Soluciones comentadas del primer parcial

MODELO 1

1) Calcular $\left(\frac{3}{p}\right)$, con p primo impar, en términos de las clases de congruencias de p módulo 12.

Si $p = 3$ el símbolo es cero. En otro caso, por la ley de reciprocidad cuadrática:

$$p \equiv 1\ (4)\ \Rightarrow\ (\frac{3}{p}) = (\frac{p}{3}) = \begin{cases} 1 & \text{si } p \equiv 1\ (3) \\ -1 & \text{si } p \equiv -1\ (3) \end{cases}$$

y

$$p \equiv -1\ (4)\ \Rightarrow\ (\frac{3}{p}) = -(\frac{p}{3}) = \begin{cases} 1 & \text{si } p \equiv -1\ (3) \\ -1 & \text{si } p \equiv 1\ (3) \end{cases}$$

Entonces para $p > 3$ el símbolo es 1 si y sólo si $p \equiv \pm 1\ (12)$, ya que esta condición equivale a $p \equiv 1\ (4)$ y $p \equiv 1\ (3)$, ó $p \equiv -1\ (4)$ y $p \equiv -1\ (3)$, por el teorema chino del resto. El resto de los casos ($p > 3$, primo) son $p \equiv \pm 5\ (12)$.

En definitiva: El símbolo es 1 si y sólo si $p \equiv \pm 1\ (12)$, es -1 si y sólo si $p \equiv \pm 5\ (12)$, y es cero si y sólo si $p = 3$.

2) Halla una fórmula para la suma de los inversos de los divisores de $n > 1$ en términos de su factorización.

La función que se considera es $F(n) = \sum_{d|n} d^{-1}$. Es multiplicativa porque $f(n) = n^{-1}$ lo es. Para p primo y $\alpha \in \mathbb{Z}^+$,

$$F(p^\alpha) = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots + \frac{1}{p^\alpha} = \frac{p^{-\alpha-1} - 1}{p^{-1} - 1}.$$

Por consiguiente, si la factorización de n es $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, se tiene

$$F(n) = \prod_{j=1}^{k} \frac{p_j^{-\alpha_j - 1} - 1}{p_j^{-1} - 1}.$$

3) Demostrar que si r es una raíz primitiva módulo p (primo impar), entonces r no es un residuo cuadrático.

Si r fuera un residuo cuadrático módulo p, por el criterio de Euler:

$$r^{(p-1)/2} \equiv (\frac{r}{p}) \equiv 1\ (p),$$

y esto contradice que r tenga orden $p-1$.

4) Demostrar que para $|z|<1$ se cumple $\displaystyle\sum_{n=1}^{\infty}\frac{\phi(n)}{n}\log(1-z^n)=\frac{z}{1-z}$.

Desarrollando por Taylor en ambos miembros, debemos probar:

$$\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{\phi(n)}{n}\frac{z^{nk}}{k}=z+z^2+z^3+z^4+\dots$$

(ambas series convergen uniformemente en $|z|<1-\epsilon$ porque $|\log(1-z^n)|\leq C_\epsilon|z|^n$).

Basta por tanto demostrar que el coeficiente de z^N en la serie de la izquierda es 1 para todo $N\in\mathbb{Z}^+$. Este coeficiente es

$$\sum_{nk=N}\frac{\phi(n)}{nk}=\frac{1}{N}\sum_{n|N}\phi(n)=\frac{1}{N}\cdot N=1.$$

La primera igualdad se sigue porque $nk=N$ equivale a $n|N$, mientras que la segunda se sigue de $N=\sum_{n|N}\phi(n)$ (visto en clase, basta comprobarlo para potencias de primos: $p^\alpha=1+(p-1)+(p^2-p)+\dots+(p^\alpha-p^{\alpha-1})$, y la suma es telescópica).

Modelo 2

1) Sea r una raíz primitiva módulo 19. Demostrar que las soluciones de $x^3\equiv 1\ (19)$ son exactamente $x\equiv 1, r^6, r^{12}$.

Evidentemente $x\equiv 0\ (19)$ no es solución de $x^3\equiv 1\ (19)$, así que toda solución se puede escribir de forma única como $x\equiv r^\alpha$, $0\leq\alpha<18$ (por la definición de raíz primitiva).

$$r^\alpha \text{ es solución } \Leftrightarrow r^{3\alpha}\equiv 1\ (19)\Leftrightarrow 18=\text{ orden de } r|3\alpha\Leftrightarrow 6|\alpha\Leftrightarrow\alpha=0,6,12$$

(recuérdese que $0\leq\alpha<18$).

