Exámen de Teoría de Números

8 de mayo de 2015

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

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

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

b) (0,5 puntos) Demostrar que $\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$.

c) (0.5 puntos) Demostrar que $\frac{1}{|\zeta(s)|} \leq \zeta(\sigma)$.

d) (0.5 puntos) Deducir de lo anterior que $\zeta(s) \neq 0$ para $\sigma > 1$.

Solución: a)

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

Todos los productos y las sumas que aparecen son convergentes porque $\sigma > 1$.

b) Primera forma:

$$\frac{1}{\zeta(s)} = \prod_p \left(1 - \frac{1}{p^s}\right) = \sum_n \frac{\mu(n)}{n^s}.$$

En el último paso hemos utilizado que en la suma sólo aparecen el 1 los n que son producto de primos distintos y que el signo de la fracción es 1 o -1 dependiendo de si el número de primos es par o impar. La función $\mu(n)$ es precisamente la que nos da esos valores.

Segunda forma:

$$\zeta(s) \left(\sum_{l=1}^{\infty} \frac{\mu(l)}{l^s}\right) = \left(\sum_{r=1}^{\infty} \frac{1}{r^s}\right) \left(\sum_{l=1}^{\infty} \frac{\mu(l)}{l^s}\right) = \sum_{r,l} \frac{\mu(l)}{(rl)^s} = \sum_{n^s} \frac{\sum_{l|n} \mu(l)}{n^s} = 1.$$

En el último paso hemos utilizado que $\sum_{l|n} \mu(l) = 0$ para $n > 1$ y que vale 1 para $n = 1$.

c)

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

En la penúltima igualdad hemos utilizado que $|n^{\sigma+it}| = |n^\sigma||n^{it}| = n^\sigma$.

d) Como $\zeta(\sigma) < \infty$ para $\sigma > 1$, del apartado c) deducimos que $|\zeta(s)| \geq \frac{1}{\zeta(\sigma)} > 0$.

Problema 2. Sea $s(n) = \prod_{p|n} \left(1 - \frac{1}{p}\right)$.

a) (0.5 puntos) Demostrar que $s(n) = \sum_{d|n} \frac{\mu(d)}{d}$.

b) (0.5 puntos) Demostrar que $\sum_{n \leq x} s(n) = \frac{x}{\zeta(2)} + O(\log x)$.

c) (1 punto) Demostrar que $\sum_{n\leq x}\frac{s(n)}{n}=\frac{\log x}{\zeta(2)}+C+O((\log x)/x)$ para una constante C.

Solución: a) Primera forma: Al desarrollar el producto los denominadores de las fracciones que salen en el sumatorio son el 1 y los divisores de n que son producto de primos distintos. El coeficiente de esas fracciones es 1 o -1 dependiendo de si el número de factores rimos es par o impar. Eso coeficiente, como ocurra en el aparado b) del problema 1, es la función de Moebius.

Segunda forma: Observar que $s(n)=\phi(n)/n$. Como $\phi(n)$ es multiplicativa entonces $s(n)$ también lo es. Por otra parte, como $\mu(n)/n$ es multiplicativa, entonces $\sum_{d|n}\mu(d)/d$ también lo es. Así que para ver que $s(n)=\sum_{d|n}\mu(d)/d$ es suficiente con ver que coinciden para las potencias de los primos:

$$s(p^\alpha)=1-\frac{1}{p},\qquad \sum_{d|p^\alpha}\mu(d)/d=1-\frac{1}{p}.$$

Problema 3. a) (0.5 puntos) Demostrar que para $p\neq 3$ primo, la congruencia $3x^2+2x+2\equiv 0\pmod p$ es equivalente a la congruencia $(3x+1)^2\equiv -5\pmod p$.

b) (0.5 puntos) Demostrar que para $p=2,3,5$ la congruencia $3x^2+2x+2\equiv 0\pmod p$ tiene una única solución.

a) (1 puntos) Hallar, para cada primo $p\neq 2,3,5$, el número de soluciones de la congruencia $3x^2+2x+2\equiv 0\pmod p$.

Solución: a) Multiplicamos por 3 para multiplicar cuadrados. Como $p\neq 3$ la congruencia es equivalente a

$$9x^2+6x+6\equiv (3x+1)^2+5\equiv \quad \pmod p.$$

b) Es tan sencillo como comprobar a mano cada uno de los casos. Las soluciones son $x=1$ para $p=2$, $x=2$ para $p=3$ y $x=3$ para $p=5$.

c) Utilizamos el apartado a)y el hecho de que $p\neq 3$ para estudiar el número de soluciones de $(3x+1)^2\equiv -5\pmod p$. Si llamamos $y=3x+1$, es claro que si y es una solución entonces $-y$ también lo es. Podría ocurrir que $y=1$, es decir que $3x+1\equiv -3x-1\pmod p$. Pero entonces tendríamos que $6x+2\equiv 0\pmod p$. Como $p\neq 2$ entonces $3x+1\equiv 0\pmod p$, pero como $p\neq 5$ entonces no es cierto que $(3x+1)^2\equiv -5\pmod p$. Resumiendo, si $p\neq 2,3,5$ entonces la congruencia tiene 0 o 2 soluciones.

