XXIV Marató de Problemes

Mamadísimos, 3 de maig de 2020

Bloc VII - No ploreu

1009. Un problema molt interessant

En Jordi Rodríguez ha trobat un problema molt interessant i ha anat ràpidament a explicar-li a la seva amiga Patri. S'ha endut una decepció en sentir la seva resposta: "Nen, un moment, en quin moment se t'ha passat pel cap que m'importa el que m'estàs dient? T'ho dic molt en serio, tu i jo deixarem de ser amics". El problema és el següent: Sigui $f(n)$ el nombre de subconjunts de $\mathbb{Z}/n\mathbb{Z}$ tals que els seus elements sumen 0 a $\mathbb{Z}/n\mathbb{Z}$ (incloent el conjunt buit). Demostreu que:

$$f(n) = \frac{1}{n} \sum_{\substack{d|n \\ d \text{ senar}}} \varphi(d) 2^{\frac{n}{d}},$$

on $\varphi(d)$ és la funció d'Euler.

Solució. Considerem el polinomi $P(x) = (1 + x^0)(1 + x^1) \dots (1 + x^{n-1})$. Aquest polinomi és tal que quan desenvolupem tots els productes, el coeficient de x^k és el nombre de subconjunts de $\{0, 1, \dots, n-1\}$ que tenen suma k, ja que quan multipliquem els n factors, per cada factor escollim si multipliquem per 1 (no fer res) o augmentem l'exponent en una quantitat (que correspon a afegir el nombre en l'exponent al conjunt i augmentar la suma). Per tant, el valor de $f(n)$ és la suma dels coeficients que acompanyen als x^k on k és múltiple de k, perquè un conjunt té suma 0 en $\mathbb{Z}/n\mathbb{Z} \iff$ té suma múltiple d'n en $\mathbb{Z}$. Recordem però, que sabem com calcular la suma dels coeficients en posicions múltiples de n. A la llista 4, al problema 706 vam veure que $P(\omega) + P(\omega^2) + \dots + P(\omega^n)$ és n vegades la suma dels coeficients en posicions múltiple de n on $\omega = e^{\frac{2\pi i}{n}}$. Per tant, tenim:

$$n \cdot f(n) = P(\omega) + P(\omega^2) + \dots + P(\omega^n)$$

així que per acabar el problema, hem de veure que

$$P(\omega) + P(\omega^2) + \dots + P(\omega^n) = \sum_{\substack{d|n \\ d \text{ senar}}} \varphi(d) 2^{\frac{n}{d}}$$

Anem a calcular $P(\omega^j)$ per un j fixat i després farem la suma per tots els j de 1 a n.

Escriurem $\omega_j = e^{\frac{2\pi i}{n} j} = e^{\frac{a}{b} 2\pi i}$ on $a = \frac{j}{(n,j)}$ i $b = \frac{n}{(n,j)}$ de manera que a i b són coprimers i (n, j) denota el màxim comú divisor de n i j. Calculem doncs $P(\omega_j) = (1 + \omega_j^0)(1 + \omega_j^1) \dots (1 + \omega_j^{n-1})$.

Sigui $d = (n, j)$ i $Q(x) = (x - \omega_j^0)(x - \omega_j^1) \dots (x - \omega_j^{n-1}) = (x - \omega_j^0)(x - \omega_j^1) \dots (x - \omega_j^{db-1}) = ((x - \omega_j^0)(x - \omega_j^1) \dots (x - \omega_j^{b-1}))^d$ on la última igualtat és certa perquè $\omega_j^0 = \omega_j^b = \dots = \omega_j^{(d-1)b}$, $\omega_j^1 = \omega_j^{b+1} = \dots = \omega_j^{(d-1)b+1}$, i així amb tots perquè $\omega_j^b = e^{2\pi i a} = 1$. Fixem-nos ara en que les arrels de $Q(x)$ són w_j^0, w_j^1, $\dots$, w_j^{b-1} cada una amb multiplicitat d. Aquestes arrels són de la forma $e^{2\pi i \frac{ak}{b}}$ per $k = 0, 1, \ldots, b-1$. A més a més, són arrels b-èssimes de la unitat perquè si les elevem a b obtenim 1. I com que a i b són coprimers, ak conté tots els residus mòdul b i per tant, per cada parell de valors de k obtenim arrels diferents. Juntant-ho tot, això vol dir que com tenim b arrels b-èssimes de la unitat diferents, les tenim totes, i per tant, $(x-\omega_j^0)(x-\omega_j^1)\ldots(x-\omega_j^{b-1}) = x^b - 1$ i $Q(x) = (x^b-1)^d$.

