n}{p^j}\right]\right) \end{aligned}$$

per un j fix. Ara podem demostrar que

$$\left[\frac{m}{p^j}\right] + \left[\frac{n}{p^j}\right] + \left[\frac{m+n}{p^j}\right] \leq \left[\frac{2m}{p^j}\right] + \left[\frac{2n}{p^j}\right],$$

resultat que es pot veure en general —si $x, y \geq 0$, $[x]+[y]+[x+y] \leq [2x]+[2y]$—, i que havíem trobat ja a la primera resposta al problema.

Si fem $x = [x] + r, y = [y] + s$, llavors $x + y = [x] + [y] + r + s$, que ens diu que $[x + y] = [x] + [y] + [r + s]$; per una altra banda, $2x = [2x] + 2r$ i $2y = [2y] + 2s$. Per tant $[2x] = 2[x] + [2r]$, $[2y] = 2[y] + [2s]$. Cal, doncs, comparar les dues expressions següents:

$$\begin{aligned} [x] + [y] + [x + y] &= [x] + [y] + [x] + [y] + [r + s] \\ [2x] + [2y] &= 2[x] + 2[y] + [2r] + [2s]. \end{aligned}$$

N'hi ha prou, doncs, a establir que $[r + s] \leq [r] + [s]$, amb $0 \leq r, s \leq 1$, relació immediata si analitzem els casos possibles: $1 < r + s < 2, r + s \leq 1$.

Segona solució

Considerem la taula triangular dels valors $a_n^m = f(m,n)$:

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 2 & & 2 & & & & & \\
 & & & & 6 & & 2 & & 6 & & & & \\
 & & & 20 & & 4 & & 4 & & 20 & & & \\
 & & 70 & & 10 & & 6 & & 10 & & 70 & & \\
 & 252 & & 28 & & 12 & & 12 & & 28 & & 252 & \\
 & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & &
\end{array}$$

Ara, a ull, hem de veure si és possible de trobar un lligam entre un cert a_{mn} i d'altres $a_{k\ell}$, amb $k < m$ o $\ell < n$.

S'observa força fàcilment que cada element és igual a quatre vegades el que té a la fila de sobre a l'esquerra menys el que té a l'esquerra. Per exemple:

$$10 = 4 \cdot 20 - 70; \quad 6 = 4 \cdot 4 - 6; \quad 10 = 4 \cdot 4 - 6; \quad 70 = 4 \cdot 20 - 10;$$

$$28 = 4 \cdot 70 - 252; \quad 12 = 4 \cdot 10 - 28; \quad 12 = 4 \cdot 6 - 12; \quad 28 = 4 \cdot 10 - 12; \quad 252 = 4 \cdot 70 - 28.$$

Ara podríem deduir perfectament la setena fila: primerament calculem

$$a_0^6 = f(6,0) = \frac{12!\,0!}{6!\,0!\,6!} = \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7}{6!} = 924.$$

Aleshores

$$a_1^5 = 4 \cdot a_0^5 - a_0^6 = 4 \cdot 252 - 924 = 84, \text{etc.}$$

Si la nostra conjectura és certa la setena filera calculada a mà i calculada amb l'expressió anterior coincidirà.

Ara, per tal de completar el problema, cal provar que

$$a_n^m = f(m,n) = 4 \cdot f(m,n-1) - f(m+1,n).$$

Provem-ho per inducció sobre n:

- Quan $n = 0, a_0^m = \begin{pmatrix} 2\mathrm{m} \\ \mathrm{m} \end{pmatrix} = \dfrac{2m!}{m!\,m!} \in \mathrm{N}$.
- Suposem-ho cert par a $n-1$ i per a tot m. Aleshores és evident que $f(m,n) \in \mathrm{N}$.

Nota. Aquest mètode, inductiu, és d'una gran utilitat per tal de poder "ensumar" relacions numèriques, però en canvi l'hem desterrat gairebé del tot de les tècniques d'ensenyament i d'aprenentatge.

15. (OI 1975) Quan $4\,444^{4\,444}$ s'escriu amb notació decimal, la suma dels seus dígits és A. Sigui B la suma dels dígits d'A. Trobeu la suma dels dígits de B. (A i B s'escriuen en notació decimal.)

Solució

Sigui $N = 4\,444^{4\,444}$ i C la suma de B. Es verifica

$$N \equiv A \equiv B \equiv C \pmod 9.$$

Pel teorema petit de Fermat[2], com que $\varphi(9) = 6$ i m.c.d$(4\,444, 9) = 1$ es té que

$$4\,444^6 \equiv 1 \pmod 9.$$

D'altra banda, $4\,444 = 740 \cdot 6 + 4$ i per tant $4\,444^{4\,444} = 4\,444^{6 \cdot 740 + 4} \equiv 4\,444^4 \pmod 9$. Però $4\,444 = 493 \cdot 9 + 7$ i per tant $4\,444^4 \equiv 7^4 \equiv 7 \pmod 9$. Es té doncs

$$N \equiv A \equiv B \equiv C \equiv 7 \pmod 9.$$

Com que

$$\log 4\,444^{4\,444} = 4\,444 \cdot \log 4\,444 = 16\,210.7077\ldots$$

el nombre de xifres d'N és 16 211 i, com que $A \equiv 7 \pmod 9$, $A \leq 16\,210 \cdot 9 + 7 = 145\,897$. Per tant el nombre de xifres d'A és com a màxim 6 i $B \leq 5 \cdot 9 + 7 = 52$. El nombre de xifres de B és doncs com a màxim 2 i la primera d'elles és ≤ 5. D'on en resulta que $C \leq 14$ i, com que $C \equiv 7 \pmod 9$, $C = 7$.

Plantejament didàctic del problema

1. Demostrar que la suma A dels dígits d'un nombre N (escrit en notació decimal) i el nombre N donen el mateix romanent al dividir-los per 9.
2. Demostrar que, si el m.c.d.$(N, 9) = 1$, el romanent de dividir N^6 per 9 és 1.
3. Demostrar que $N = 4\,444^{4\,444}$ dóna com a romanent 7 al dividir-lo per 9.
4. Tenint en compte el significat de la característica del logaritme decimal d'un nombre, calcular el nombre de xifres d'$N = 4\,444^{4\,444}$.
5. Si B és la suma dels dígits d'A, quan val la suma dels dígits de B quan $N = 4\,444^{4\,444}$?

Nota. Es pot utilitzar aquest problema per introduir el concepte de equivalència i fins i tot per arribar al *teorema petit de Fermat*.

[2]Recordem que el *teorema petit de Fermat* diu que, si m.c.d$(a, m) = 1$, aleshores $a^{\varphi(m)} \equiv 1$ (mòod m), a on $\varphi(x)$ és la *funció d'Euler*, que ens dóna el nombre de números sencers $1 \leq k < m$, primers amb m.