Divisibilidad, Congruencias y Aritmética Módulo n

CARLOS GUSTAVO MOREIRA

Instituto de Matemática Pura e Aplicada IMPA
Estrada Dona Castorina 110
Jardim Botânico
CEP22460-320
E-mail: fercasgu@Hotmail.com
Rio de Janeiro - RJ
BRASIL

Introducción

Este artículo propone hacer una referencia elemental sobre los temas citados en el título, que aparecen naturalmente en diversos problemas de Matemática elemental, algunos de los cuales serán explícitamente tratados aquí.

Sección 1: División euclidiana y el teorema fundamental de la aritmética

Los resultados que siguen tienen como base el siguiente hecho sobre los enteros: Dados $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$ existen $q, r \in \mathbb{Z}$ con $0 \leq r < b$ y $a = bq + r$. Tales q y r estan únicamente determinados. De hecho, $q = [a/b]$ y $r = a - bq$ (aquí $[x]$ denota el único entero k tal que $k \leq x < k + 1$). Como consecuencia tenemos la

Proposición 0 (División Euclidiana): *Dados $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$ existen q, $r \in \mathbb{Z}$ únicamente determinados tales que $0 \leq r < |b|$ y $a = bq + r$.*

Definición: *Dados dos enteros a y b, con $a \neq 0$ decimos que a divide b (denotamos $a|b$) si existe c entero tal que $b = ac$.*

Proposición 1: *Dados a, $b \in \mathbb{Z}$ no ambos nulos existe $d \in \mathbb{N}^*$ tal que $d|a$, $d|b$ y, para todo $c \in \mathbb{N}^*$, $c|a$, $c|b \Rightarrow c|d$. Además, existen x, $y \in \mathbb{Z}$ con $d = ax + by$. (Ese d es llamado el máximo divisor común entre a y b : $d = mdc(a, b)$).*

Demostración: Sea $A = \{k > 0 : \exists\ x,\ y \in \mathbb{Z}$ tales que $k = ax + by\}$ y sea $d = ax_0 + by_0$ el menor elemento de A. Mostraremos que $d|a$. Como $d \in \mathbb{N}^*$, existen q, $r \in \mathbb{Z}$ con $a = dq + r$ y $0 \leq r < d$. Queremos mostrar que $r = 0$. De hecho, si $r > 0$, $r = a - dq = a(1 - qx_0) + b(-qy_0) \in A$, contradiciendo el hecho de d ser el menor elemento de A. Por lo tanto, $r = 0$ y $a = dq \Rightarrow d|a$. Del mismo modo se prueba que $d|b$. Suponga ahora que $c|a$ y $c|b$. Entonces $c|ax_0 + by_0 = d$, como queríamos probar. □

Lema: *Si $mdc(q,\ n) = 1$ y $n|qk$ entonces $n|k$.*

Prueba del Lema: Como $mdc(q,\ n) = 1$, existen $x,\ y \in \mathbb{Z}$ con $qx + ny = 1$, luego $qkx + nky = k$, por lo tanto $n|k$ (pues $n|qkx$ y $n|nky$). □

Corolario: *Sean p un número primo y a, $b \in \mathbb{Z}$. Si $p|ab$ entonces $p|a$ o $p|b$.*

Teorema fundamental de la aritmética: *Todo número natural $n \geq 2$ posee una única factorización (a menos del orden de los factores), como producto de primos.*

Demostración: $n = 2$ es primo. Vamos a mostrar la existencia de la factorización por primos por inducción: Si n es primo no hay que probarlo. Si n es compuesto, $n = ab$, a, $b \in \mathbb{N}$, $a < n$, $b < n$ y, por hipótesis de inducción, a y b se descomponen como producto de primos, por lo tanto n se descompone como producto de primos.

