Preparación Olímpica I

Glenier Bello (gbello@unizar.es)

§1. Aritmética Modular

Denotaremos por $\mathbb{Z}$ a los números enteros y por $\mathbb{N}$ a los números enteros positivos; es decir,

$$\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\} \quad \text{y} \quad \mathbb{N} := \{1, 2, 3 \dots\}.$$

Definición 1.1. Sea $n \in \mathbb{N}$ y sean $a, b \in \mathbb{Z}$. Diremos que a y b son *congruentes módulo* n, y escribiremos $a \equiv b \pmod{n}$, si n divide a $a - b$.

Recordemos que dos enteros a y b se dicen *coprimos* si no tienen ningún divisor primo común. Por ejemplo, el 6 y el 25 son coprimos.

Proposición 1.2 (Propiedades elementales de las congruencias)**.** *Sea $n \in \mathbb{N}$ y sean $a, b, c, d \in \mathbb{Z}$.*

(a) $a \equiv a \pmod{n}$.

(b) *Si* $a \equiv b \pmod{n}$ *y* $b \equiv c \pmod{n}$ *entonces* $a \equiv c \pmod{n}$.

(c) *Si* $a \equiv b \pmod{n}$ *entonces* $b \equiv a \pmod{n}$.

(d) *Si* $a \equiv b \pmod{n}$ *y* $c \equiv d \pmod{n}$ *entonces* $a \pm c \equiv b \pm d \pmod{n}$.

(e) *Si* $a \equiv b \pmod{n}$ *entonces* $ka \equiv kb \pmod{n}$ *para todo* $k \in \mathbb{Z}$.

(f) *Si* $ac \equiv bc \pmod{n}$ *y* n *y* c *son coprimos, entonces* $a \equiv b \pmod{n}$.

(g) *Si* $a \equiv b \pmod{n}$ *y* $c \equiv d \pmod{n}$ *entonces* $ac \equiv bd \pmod{n}$.

(h) *Si* $a_i \equiv b_i \pmod{n}$ *para* $i = 1, \dots, k$, *entonces* $a_1 \cdots a_k \equiv b_1 \cdots b_k \pmod{n}$. *En particular, si* $a \equiv b \pmod{n}$ *entonces* $a^k \equiv b^k \pmod{n}$ *para todo* $k \in \mathbb{N}$.

(i) $a \equiv b \pmod{n_i}$ *para* $i = 1, \dots, k$ *si y sólo si* $a \equiv b \pmod{\operatorname{mcm}(n_1, \dots, n_k)}$. *En particular, si* $n_1, \dots, n_k$ *son coprimos, entonces* $a \equiv b \pmod{n_i}$ *si y sólo si* $a \equiv b \pmod{n_1 \cdots n_k}$.

Demostración. Ejercicio. (Se deduce de la definición 1.1.) □

Proposición 1.3. *Sean $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, y sean $r_1, r_2 \in \{0, 1, \dots, n-1\}$ tales que*

$$a = nq_1 + r_1 \quad \text{y} \quad b = nq_2 + r_2.$$

Entonces $a \equiv b \pmod{n}$ *si y sólo si* $r_1 = r_2$.

Demostración. Notar que $a-b = n(q_1-q_2)+(r_1-r_2)$. Por tanto, $n|(a-b)$ si y sólo si $n|(r_1-r_2)$. Como $|r_1 - r_2| \in \{0, 1, \ldots, n-1\}$, tenemos que $n|(r_1 - r_2)$ si y sólo si $r_1 = r_2$. □

Ejercicio 1.4. Sea $n \in \mathbb{Z}$. Demostrar las siguientes afirmaciones:

(a) $n^2 \equiv 0$ ó $1 \pmod 3$,

(b) $n^2 \equiv 0,\ 1$ ó $-1 \pmod 5$,

(c) $n^2 \equiv 0,\ 1$ ó $4 \pmod 8$,

(d) $n^3 \equiv 0,\ 1$ ó $-1 \pmod 9$,

(e) $n^4 \equiv 0$ ó $1 \pmod{16}$.