Observem que volíem calcular $P(\omega_j) = (1+\omega_j^0)(1+\omega_j^1)\ldots(1+\omega_j^{n-1})$ i que com $Q(x) = (x-\omega_j^0)(x-\omega_j^1)\ldots(x-\omega_j^{n-1})$, $(-1)^n Q(-1) = (-1)^n(-1-\omega_j^0)(-1-\omega_j^1)\ldots(-1-\omega_j^{n-1}) = (1+\omega_j^0)(1+\omega_j^1)\ldots(1+\omega_j^{n-1}) = P(\omega_j)$. Utilitzant que $Q(x) = (x^b-1)^d$, deduïm que $P(\omega_j) = (-1)^n((-1)^b-1)^d = (-1)^{bd}((-1)^b-1)^d = ((-1)^b((-1)^b-1))^d = (1-(-1)^b)^d = (1-(-1)^{\frac{n}{(n,j)}})^{(n,j)}$, desfent els canvis de variable. Ara ja podem acabar el problema. Recordem que volíem veure

$$P(\omega) + P(\omega^2) + \ldots + P(\omega^n) = \sum_{\substack{d|n \\ d \text{ senar}}} \varphi(d) 2^{\frac{n}{d}}$$

Fins ara hem vist:

$$P(\omega) + P(\omega^2) + \ldots + P(\omega^n) = \sum_{j=1}^{n} (1-(-1)^{\frac{n}{(n,j)}})^{(n,j)}$$

Per fer aquesta última suma, enlloc de considerar cada valor de j, considerem cada valor que pot prendre (n,j) (ja que cada sumand només depèn d'això). Vegem primer per un d qualsevol, per quants j $(1 \leq j \leq n)$, tenim $(n,j) = d$. Si $(n,j) = d$, d divideix n i j i $(\frac{n}{d}, \frac{j}{d}) = 1$ Aleshores només hem de considerar els d que divideixen n i la quantitat de j que satisfan $(\frac{n}{d}, \frac{j}{d}) = 1$ és $\varphi(\frac{n}{d})$, perquè per tot nombre c entre 1 i $\frac{n}{d}$, existeix un j entre 1 i n tal que $c = \frac{j}{d}$. I la funció $\varphi(m)$ compta els nombres entre 1 i m coprimers amb m. Així doncs,

$$P(\omega) + P(\omega^2) + \ldots + P(\omega^n) = \sum_{j=1}^{n} (1-(-1)^{\frac{n}{(n,j)}})^{(n,j)} = \sum_{d|n} \varphi(\frac{n}{d})(1-(-1)^{\frac{n}{d}})^d$$

Ara fem el canvi de variable $d' = \frac{n}{d}$ i com sumar pels d tal que $d|n$ és sumar pels d tals que $\frac{n}{d}|n$:

$$P(\omega) + P(\omega^2) + \ldots + P(\omega^n) = \sum_{d|n} \varphi(\frac{n}{d})(1-(-1)^{\frac{n}{d}})^d = \sum_{d'|n} \varphi(d')(1-(-1)^{d'})^{\frac{n}{d'}}$$

Ara separem la suma segons la paritat de d'. Si d' és parell, aleshores $1-(-1)^{d'} = 0$ i aquest terme no contribueix a la suma. Si d' és senar $1-(-1)^{d'} = 2$ i per tant,

$$n \cdot f(n) = P(\omega) + P(\omega^2) + \ldots + P(\omega^n) = \sum_{\substack{d'|n \\ d' \text{ senar}}} \varphi(d') 2^{\frac{n}{d'}}$$

que era just el que volíem veure.