Exámen de Teoría de Números

12 de enero de 2016

Hacer 5 de los 6 problemas. La puntuación es sobre 10 puntos.

Problema 1.

a) (0,5 puntos) Hallar $d(2016)$ y $\phi(2016)$.

b) (0,5 puntos) ¿Se puede escribir 2016 como suma de dos cuadrados perfectos? ¿Y como suma de tres? ¿Y como suma de cuatro? Razonar las respuestas.

c) (1 puntos) Hallar alguna solución en enteros positivos de la ecuación diofántica $2016 = x^2 - y^2$. Calcular el número exacto de soluciones de dicha ecuación.

Solución: a) $2016 = 2^5 3^2 7$, así que $d(2016) = (1+5)(1+2)(1+1) = 36$ y $\phi(2016) = 2016 \prod_{p|2016} \left(1 - \frac{1}{p}\right) = 2016(1-1/2)(1-1/3)(1-1/7) = 576$.

b) 2016 no es suma de dos cuadrados porque $7 \equiv 3 \pmod 4$ y aparece con exponente impar en la descomposión en factores primos de 2016.

Por otra parte $2016 = 4^2 + 2000$. Como sabemos que 2000 es suma de dos cuadrados (viendo su factorización en primos), deducimos que 2016 es suma de tres cuadrados. También podemos escribir directamente $2016 = 4^2 + 20^2 + 40^2$.

Si es suma de tres cuadrados también es suma de cuatro: $2016 = 0^2 + 4^2 + 20^2 + 40^2$, aunque esto último lo podíamos haber deducido invocando directamente el Teoremad de Lagrange que afirma que todo entero positivo es suma de cuatro cuadrados.

c) Si $2016 = (x-y)(x+y)$ con $1 \leq x, y$ entonces $x - y = a$ y $x + y = b$ con $ab = 2016$, $a < b$. Es decir, $x = \frac{b+a}{2}$, $y = \frac{b-a}{2}$. Para que x e y sean enteros necesariamente a y b tienen que tener la misma paridad. Como no pueden ser los dos impares, tendrán que ser los dos pares. Resumiendo, el número de soluciones es igual al número de parejas de divisores pares a, b tales que $ab = 2016$ y $a < b$. Si hacemos $a = 2a'$ y $b = 2b'$ estamos hablando del número de parejas a', b' tales que $a'b' = 2^3 3^2 7$ tales que $a' < b'$, que exactamente igual a la mitad del número de divisores de $2^3 3^2 7$; es decir $\frac{(1+3)(1+2)(1+1)}{2} = 12$.

Por ejemplo, la solución concreta que corresponde a $a = 2,\ b = 1008$ es $2016 = 505^2 - 503^2$.

Problema 2. Se dice que un punto de coordenadas enteras (a, b, c) en $\mathbb{N}^3$ es visible desde el origen si el segmento que une el origen con (a, b, c) no contiene más puntos de coordenadas enteras que los extremos.

a) (0,5 puntos) Demostrar que

$$\sum_{d|\text{m.c.d.}(a,b,c)} \mu(d) = \begin{cases} 1, \text{ si } (a,b,c) \text{ es visible desde el origen} \\ 0 \text{ en otro caso} \end{cases}$$

b) (0,5 puntos) Demostrar que $\sum_d \frac{\mu(d)}{d^3} = 1/\zeta(3)$.

c) (1 punto) Hallar una fórmula asintótica para el número de puntos visibles desde el origen con coordenadas $1 \leq a, b, c \leq x$.

Solución: a) Si (a, b, c) no es visible desde el origen entonces existe otro punto (a', b', c') en la recta que une el origen con (a, b, c). Pero entonces $(a, b, c) = t(a', b', c')$ para algún $t \geq 2$, que sería un divisor de las tres coordenadas a, b, c. Es decir, (a, b, c) es visible desde el origen si m.c.d.$(a, b, c) = 1$. Por otra parte sabemos que $\sum_{d|n} \mu(d)$ vale 1 si $n = 1$ y que vale 0 en otro caso.