Ejercicio 1.5. Probar que los números de la forma $4k + 3$, con k entero no negativo, no son suma de dos cuadrados.

§2. La función indicatriz de Euler

Definición 2.1. Para cada entero positivo m sea $\varphi(m)$ el número de enteros positivos menores o iguales que m que son coprimos con m. La función φ se llama *función indicatriz de Euler*.

Ejemplos 2.2. $\varphi(1) = 1, \varphi(7) = 6, \varphi(10) = 4, \varphi(16) = 8$.

Proposición 2.3. *Sea $p \in \mathbb{N}$. Entonces p es primo si y sólo si $\varphi(p) = p - 1$.*

Demostración. Ejercicio. (Se deduce de la definición 2.1.) □

Proposición 2.4. *Sean p un número primo y a un entero positivo. Entonces*

$$\varphi(p^a) = p^a - p^{a-1}.$$

Demostración. Entre todos los enteros positivos menores o iguales que p^a, los únicos que no son coprimos con p^a son $p, 2p, 3p, \ldots, p^{a-1}p$. □

Proposición 2.5. *Sean a y b dos enteros positivos coprimos. Entonces*

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Demostración. Agrupamos los números $1, 2, \ldots, ab$ en la siguiente tabla de tamaño $a \times b$:

$$\begin{array}{cccc} 1 & 2 & \ldots & a \\ a+1 & a+2 & \ldots & 2a \\ \vdots & \vdots & \ddots & \vdots \\ a(b-1)+1 & a(b-1)+2 & \ldots & ab \end{array}$$

Claramente hay $\varphi(ab)$ números en la tabla superior coprimos con ab. Por otro lado, notar que hay $\varphi(a)$ columnas que contienen los elementos de la tabla coprimos con a y hay exactamente $\varphi(b)$ elementos en cada columna coprimos con b. Por tanto hay $\varphi(a)\varphi(b)$ elementos en la tabla coprimos con ab. Luego $\varphi(ab) = \varphi(a)\varphi(b)$. □

Teorema 2.6. *Sea $n \in \mathbb{N}$ y sea $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ su descomposición en factores primos. Entonces*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Demostración. Basta usar la proposiciones 2.4 y 2.5. □

§3. Los teoremas de Euler y de Fermat

Definición 3.1. Sea $m \in \mathbb{N}$. Diremos que $S \subset \mathbb{Z}$ es un *conjunto completo reducido de clases de residuos módulo m* si para cada $a \in \mathbb{Z}$ coprimo con m existe un único elemento $b \in S$ tal que $a \equiv b \pmod{m}$.

Teorema 3.2 (Euler)**.** *Si a y m son enteros positivos coprimos, entonces*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \qquad (*)$$

Demostración. Sea $S := \{a_1, \ldots, a_{\varphi(m)}\}$ el conjunto de todos los enteros positivos menores o iguales que m coprimos con m. Como mcd(a,m)=1, tenemos que $\{aa_1, \ldots, aa_{\varphi(m)}\}$ es otro conjunto completo reducido de clases de residuos módulo m. Luego

$$(aa_1)\cdots(aa_{\varphi(m)}) \equiv a_1 \cdots a_{\varphi(m)} \pmod{m}$$

Como mcd($a_1 \cdots a_{\varphi(m)}$,$m$)=1, usando el apartado (f) de la proposición 1.2 obtenemos $(*)$. □

Corolario 3.3 (Pequeño teorema de Fermat)**.** *Sean $a \in \mathbb{N}$ y p un número primo. Entonces*

$$a^p \equiv a \pmod{p}.$$

Demostración. Si p divide a a el resultado es obvio. En caso contrario, como $\varphi(p) = p - 1$, usando el teorema de Euler 3.2 tenemos que

$$a^{p-1} \equiv 1 \pmod{p},$$

de donde se deduce que $a^p \equiv a \pmod{p}$. □

Ejercicio 3.4. Sea $p \geq 7$ un número primo. Probar que el número

$$\underbrace{11\ldots1}_{p-1}$$

es divisible por p