Ahora utilizamos la ley de reciprocidad cuadrática para clasificar los primos p para los que tiene dos soluciones:

$$\left(\frac{-5}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{1}{5}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{5}{p}\right).$$

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

Combinando los dos casos mediante el Teorema chino del resto se tiene que

$$\left(\frac{-5}{p}\right) = \begin{cases} 1 \text{ si } p \equiv 1,3,7,9 \pmod{20} \\ -1 \text{ si } p \equiv 11,13,17,19 \pmod{20} \end{cases}.$$

Es decir, si $p \neq 2,3,5$ y $p \equiv 1,3,7$ ó $9 \pmod{20}$ entonces la congruencia tiene dos soluciones. Y si $p \neq 2,3,5$ y $p \equiv 11,13,17$ ó $19 \pmod{20}$ no tiene ninguna solución.

Problema 4. a) (1 punto) Demostrar que la ecuación $x^2+y^2=7z^2$ no tiene soluciones en enteros excepto la solución $x=y=z=0$.

b) b) (1 punto) Hallar el número de soluciones en enteros positivos de la ecuación $x^2-y^2=3\cdot 5\cdot 7\cdot 9\cdot 11\cdot 13\cdot 15$.

Solución: a) Por el método del descenso. Supongamos que $(x,y,z)\neq(0,0,0)$ es la solución mínima de esta ecuación. En particular tendríamos que $x^2+y^2\equiv 0 \pmod 7$. Si $y \not\equiv 0 \pmod 7$ entonces $(xy^{-1})^2 \equiv -1 \pmod 7$ lo cual es imposible porque -1 no es un residuo cuadrático módulo 7. Así que $y\equiv 0 \pmod 7$ y por lo tanto $x \equiv 0 \pmod 7$. Podeos escribir $y=7y'$ y $x=7x'$ con lo que tenemos que $7(x'^2+y'^2)=z^2$ y tenemos que $z=7z'$. Pero entonces $x'^2+y'^2=7z'^2$ es una solución más pequeña que (x,y,z) y que también cumple que $(x',y',z')\neq(0,0,0)$.

b) Llamemos $N=3\cdot 5\cdot 7\cdot 9\cdot 11\cdot 13\cdot 15=3^4\cdot 5^2\cdot 7\cdot 11\cdot 13$.

Si $x^2-y^2=N$ entonces $x+y=d$ y $x-y=N/d$ para un divisor d de N mayor que N/d (para que $y>0$). Tendremos entonces que $x=(d+N/d)/2$ y $y=(d-N/d)/2$. Como N es impar todos sus divisores tamién lo son y por lo tanto x e y son enteros positivos. La mitad de los divisores d de N son mayores que N/d, así que el número de soluciones será exactamente la mitad del número de divisores de N, que es $\tau(N)/2=5\cdot 3\cdot 2\cdot 2\cdot 2/2=60$.

Problema 5. Sea $l(\alpha)=\lim_{n\to\infty}\frac{1}{n}\sum_{m\leq n}\frac{1}{(\alpha m)+1}$, donde (αm) es la parte fraccionaria de αm. Hallar $l(\alpha)$ para

a) (1 punto) $\alpha = 1/\sqrt{p}$, con p primo. b) (1 punto) $\alpha=1/p$, con p primo.

Solución: a) Como p no es un cuadrado entero entonces $1/\sqrt{p}$ es irracional y la sucesión $(m/\sqrt{p})$ está uniformemente distribuida en el intervalo $[0,1)$. Eso implica en particular que

$$\lim_{n\to\infty}\frac{1}{n}\sum_{m\leq n}\frac{1}{(m/\sqrt{p})+1} = \int_0^1 \frac{dt}{t+1} = \log 2.$$

b) Observemos que si $m\equiv r \pmod p$ entonces $(m/p)=r/p$. Así que

$$\sum_{m\leq n}\frac{1}{(m/p)+1} = \sum_{r=0}^{p-1}\sum_{\substack{m\leq n\\ m\equiv r \pmod p}}\frac{1}{r/p+1} = \sum_{r=0}^{p-1}(n/p+O(1))\frac{1}{r/p+1}$$

$$= n\sum_{r=0}^{p-1}\frac{1}{r+p}+O(p).$$

Como p es fijo, dividiendo entre n y haciendo tender n a infinito tenemos que nuestro límite es $\sum_{r=0}^{p-1} \frac{1}{r+p}$.

Problema 6. a) (1 puntos) Demostrar que si A es un conjunto de Sidon en $\mathbf{Z}_p \times \mathbf{Z}_p$, entonces $|A| \leq p$

b) (1 punto) Demostrar que si $p \neq 2$ es primo, el conjunto $A = \{(x, x^2) : x \in \mathbf{Z}_p\}$ es un conjunto de Sidon en $\mathbf{Z}_p \times \mathbf{Z}_p$ con p elementos.

Solución: a) Si $|A| \geq p+1$ el número de diferencias no nulas sería $|A|(|A|-1) \geq p(p+1)$. Pero eso es imposible porque sobrepasaríamos el número de elmentos no nulos del grupo, que es $p^2 - 1$.

b) Hay que ver que si $(x, y) \neq (0, 0)$, la ecuación $(a, a^2) - (b, b^2) = (x, y)$ en $\mathbf{Z}_2 \times \mathbf{Z}_2$ determina los valores a y b. Pero esa iguualdad es equivalente a las congruencias $a - b \equiv x \pmod{p}$ y $a^2 - b^2 \equiv y \pmod{}$. Sustituyendo a en la segunda llegamos a $(b + x)^2 - b^2 \equiv y \pmod{p}$; es decir, $2bx \equiv y - x^2 \pmod{p}$. Si $x = 0$ entonces $a = b$ y por lo tanto $y = 0$ lo cual está descartado. Como $p \neq 2$ tenemos entonces que $b \equiv (2x)^{-1}(y - x^2) \pmod{p}$. El valor de b determina el valor de a.