Vamos ahora mostrar la unicidad, también por inducción: Suponga que n admita dos factorizaciones $n = p_1p_2 \ldots p_r$ y $n = q_1q_2 \ldots q_s$ como producto de primos. El Corolario arriba muestra que, como $p_1|q_1q_2 \ldots q_r$, p_1 debe dividir algún q_i y por lo tanto $p_1 = q_i$ (pues ambos son números primos) y, como $n/p_1 = n/q_i < n$ admite una única factorización prima, por hipótesis de inducción, concluímos que la factorización de n es única. □

Proposición 2: *El conjunto de los números primos es infinito.*

Demostración: Suponga que el conjunto de los números primos sea finito, digamos $\{p_1,\ p_2, \ldots,\ p_n\}$. En ese caso, el número $N = p_1p_2 \ldots p_n + 1$ sería mayor que todos

los primos, pero no divisible por ninguno de ellos, pues $p_i|(p_1p_2\ldots p_n+1) \Rightarrow p_i|1$, absurdo. Tendríamos entonces un natural $N>2$ que no sería múltiplo de ningún primo, contradiciendo el teorema fundamental de la aritmética.□

Observación: *Las ideas de esta sección pueden ser utilizadas en situaciones más generales, como en el estudio de polinomios (por ejemplo con coeficientes racionales), donde existe un algoritmo de división, a partir del cual se puede probar de modo análogo resultados correspondientes a los aquí presentados sobre máximo divisor común, existencia y unicidad de factorización.*

Sección 2: Congruencias

Definición: *Sean* $a, b, n \in \mathbb{Z}$, $n>0$. *Decimos que* a *es congruente a* b (módulo n) *(denotamos* $a \equiv b$ (módulo n)*) si* $n|(b-a)$.

Observación: $a \equiv a$ (módulo n), $a \equiv b$ (módulo n) $\Leftrightarrow$ $b \equiv a$ (módulo n), $a \equiv b$ (módulo n), $b \equiv c$ (módulo n)$\Rightarrow$ $a \equiv c$ (módulo n), *o sea, congruencia* (módulo n) *es una relación de equivalencia.*

Proposición: *Si* $a \equiv b$ (módulo n) *y* $c \equiv d$ (módulo n) *entonces* $a+c \equiv b+d$ (módulo n) *y* $ac \equiv bd$ (módulo n).

Demostración: $n|(b-a)$, $n|(d-c) \Rightarrow n|(b+d)-(a+c) \Rightarrow (a+c) \equiv (b+d)$ (módulo n), y $bd-ac = b(d-c)+c(b-a) \Rightarrow n|(bd-ac) \Rightarrow bd \equiv ac$ (módulo n).□

Definición: *Dados* $n, a \in \mathbb{Z}$, $n>0$, *definimos* $\overline{a} = \overline{a}$ (módulo n)$= \{k \in \mathbb{Z} | k \equiv a$ (módulo n)$\}$.

Dados $a, b \in \mathbb{Z}$ *definimos* $\overline{a}+\overline{b} = \overline{a+b}$ *y* $\overline{a}\cdot\overline{b} = \overline{ab}$ *(estas operaciones de suma y producto están bien definidas por la proposición anterior).*

Definimos aún $\mathbb{Z}/n\mathbb{Z} = \{\overline{a}$ (módulo n), $a \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$. *Cada* $\overline{a}$ *es llamada una clase de congruencia* módulo n.

Definición: *Sean* $n, a \in \mathbb{Z}$, $n>0$. *Decimos que* a *es invertible* módulo n *si existe* $b \in \mathbb{Z}$ *con* $ab \equiv 1$ (módulo n) *(o sea, tal que* $\overline{a}\cdot\overline{b} = 1$*). Decimos que* $\overline{b}$ *es el inverso de* $\overline{a}$ *en* $\mathbb{Z}/n\mathbb{Z}$.

Definición: $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a} : a \in \mathbb{Z}$ *y* a *es invertible* (módulo n)$\}$.

Observación: a *es invertible* (módulo n)$\Leftrightarrow$ $mdc(a, n) = 1$. *De hecho,* $mdc(a, n) = 1 \Leftrightarrow \exists x, y \in \mathbb{Z}$ *tales que* $ax+ny = 1 \Leftrightarrow \overline{a}\cdot\overline{x} = \overline{1}$ (módulo n).

Notación: Dado un conjunto finito X, escribimos $\#X$ para significar el número de elementos de X.

Definición: *La función φ de Euler, $\varphi : N \to N$ es definida por* $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^* = \#\{k \in \mathbb{Z} : 0 \leq k < n \text{ y } mdc(k,\ n) = 1\}$.

