Exámen de Teoría de Números

25 de Enero de 2010

Las notas saldrán el 29 de Enero y la revisión será el miércoles 3 de Febrero, a las 10:00 en el C-XV-304. La solución del examen aparecerá en mi página web.

1. a) Demostrar que $\alpha = \sum_{p \text{ primo}} \frac{1}{p!}$ es un número irracional. (La demostración es muy similar a la que hicimos para el número e)

b) Hallar el comportamiento asintótico de $\sum_{k=1}^{n} \cos^2(2\pi k\alpha)$.

Solución: a) Supongamos que $\alpha = \frac{a}{b}$ y consideremos la sucesión infinita de fracciones $\frac{P_n}{Q_n} = \sum_{i=1}^{n} \frac{1}{p_i!}$. El mínimo común múltiplo de los denominadores de esta suma es $p_n!$, así que $Q_n \leq p_n!$.

Por una parte, y como $\alpha \neq \frac{P_n}{Q_n}$ tenemos que

$$\left|\frac{a}{b} - \frac{P_n}{Q_n}\right| \geq \left|\frac{aQ_n - bP_n}{bQ_n}\right| \geq \frac{1}{bQ_n} \geq \frac{1}{bp_n!}$$

Por otra parte

$$\left|\alpha - \frac{P_n}{Q_n}\right| = \sum_{i=n+1}^{\infty} \frac{1}{p_{n+1}!} \leq \frac{2}{p_{n+1}!} \leq \frac{1}{p_n! p_{n+1}}.$$

De las dos desigualdades obtenemos que $b \geq p_{n+1}$, lo cual no puede ser cierto para todo n.

b) Sabemos que si α es irracional entonces la sucesión cuyo término general es $a_k = \{k\alpha\}$ está uniformemente distribuida en $[0, 1)$. Por otra parte, si una sucesión a_k está uniformemente distribuida en $[0, 1)$ se tiene que $\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} f(a_k) = \int_0^1 f(t)dt$. Aplicando este resultado a la función $f(t) = \cos^2(2\pi t)$ y observando que $f(t) = f(\{t\})$ tenemos que

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \cos(2\pi k\alpha) = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \cos(2\pi\{k\alpha\}) = \int_0^1 \cos^2 t dt = 1/2,$$

y por tanto $\sum_{k=1}^{n} \cos^2(2\pi k\alpha) \sim n/2$.

2. Sea $A = \{n \in \mathbb{N} : \ (n, 2010) = 1\}$.

a) Demostrar que $A(x) = \frac{\phi(2010)}{2010} x + O(1)$.

b) Demostrar que existen dos constantes c_1, c_2 tales que

$$\sum_{\substack{n\leq x,\\ (n,2010)=1}} \frac{1}{n} = c_1 \log x + c_2 + O\left(\frac{1}{x}\right).$$

Solución: a) (primera manera) En cada intervalo de lo longitud 2001 hay exactamente $\phi(2010)$ elementos primos con 2010. Entonces $A(2010m) = \phi(2010)m$ para todo $m \in \mathbb{N}$.

Sea m tal que $2010m \le x < 2010(m+1)$ Entonces

$$\begin{aligned} A(x) &= A(2010m) + O(1) = \phi(2010)m + O(1) \\ &= \phi(2010)\Big(\frac{x}{2010} + O(1)\Big) + O(1) = \frac{\phi(2010)}{2010}x + O(1) \end{aligned}$$

a)(segunda manera)

$$\begin{aligned} A(x) &= \sum_{n\le x}\sum_{d\mid(n,2010)}\mu(d) = \sum_{d\mid 2010}\mu(d)\sum_{\substack{n\le x\\ d\mid n}}1 = \sum_{d\mid 2010}\mu(d)\left[\frac{x}{d}\right] \\ &= \sum_{d\mid 2010}\mu(d)\frac{x}{d} - \sum_{d\mid 2010}\mu(d)\left\{\frac{x}{d}\right\} = x\sum_{d\mid 2010}\frac{\mu(d)}{d} + O(1) \end{aligned}$$

y la demostración se acaba utilizando la fórmula $\phi(n) = n\sum_{d\mid n}\frac{\mu(d)}{d}$.

b) Llamemos a_n a la función aritmética que vale 1 si $(n, 2010) = 1$ y que vale 0 en caso contrario. Por el apartado a) sabemos que $A(t) = \sum_{n\le t} a_n = ct + E(t)$ donde $c = \frac{\phi(2010)}{2010}$ y $E(t) = O(1)$. Utilizando la identidad de Abel tenemos

$$\begin{aligned} \sum_{\substack{n\le x,\\ (n,2010)=1}}\frac{1}{n} &= \sum_{n\le x}\frac{a_n}{n} = \frac{A(x)}{x} + \int_1^x \frac{A(t)dt}{t^2} \\ &= \frac{cx + O(1)}{x} + \int_1^x \frac{cdt}{t} + \int_1^x \frac{E(t)}{t^2} \\ &= c + O(1/x) + c\log x + \int_1^\infty \frac{E(t)dt}{t^2} - \int_x^\infty \frac{E(t)dt}{t^2} \\ &= c_1\log x + c_2 + O(1/x) \end{aligned}$$

donde $c_1 = c$ y $c_2 = c + \int_1^\infty \frac{E(t)dt}{t^2}$

3. Sea $f(x) = x^2 + x + 1$.

a) Decidir razonadamente si la congruencia $f(x) \equiv 0 \pmod{91577}$ tiene solución. (Observación: el número 91577 es primo).

b) Demostrar que la congruencia $f(x) \equiv 0 \pmod{p}$ tiene solución para infinitos primos p.