Comentarios: Muchos alumnos olvidan probar que las soluciones son exactamente las que se indican. Es decir, hay que probar las dos implicaciones: x es solución si y sólo si $x\equiv 1, r^6, r^{12}\ (19)$. En la mayor parte de los casos he penalizado este olvido con medio punto.

2) ¿Para qué valores impares de n es $\sigma(n)$ impar?

$\sigma(n)=\sum_{d|n}f(d)$ con f la identidad. Como f es multiplicativa, σ también lo es. Si $n>1$ es impar, su factorización $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ consta de primos impares p_j, y por ser multiplicativa

$$\sigma(n)=\sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2})\cdots\sigma(p_k^{\alpha_k}).$$

De modo que (para $n > 1$) $\sigma(n)$ es impar $\Leftrightarrow \sigma(p_j^{\alpha_j})$ es impar para todo $1 \leq j \leq k$. Ahora bien, para cualquier primo impar p y $\alpha \in \mathbb{Z}^+$

$$\sigma(p^\alpha) = 1 + p + p^2 + p^3 + \cdots + p^\alpha \equiv 1 + 1 + \cdots + 1 \equiv 1 + \alpha \ (2).$$

Así pues $\sigma(n)$ es impar si y sólo si α_j es par para todo $1 \leq j \leq k$. Es decir,

$$\sigma(n) \text{ es impar } \Leftrightarrow \ n \text{ es un cuadrado perfecto.}$$

Evidentemente, como $\sigma(1) = 1$, el caso $n = 1$ también se ajusta a esta caracterización.

Comentarios: He penalizado (típicamente con medio punto) no simplicar la condición, esto es, no llegar a que n es un cuadrado perfecto.

3) Decidir si las ecuaciones $x^2 \equiv 13\ (67)$ y $x^2 \equiv 3\ (25)$ tienen solución.

Como 67 es primo, $x^2 \equiv 13\ (67)$ tiene solución si y sólo si $\left(\frac{13}{67}\right) = 1$. Por la ley de reciprocida cuadrática:

$$\left(\frac{13}{67}\right) = \left(\frac{67}{13}\right) = \left(\frac{2}{13}\right) = -1 \text{ porque } 13 \neq 8n \pm 1.$$

(En la segunda igualdad se usa que $67 \equiv 2\ (13)$, y en la primera que 13 es de la forma $4n + 1$).

Si $x^2 \equiv 3\ (25)$ tuviera solución, entonces también la tendría $x^2 \equiv 3\ (5)$ (ya que $25|x^2 - 3 \ \Rightarrow \ 5|x^2 - 3$) pero esta última ecuación no la tiene: $(\pm 1)^2, (\pm 2)^2 \not\equiv 3\ (5)$.

Comentarios: El símbolo de Jacobi $\left(\frac{3}{25}\right)$ es uno, pero esto no implica que $x^2 \equiv 3\ (25)$ tenga solución.

4) Demostrar que hay infinitos primos de la forma $6n + 1$, probando primero que para $p > 3$, $p|k^2 + 3 \Rightarrow p \equiv 1\ (6)$.

$p > 3$, $p|k^2 + 3 \Rightarrow \left(\frac{-3}{p}\right) = 1$. Por la ley de reciprocidad cuadrática:

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p-1)/2}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Y esto es 1 si y sólo si $p \equiv 1\ (3)$, lo que implica $p \equiv 1\ (6)$ ($p - 1$ es par).

Si hubiera sólo m primos de la forma $6n + 1$, digamos $p_1, p_2, \ldots, p_m$; tomemos $k = 2p_1p_2 \cdots p_m$. Evidentemente 2 y 3 no dividen a $k^2 + 3$ (k es par y no es múltiplo de 3). Por el resultado anterior cada uno de los factores primos de k^2+3 son de la forma $6n+1$. Como $p_j \not| k^2 + 3$, hemos encontrado un nuevo primo que no está en la lista.

Comentarios: 1) Que un número sea de la forma $6n + 1$ no implica que alguno de sus factores lo sea (por ejemplo $121 = 11 \cdot 11 = 6 \cdot 20 + 1$). 2) El número $(p_1p_2 \cdots p_m)^2 + 3$, si no se prueba lo contrario, podría ser una potencia de 2. Un argumento del tipo "sea $p > 3$ dividiendo a $(p_1p_2 \cdots p_m)^2 + 3 \ldots$" necesita justificación.