Notemos que si p es un número primo y $k \in \mathbb{N}$ entonces $\varphi(p^k) = p^k - p^{k-1} = p^k(1-1/p)$. De hecho, $mdc(r,\ p^k) = 1$ si y solo si p no divide r. Luego $\varphi(p^k) = \#\{r \in \mathbb{Z} : 0 \leq r < p^k \text{ y } mdc(r,\ p^k) = 1\} = \#\{r \in \mathbb{Z} : 0 \leq r < p^k\} - \#\{r \in \mathbb{Z} : 0 \leq r < p^k \text{ y } p|r\} = p^k - p^{k-1}$.

Definición: *n números enteros $a_1, a_2, \ldots, a_n$ forman un sistema completo de residuos (s.c.r.)*módulo n *si $\{\bar{a}_1,\ \bar{a}_2, \ldots, \bar{a}_n\} = \mathbb{Z}/n\mathbb{Z}$, esto es, si los a_i representan todas las clases de congruencia* módulo n *(por ejemplo,* 0, 1, 2, $\ldots$, $n-1$ *forman un s.c.r. (*módulo n*)).*

$\varphi(n)$ números enteros $b_1,\ b_2, \ldots,\ b_{\varphi(n)}$ forman un sistema completo de invertibles (s.c.i.) módulo n *si $\{\bar{b}_1,\ \bar{b}_2, \ldots,\ \bar{b}_{\varphi(n)}\} = (\mathbb{Z}/n\mathbb{Z})^*$, esto es, si los b_i representan todas las clases de congruencias invertibles* módulo n.

Proposición: *Sean $q,\ r,\ n \in \mathbb{Z}$, $n > 0$, q invertible* módulo n, *$a_1,\ a_2, \ldots,\ a_n$ un s.c.r. (*módulo n*) y $b_1,\ b_2, \ldots,\ b_{\varphi(n)}$ un s.c.i. (*módulo n*).*

*Entonces $qa_1 + r$, $qa_2 + r$, $\ldots$, $qa_n + r$ forman un s.c.r. (*módulo n*) y qb_1, qb_2, $\ldots$, $qb_{\varphi(n)}$ forman un s.c.i. (*módulo n*).*

Demostración: Vamos a probar que si $a_1,\ \ldots,\ a_n$ forman un s.c.r. (módulo n) entonces $qa_1+r,\ \ldots,\ qa_n+r$ forman un s.c.r. (módulo n). Basta probar que $qa_i+r \equiv qa_j + r$ (módulo n) $\Rightarrow i = j$, pues en ese caso tendremos n clases de congruencias distintas módulo n, que deben ser todas las clases de $\mathbb{Z}/n\mathbb{Z}$. Sea $y \in \mathbb{Z}$ tal que $qy \equiv 1$ (módulo n). Tenemos

$$\begin{aligned} & qa_i = qa_i + r - r \equiv qa_j + r - r = qa_j \text{ (módulo } n) \\ & \Rightarrow qya_i \equiv qya_j \text{ (módulo } n) \\ & \Rightarrow a_i \equiv a_j \text{ (módulo } n) \\ & \Rightarrow i = j. \end{aligned}$$

Sea ahora $b_1,\ b_2, \ldots, b_{\varphi(n)}$ un s.c.r. (módulo n). Tenemos que qb_i es invertible módulo n, para todo i, $1 \leq i \leq \varphi(n)$, pues si x_i es tal que $b_ix_i \equiv 1$ (módulo n), entonces $(qb_i)(x_iy) = (qy)(b_ix_i) \equiv 1$ (módulo n). Por otro lado, si $qb_i \equiv qb_j$ (módulo n) entonces $b_i \equiv yqb_i \equiv yqb_j \equiv b_j$ (módulo n)$\Rightarrow i = j$, y por lo tanto $qb_1,\ qb_2, \ldots,\ qb_{\varphi(n)}$ es un s.c.i. (módulo n).□

Teorema (Euler): *Sean $a,\ n \in \mathbb{Z}$, $n > 0$, tales que $mdc(a,\ n) = 1$. Entonces $a^{\varphi(n)} \equiv 1$ (módulo n).*