Solución:

a) Si p es un primo impar la congruencia $x^2 + x + 1 \equiv 0 \pmod{p}$ es equivalente a la congruencia $4x^2 + 4x + 4 \equiv 0 \pmod{p} \iff (2x+1)^2 + 3 \equiv 0 \pmod{p}$. Así que la congruencia tendrá solución si y sólo si $\left(\frac{-3}{p}\right) = 1$. Por la ley de reciprocidad cuadrática tenemos que

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

Como $p = 91577 \equiv 2 \pmod 3$, entonces la congruencia no tiene solución.

b) Supongamos que sólo tiene solución para un número finito de primos $p_1, \ldots, p_k$. Consideremos el número $f(p_1 \cdots p_k)$. Claramente no es divisible por ninguno de

esos primos, luego será divisible por otro primo p distinto y $x = p_1 \cdots p_k$ será una solución de la congruencia $f(x) \equiv 0 \pmod{p}$.

4. Sea $s = \sigma + it,\ \sigma > 1$ y $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

a) Demostrar que $\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$.

b) Demostrar que $\frac{1}{|\zeta(s)|} \leq \zeta(\sigma)$ y deducir que la función $\zeta(s)$ no se anula en $\Re(s) > 1$.

Solución: a) (primera manera): Como $\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$ entonces $\frac{1}{\zeta(s)} = \prod_p \left(1 - \frac{1}{p^s}\right)$. El resultado de la suma será el sumatorio sobre donde los denominadores son productos de primos distintos elevados a s y los coeficientes serán $(-1)^k$, donde k es el números de primos distintos que dividen a estos enteros. Es decir, los sumandos serán de la forma $\frac{\mu(n)}{n^s}$.

a) (segunda manera).

$$\left(\sum_{m=1}^{\infty} \frac{1}{m^s}\right)\left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right) = \sum_{n,m} \frac{\mu(n)}{(nm)^s} = \sum_{k=1}^{\infty} \frac{\sum_{n|k} \mu(n)}{k^s} = 1$$

porque $\mu(1) = 1$ y $\sum_{n|k} \mu(n) = 0$ si $k > 1$. Así que

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\sum_{m=1}^{\infty} \frac{1}{m^s}} = \frac{1}{\zeta(s)}.$$

b)

$$\frac{1}{|\zeta(s)|} = \left|\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right| \leq \sum_{n^1}^{\infty} \frac{1}{|n^s|} = \sum_{n=1}^{\infty} \frac{1}{n^\sigma} = \zeta(\sigma)$$

Como $\zeta(\sigma) < \infty$ para todo $\sigma > 1$, entonces $\zeta(s)$ no se puede anular en ningún $s = \sigma + it$ cuando $\sigma > 1$.

5. Sea g una raíz primitiva de $\mathbf{F}_p$.

a) Demostrar que si $e_1 \not\equiv 0 \pmod{p-1}$ y $e_2 \not\equiv 0 \pmod{p}$ entonces existen dos únicos $x, y \in \mathbf{Z}_{p-1}$ tales que

$$\begin{cases} x - y \equiv e_1 \pmod{p-1} \\ g^x - g^y \equiv e_2 \pmod{p} \end{cases}$$

(*Observación: Tenéis que explicar bien donde se utiliza que g es una raíz primitiva*)

b) Demostrar que si $A \subset \mathbf{Z}_{p-1} \times \mathbf{F}_p$ es un conjunto de Son entonces $|A| \leq p-1$ y utilizar a) para demostrar que el conjunto $A = \{(x, g^x) :\ x \in \mathbf{Z}_{p-1}\} \subset \mathbf{Z}_{p-1} \times \mathbf{F}_p$ es un conjunto de Sidon.

Solución: a) La primera congruencia implica que $g^{x-y} \equiv g^{e_1} \pmod{p} \implies g^x \equiv g^y g^{e_1} \pmod{p}$. Sustituyendo en la segunda congruencia tenemos que $g^y(g^{e_1} - 1) \equiv e_2 \pmod{p}$, Como $e_1 \neq 0$ y g es una raíz primitiva, entonces $g^{e_1} - 1 \not\equiv 0 \pmod{p}$ y podemos escribir

$$g^y \equiv e_2(g^{e_1} - 1)^{-1} \pmod{p}.$$

Como la parte de la derecha es distinta de cero, y g es una raíz primitiva, existirá un único y que satisfaga la ecuación. Ese valor de y y la primera congruencia determinan el valor de x.

b) El número total de diferencias $a - a' : \ a, a' \in A, \ a \neq a'$ es exactamente $|A|(|A|-1)$. Como todas estas diferencias son distintas y diferentes de $(0, 0)$ entonces $|A|(|A| - 1) \leq p(p - 1) - 1$. De aquí ya vemos que si $|A| \geq p$ obtenemos una contradicción.

El conjunto del enunciado es un conjunto de Sidon porque el apartado a) nos muestra que una diferencia sólo puede venir como diferencia de dos únicos elementos del conjunto.