# TEORÍA DE NÚMEROS

GLENIER BELLO

## 1. Aritmética Modular

**Definición.** Sean $a$, $b$ y $m$ enteros, con $m \neq 0$. Decimos que $a$ y $b$ son *congruentes* módulo $m$ si $m$ divide a $a - b$ y lo denotamos por

$$a \equiv b \pmod{m}.$$

Si $m$ no divide a $a - b$, decimos que $a$ y $b$ no son congruentes módulo $m$ y lo denotamos por $a \not\equiv b \pmod{m}$.

**Proposición.**

*(1)* $a \equiv a \ (mod\ m)$.
*(2) Si* $a \equiv b \ (mod\ m)$ *y* $b \equiv c \ (mod\ m)$ *entonces* $a \equiv c \ (mod\ m)$.
*(3) Si* $a \equiv b \ (mod\ m)$ *entonces* $b \equiv a \ (mod\ m)$.
*(4) Si* $a \equiv b \ (mod\ m)$ *y* $c \equiv d \ (mod\ m)$ *entonces* $a \pm c \equiv b \pm d \ (mod\ m)$.
*(5) Si* $a \equiv b \ (mod\ m)$ *entonces* $ka \equiv kb \ (mod\ m)$ *para todo* $k \in \mathbb{Z}$.
*(6) Si* $ac \equiv bc \ (mod\ m)$ *y* $m$ *y* $c$ *son coprimos, entonces* $a \equiv b \ (mod\ m)$.
*(7) Si* $a \equiv b \ (mod\, m)$ *y* $c \equiv d \ (mod\, m)$ *entonces* $ac \equiv bd \ (mod\, m)$. *En general, si* $a_i \equiv b_i \ (mod\, m)$ *para* $i = 1, \ldots, k$, *entonces* $a_1 \cdots a_k \equiv b_1 \cdots b_k \ (mod\, m)$. *En particular, si* $a \equiv b \ (mod\, m)$ *entonces* $a^k \equiv b^k \ (mod\, m)$ *para todo* $k \in \mathbb{N}$.
*(8)* $a \equiv b \ (mod\, m_i)$ *para* $i = 1, \ldots, k$ *si y sólo si* $a \equiv b \ (mod\ mcm(m_1, \ldots, m_k))$. *En particular, si* $m_1, \ldots, m_k$ *son coprimos, entonces* $a \equiv b \ (mod\ m_i)$ *si y sólo si* $a \equiv b \ (mod\ m_1 \cdots m_k)$.

*Demostración.* Se deduce inmediatamente de la definición. Ejercicio. □

**Proposición.** *Sean* $a$, $b$ *y* $n$ *enteros, con* $n \neq 0$, *tales que* $a = nq_1 + r_1$ *y* $b = nq_2 + r_2$, *con* $0 \leq r_1, r_2 < |n|$. *Entonces* $a \equiv b \ (mod\ n)$ *si y sólo si* $r_1 = r_2$.

*Demostración.* Notar que $a - b = n(q_1 - q_2) + (r_1 - r_2)$, luego $n|(a - b)$ si y sólo si $n|(r_1 - r_2)$. Como $|r_1 - r_2| < |n|$, tenemos que $n|(r_1 - r_2)$ si y sólo si $r_1 = r_2$. □

Por los apartados (1), (2) y (3) de la primera proposición, deducimos que para cada entero positivo $m$ podemos clasificar los enteros en clases de acuerdo a su resto al dividirlos por $m$. Claramente, hay $m$ clases.

Un conjunto $S$ de enteros se dice *conjunto completo de clases de residuos* módulo $m$ si para cada $0 \leq i \leq m - 1$, existe un único elemento $s \in S$ tal que

$i \equiv s \pmod{m}$. Por ejemplo, $\{a, a+1, \ldots, a+m-1\}$ es un conjunto completo de clases de residuos módulo $m$ para cada entero $a$.

**Ejemplo.** Sea $n$ un entero. Entonces

(1) $n^2 \equiv 0$ ó $1 \pmod 3$,
(2) $n^2 \equiv 0,\ 1$ ó $-1 \pmod 5$,
(3) $n^2 \equiv 0,\ 1$ ó $4 \pmod 8$,
(4) $n^3 \equiv 0,\ 1$ ó $-1 \pmod 9$,
(5) $n^4 \equiv 0$ ó $1 \pmod{16}$.