b) En general se tiene que $\frac{1}{\zeta(s)} = \prod_p \left(1 - \frac{1}{p^s}\right) = \sum_{n\geq 1} \frac{\mu(n)}{n^s}$. Otra manera de probarlo es la siguiente:

$$\zeta(3) \sum_{n\geq 1} \frac{\mu(n)}{n^3} = \sum_{m\geq 1} \frac{1}{m^3} \sum_{n\geq 1} \frac{\mu(n)}{n^3} = \sum_{n,m\geq 1} \frac{\mu(n)}{(nm)^3} = \sum_k \frac{\sum_{n|k} \mu(n)}{k^3} = 1.$$

c) Llamemos $V(x)$ al número de puntos visibles con coordenadas $1 \leq a, b, c \leq x$. Utilizando los apartado a) y b) tenemos que

$$\begin{aligned} V(x) &= \sum_{1\leq a,b,c\leq x} \sum_{d|\text{m.c.d.}(a,b,c)} \mu(d) = \sum_{d\leq x} \mu(d) \sum_{\substack{1\leq a,b,c\leq x \\ d|a,\ d|b,\ d|c}} 1 = \sum_{d\leq x} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor^3 \\ &= \sum_{d\leq x} \mu(d) \left(\frac{x}{d} + O(1)\right)^3 = x^3 \sum_{d\leq x} \frac{\mu(d)}{d^3} + O\left(x^2 \sum_{d\leq x} \frac{1}{d^2}\right) \\ &= x^3 \sum_{d=1}^{\infty} \frac{\mu(d)}{d^3} + O\left(x^3 \sum_{d>x} \frac{1}{d^3}\right) + O(x^2) = \frac{x^3}{\zeta(3)} + O(x^2), \end{aligned}$$

ya que $\sum_{d>x} \frac{1}{d^3} = O(1/x^2)$ y $\sum_{d\leq x} \frac{1}{d^2} = O(1)$.

Problema 3.

a) (1 punto) Caracterizar los primos p tales que la congruencia $x^2 + 3x + 1 \equiv 0 \pmod{p}$ tiene solución.

b) (1 punto) Demostrar que existen infinitos primos p para los que dicha congruencia tiene solución.

Pista para b): Utilizar un argumento similar al que utilizó Euclides para demostrar la existencia de infinitos números primos.

Solución: a) Es claro que para $p = 2$ la congruencia no tiene solución. Para $p \neq 2$ la congruencia es equivalente a $4(x^2+3x+1) \equiv 0 \pmod{p}$, que, completando cuadrados, es a su vez equivalente a la congruencia $(2x + 3)^2 \equiv 5 \pmod{p}$. Esta congruencia tiene solución para $p = 5$. Para $p \neq 5$ tiene solución si y sólo si 5 es un residuo cuadrático módulo p. La ley de reciprocidad cuadrática nos dice que

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) (-1)^{\frac{(p-1)(5-1)}{4}} = \left(\frac{p}{5}\right) = \begin{cases} 1 \text{ si } p \equiv 1, 4 \pmod 5 \\ 0 \text{ si } p \equiv 2, 3 \pmod 5 \end{cases}.$$

Resumiendo, la congruencia tiene solución para $p = 5$ y para los primos $p \equiv 1, 4 \pmod 5$.

b) Supongamos que la congruencia sólo tiene solución para un número finito de primos $p_1, \ldots, p_k$. Consideremos el entero $N = p_1 \cdots p_k$. Es claro que $N^2 + 3N + 1$ no es divisible por ninguno de los primos $p_1, \ldots, p_k$; así que tendrá que ser divisible por algún otro primo p y la congruencia $x^2 + 3x + 1 \equiv 0 \pmod p$ tendrá solución para ese primo p, contradiciendo los supuesto.

Problema 4. Para $s > 1$ sea $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

a) (0,5 puntos) Demostrar que $\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$.

b) (0,5 puntos) Demostrar que $\zeta(s) = \zeta(2s) \prod_p \left(1 + \frac{1}{p^s}\right)$.

c) (1 punto) Utilizar el apartado b) y la desigualdad $\log(1 + t) \leq t$ para $t \geq 0$ para demostrar que la suma de los inversos de los números primos es infinita.

Solución: a)

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \sum_n \frac{1}{n^s}.$$

En el último paso hemos utilizado que para $n \geq 2$, existe una sóla manera de escribir n como producto de primos (por eso aparece 1 en el numerador).

b)

$$\begin{aligned}
\zeta(2s) \prod_p \left(1 + \frac{1}{p^s}\right) &= \prod_p \left(1 - \frac{1}{p^{2s}}\right)^{-1} \prod_p \left(1 + \frac{1}{p^s}\right) \\
&= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \prod_p \left(1 + \frac{1}{p^s}\right)^{-1} \prod_p \left(1 + \frac{1}{p^s}\right) \\
&= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s).
\end{aligned}$$

c) Tomando logaritmos en b) tenemos que

$$\log \zeta(s) - \log \zeta(2s) = \sum_p \log \left(1 + \frac{1}{p^s}\right) \leq \sum_p \frac{1}{p^s}.$$

Cuando $s \to 1$ el lado izquierdo tiende a infinito porque $\zeta(s)$ tiene a infinito y $\zeta(2s)$ tiende a $\zeta(2)$, mientras que el lado derecho tiende a la suma de los inversos de los primos.

