Tarea de Teoria de Números 2014
Entrenamiento XXVIII OMM Zacatecas
Adrián Celes
Julio 2014

Hola. He aquí la tarea de Teoría de Números para avanzados. La tarea debe de entregarse al inicio de la primera sesión de su próximo entrenamiento en Agosto. Como ya les habían comentado, son 10 problemas los cuáles hay qué hacerlos todos. Les comento también que yo calificaré la tarea de Teoría de Números :).

Como ya lo saben, es bien importante el trabajo que hagan ustedes en casa, nosotros como entrenadores tenemos la tarea de darles herramientas y consejos para la resolución de problemas, pero justo de eso es lo que se tienen qué encargar ustedes, de resolver problemas. Procuren escribir sus ideas en cada problema aunque no lleguen a la solución: Es mejor tener 2 o 3 puntos que 0 puntos.

Les recuerdo mi correo: adrianceles@cimat.mx, en el cuál pueden preguntarme dudas de redacción en los problemas de tarea, comentarme alguna idea, incluso preguntarme si van bien o mal en su procedimiento o alguna sugerencia sobre cómo proceder de donde se quedaron, lo importante es que sigan trabajando en su tarea.

Con respecto al problema 10, son incisos cuya respuesta es corta, no se espanten. Finalmente, les deseo suerte en este proceso rumbo al nacional de la OMM

Adrián Celes.

Enunciados de los Problemas

1. Sean $a, b \in \mathbb{N}$ y supongamos que $a \mid b^2,\ b^2 \mid a^3,\ a^3 \mid b^4,\ b^4 \mid a^5,\ \ldots,$ demuestra que $a = b$.

2. - Sean n, a, b enteros positivos. Demuestra que
   $$n^{mcd(a,b)} - 1 = mcd(n^a - 1, n^b - 1)$$
   - Sean a y b enteros positivos. Usando lo anterior, demuestra que el máximo común divisor de $2^a + 1$ y $2^b + 1$ divide a $2^{mcd(a,b)} + 1$.

3. Demuestra que si n, m son enteros positivos con $n \geq m$, entonces
   $$\frac{mcd(m,n)}{n}\binom{n}{m}$$
   es un número entero.

4. Encuentra todas las tripletas (m, n, l) de enteros positivos tales que
   $$m + n = mcd(m,n)^2, \quad m + l = mcd(m,l)^2, \quad n + l = mcd(n,l)^2$$

5. Encuentra todas las parejas de enteros positivos (a, b) con la propiedad de que $ab + a + b$ divide a $a^2 + b^2 + 1$.

6. Sea $p > 3$ un número primo y sea
   $$\frac{r}{ps} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p}$$
   Demuestra que $p^3 | r - s$.

7. Para cualquier primo p, demuestra que $p^{p+1}(p+1)^p$ no es un cuadrado perfecto.

8. Sea p un número primo y n un entero tal que $1 \leq n \leq p$. Demuestra que

$$(p-n)!(n-1)! \equiv (-1)^n \pmod{p}$$

9. - Juan y Carlos juegan un juego en el cuál ellos por turnos remueven piedras de un montón que inicialmente tiene n piedras. El número de piedras que ellos remueven en cada turno debe ser uno menos que un número primo. El ganador es el jugador que toma la última piedra. Juan juega primero. Demuestra que existen infinitos números n tales que Carlos tiene una estrategia ganadora. (Por ejemplo, si $n = 17$, Juan toma 6 dejando 11, luego Carlos toma 1 dejando 10, luego Juan toma las 10 piedras restantes para ganar.)
   - Un punto latiz $(x, y) \in \mathbb{Z}^2$ se dice *visible desde el origen* si $mcd(x, y) = 1$. Demuestra que para cualquier entero positivo n existe un punto latiz (a, b) cuya distancia a cada punto visible es mayor que n.

Para el problema 10, necesitaremos las siguientes definiciones y proposiciones:

Definición. Una función aritmética (i.e., una función de la forma $f : \mathbb{N} \to \mathbb{C}$) se dice *multiplicativa* si para cada par de primos relativos m y n, se satisface que $f(mn) = f(m)f(n)$. Si más aún, se satisface la ecuación anterior para cualquier par de enteros, decimos que la función es *completamente multiplicativa*.

Claramente para definir una función multiplicativa, basta definir los valores que toma la función en potencias de primos.

Definición. Dada una sucesión $\{a_n\}_{n=1}^{\infty}$, definimos

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

la *Serie de Dirichlet* de la sucesión $\{a_n\}_{n=1}^{\infty}$.

Proposición. Si $F(s)$ es la serie de Dirichlet de $\{a_n\}_{n=1}^{\infty}$, y $G(s)$ es la serie de Dirichlet de $\{b_n\}_{n=1}^{\infty}$, entonces $F(s)G(s)$ es la serie de Dirichlet de la sucesión $\{c_n\}_{n=1}^{\infty}$ definida como

$$\sum_{d|n} a_d b_{\frac{n}{d}}$$

Definición. La serie de Dirichlet de la sucesión constante $\{1\}_{n=1}^{\infty}$ es llamada la *Función Zeta de Riemann*, y es denotada por $\zeta(s)$.

Definición. Definamos la función multiplicativa $\mu(n)$ cuyos valores en las potencias de primos están dadas por

$$\mu(p^a) = \begin{cases} 1 & \text{si } a = 0 \\ -1 & \text{si } a = 1 \\ 0 & \text{si } a \geq 2 \end{cases}$$

La función $\mu(n)$ es llamada la *Función de Möbius*. La serie de Dirichlet asociada a $\{\mu(n)\}_{n=1}^{\infty}$ la denotamos por $M(s)$.

Definición. Sean f y g dos funciones aritméticas. Definimos su *convolución* como la función aritmética

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d)$$

Proposición. Si f y g son dos funciones multiplicativas, su convolución también lo es.

10. Demuestra los siguientes enunciados:

    - Sea f una función multiplicativa. Se satisface la siguiente identidad:

    $$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \{1 + f(p)p^{-s} + f(p^2)p^{-2s} + f(p^3)p^{-3s} + \cdots\}$$

    donde el producto se extiende sobre todos los números primos.

    - Demuestra la célebre *Fórmula de Inversión de Möbius*: Sea $f(n)$ una función multiplicativa. Definamos $g(n) = \sum_{d|n} f(d)$. Entonces

    $$f(n) = \sum_{d|n} \mu(d)g(n/d)$$

    (Hint: Demuestra que $M(s)\zeta(s) = \zeta(s)M(s) = 1$).

    - Demuestra (usando un argumento combinatorio) que

    $$n = \sum_{d|n} \varphi(d)$$

    - Concluye que φ es multiplicativa.
    - Deduce una fórmula explícita para $\varphi(n)$.
    - Si $x \in \mathbb{R}$, demuestra la identidad

    $$\sum_{n=1}^{\infty} \frac{\mu(n)x^n}{1 - x^n} = x$$