*Solución.* En cada caso, basta comprobarlo para un conjunto completo de clases de residuos del módulo correspondiente. Ejercicio.

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

*Solución.* Basta usar que los cuadrados perfectos son congruentes con 0 ó 1 módulo 4.

## 2. La función indicatriz de Euler

**Definición.** 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 $\varphi$ se llama *función indicatriz de Euler*.

**Ejemplos.** $\varphi(1) = 1, \varphi(7) = 6, \varphi(10) = 4, \varphi(16) = 8$. Observar que $\varphi(p) = p - 1$ si y sólo si $p$ es primo.

**Proposición.** *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.** *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 $a \times b$:

| | | | |
|---|---|---|---|
| 1 | 2 | ... | $a$ |
| a+1 | a+2 | ... | $2a$ |
| ⋮ | ⋮ | | ⋮ |
| a(b-1)+1 | a(b-1)+2 | ... | $ab$ |

Claramente hay $\varphi(ab)$ números en la tabla superior coprimos con $ab$. Por otra parte, 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.** *Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ es la descomposición en factores primos de $n > 1$, entonces*

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

*Demostración.* Basta usar las dos proposiciones anteriores. □

## 3. Los teoremas de Euler y Fermat

Un conjunto $S$ de enteros se dice *conjunto completo reducido de clases de residuos* módulo $m$ si para cada $i$ coprimo con $m$ tal que $0 \leq i \leq m-1$, existe un único elemento $s \in S$ tal que $i \equiv s \pmod{m}$.

**Teorema.** (Teorema de Euler) *Sean $a$ y $m$ enteros positivos coprimos. Entonces*

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

*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, de lo anterior se deduce el teorema. □

**Corolario.** (Teorema pequeño de Fermat) *Sean $a$ un entero positivo 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, podemos aplicar el Teorema de Euler con $m = p$ y usando que $\varphi(p) = p - 1$ tenemos

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

que multiplicado por $a$ prueba el teorema. □

**Ejemplo.** Sea $p \geq 7$ un número primo. Probar que el número

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

es divisible por $p$

*Solución.* Notar que

$$\underbrace{11\ldots1}_{p-1} = \frac{10^{p-1}-1}{9}.$$

Como mcd(10,$p$)=1, por el Teorema pequeño de Fermat $10^{p-1}-1 \equiv 0 \pmod{p}$. Además $p$ no divide a 9, luego el resultado se cumple.

## 4. Problemas

**Problema 1.** Probar que existen infinitos números primos congruentes con 3 módulo 4.

**Problema 2.** Sea $m$ un entero positivo y sean $a$ y $b$ enteros, con mcd($a$,$m$)=1. Sea $S$ un conjunto completo de clases de residuos módulo $m$. Entonces el conjunto

$$T = aS + b = \{as + b : s \in S\}$$

también es un conjunto completo de clases de residuos módulo $m$.

**Problema 3.** (Gauss). Probar que para todo entero positivo $n$ se cumple

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

**Problema 4.** (OME 2014, Fase Local). Hallar las soluciones enteras de la ecuación

$$x^4 + y^4 = 3x^3y.$$

**Problema 5.** (OME 2014, Fase Local). Probar que

$$2014^3 - 1013^3 - 1001^3$$

divide a

$$2014^{2013} - 1013^{2013} - 1001^{2013}.$$

**Problema 6.** (OME 2014, Fase Local). Hallar las tres últimas cifras de $7^{2014}$.

**Problema 7.** Probar que para cada $n$ entero positivo, $n^3 - 1$ no tiene ningún divisor congruente con 2 módulo 3.

**Problema 8.** Sea $n$ un entero positivo y sean $a_1, ..., a_k$ ($k \geq 2$) enteros distintos del conjunto $1, ..., n$, tales que $n$ divide a $a_i(a_{i+1} - 1)$, para $i = 1, ..., k - 1$. Demostrar que $n$ no divide a $a_k(a_1 - 1)$.

**Problema 9.** Consideremos la sucesión $a_1, a_2, \ldots$ definida por

$$a_n = 2^n + 3^n + 6^n - 1,$$

para todos los enteros positivos $n$. Hallar todos los enteros positivos coprimos con todos los términos de la sucesión.