Problema 5.

a) (1 punto) Demostrar que el número

$$c = \sum_{p \text{ primo}} \frac{1}{p!}$$

es un número irracional.

b) (1 punto) Hallar el comportamiento asintótico de

$$\sum_{n \leq x} |\sin(2\pi cn)|$$

cuando $x \to \infty$.

Solución: a) Sea p_n el primo n-ésimo y consideemos el número racional $\frac{a_n}{b_n} = \sum_{k=1}^{n} \frac{1}{p_n!}$. Es claro que $b_n = p_n!$ y que

$$\begin{aligned} \left| c - \frac{a_n}{b_n} \right| &= \sum_{k \geq n+1} \frac{1}{p_k!} \leq \frac{1}{p_{n+1}!} + \frac{1}{(p_{n+1}+1)!} + \cdots \\ &\leq \frac{1}{p_{n+1}!} \left(1 + \frac{1}{p_{n+1}+1} + \frac{1}{(p_{n+1}+1)(p_{n+1}+2)} + \cdots \right) \\ &\leq \frac{1}{p_{n+1}!} \left(1 + \frac{1}{2} + \frac{1}{4} + \cdots \right) \leq \frac{2}{p_{n+1}!}. \end{aligned}$$

Por lo tanto,

$$b_n \left| c - \frac{a_n}{b_n} \right| \leq \frac{2b_n}{p_{n+1}!} = \frac{2p_n!}{p_{n+1}!} \to 0,$$

lo que demuestra que c es irracional.

b) Como c es irracional, la sucesión $\{cn\}$ está uniformemente distribuida en el intervalo $[0, 1]$ y por lo tanto

$$\sum_{n \leq x} f(\{cn\}) \sim x \int_0^1 f(t)dt$$

para toda función continua a trozos $f(t)$. En nuestro caso la función $f(t) = |\sin(2\pi t)|$ satisface que $f(\{cn\}) = f(cn)$ y entonces tenemos que

$$\sum_{n \leq x} f(cn) = \sum_{n \leq x} f(\{cn\}) \sim x \int_0^1 |\sin(2\pi t)|dt = \frac{2}{\pi} x.$$

Problema 6. Sea A un conjunto de n números enteros positivos.

a) (1 punto) Demostrar que las desigualdades

$$2n - 1 \leq |A \cdot A|, |A + A| \leq \frac{n(n+1)}{2}.$$

b) (1 punto) Demostrar que para todo n existe un conjunto de enteros positivos A con $|A| = n$ tal que $|A \cdot A| = 2n - 1$ y $|A + A| = n(n+1)/2$.

Solución: a) Lo demostramos sólo para $|A \cdot A|$. Para $|A + A|$ es exactamente igual cambiando la operación producto por la suma.

Sea $A := a_1 < \cdots < a_n$. Los siguientes $2n - 1$ enteros están en $A \cdot A$ y son distintos:

$$a_1a_1 < a_1a_2 < \cdots < a_1a_n < a_2a_n < \cdots a_na_n.$$

Esto demuestra que $|A \cdot A| \geq 2n-1$. Para la cota superior, obervemos que todos los productos son de la forma a_ia_j con $1 \leq i \leq j \leq n$ y que hay exactamente $n(n+1)/2$ maneras de elegir estos índices i, j. Para convencernos del todo, el número de índices i, j con $i \neq j$ es $\binom{n}{2}$ y el número de índices i, j con $i = j$ es n, Así que $\binom{n}{2} + n = n(n+1)/2$.

b) Por ejemplo consideremos el conjunto $A = \{10^1, \ldots, 10^n\}$. Es claro que $A \cdot A = \{10^2, \ldots, 10^{2n}\}$. Por otra parte todas las sumas $10^i + 10^j$, $i \leq j$ son distintas y por lo tanto $|A + A| = n(n+1)/2$. Para convencernos del todo de que esas sumas son distintas, supongamos que $10^i + 10^j = 10^{i'} + 10^{j'}$ con $i' < i \leq j < j'$. Entonces $10^{j'} \leq 10^i + 10^j \leq 10^{j'-1} + 10^{j'-1} = \frac{1}{5}10^{j'}$, lo que es claramente falso.