Demostración: Sea $b_1,\ b_2, \ldots,\ b_{\varphi(n)}$ un s.c.i. (módulo n). Por la proposición anterior, $(ab_1),\ (ab_2),\ \ldots,\ (ab_{\varphi(n)})$ forman un s.c.i. (módulo n), y tenemos $\{\overline{b}_1,\ \overline{b}_2, \ldots,\ \overline{b}_{\varphi(n)}\} = \{\overline{ab}_1,\ \overline{ab}_2, \ldots,\ \overline{ab}_{\varphi(n)}\} = (\mathbb{Z}/n\mathbb{Z})^* \Rightarrow \overline{b_1} \cdot \overline{b_2} \cdots \overline{b}_{\varphi(n)} = \overline{ab}_1 \cdot \overline{ab}_2 \cdot \ldots \overline{ab}_{\varphi(n)} = a^{\varphi(n)} \cdot \overline{b_1}\ \overline{b_2} \cdots \overline{b}_{\varphi(n)} \Rightarrow \overline{b_1} \cdot \overline{b_2} \cdots \overline{b}_{\varphi(n)}(\overline{a^{\varphi(n)}} - \overline{1}) = 0 \Rightarrow \overline{a^{\varphi(n)}} = \overline{1}$ pues $b_1,\ b_2, \ldots,\ b_{\varphi(n)}$ son invertibles (módulo n) $\Rightarrow a^{\varphi(n)} \equiv 1$ (módulo n).□

Corolario: (Pequeño Teorema de Fermat): *Si $a \in \mathbb{Z}$ y p es primo entonces $a^p \equiv a$ (módulo p).*

Prueba: Si $p|a$, entonces $a^p \equiv a \equiv 0$ (módulo p). Si p no divide a, entonces $mdc(a,\ p) = 1 \Rightarrow a^{p-1} \equiv 1$ (módulo p)$\Rightarrow a^p \equiv a$ (módulo p).□

Ejercicio: Exiva $n \in \mathbb{N}$ tal que 2^n tenga más de dos mil casas decimales y tenga entre sus 2000 últimas casas decimales 1000 ceros consecutivos.

Solución: $2^{\varphi(5^{2000})} \equiv 1$ (módulo 5^{2000}), por teorema de Euler. Por lo tanto, existe $b \in \mathbb{N}$ con $2^{\varphi(5^{2000})} = 5^{2000}b + 1$, y tendremos $2^{2000+\varphi(5^{2000})} = 10^{2000}b + 2^{2000}$, y por lo tanto los 2000 últimos dígitos de $2^{2000+\varphi(5^{2000})}$ coinciden con la representación decimal de 2^{2000}, que tiene a lo sumo 667 dígitos, pues

$$2^3 < 10 \Rightarrow 2^{2000} < 2^{3.667} < 10^{667}$$

Así, $2^{2000+\varphi(5^{2000})}$ tiene por lo menos $2000 - 667 = 1333$ ceros consecutivos de entre las 2000 últimas casas decimales, de modo que $n = 4 \cdot 5^{1999} + 2000$ satisface las condiciones del enunciado (pues $\varphi(5^{2000}) = 4 \cdot 5^{1999}$).□

Teorema Chino de los restos: *Si $mdc(m,\ n) = 1$ entonces $f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, definida por*

$$f(\overline{a}(\text{módulo } mn)) = (\overline{a}(\text{módulo } m),\ \overline{a}(\text{módulo } n))$$

es una biyección.

Demostración: f está bien definida, pues si $a = b$ (módulo mn) entonces $a \equiv b$ (módulo m) y $a \equiv b$ (módulo n). Como $\mathbb{Z}/mn\mathbb{Z}$ y $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tienen mn elementos cada, es suficiente verificar que f es inyectiva. Y, de hecho, si $a \equiv b$ (módulo m) y $a \equiv b$ (módulo n) entonces $m|(b-a)$ y $n|(b-a) \Rightarrow b - a = mk$, $n|mk \Rightarrow n|k$, pues $mdc(m,\ n) = 1 \Rightarrow mn|(b-a) \Rightarrow a \equiv b$ (módulo mn).□

Corolario: *Si $m_1,\ m_2, \ldots,\ m_r \geq 1$ son enteros, y $mdc(m_i,\ m_j) = 1$ para $i \neq j$ entonces $f : \mathbb{Z}/m_1m_2 \ldots m_r\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z}$, definida por*

$$f(\overline{a}(\text{módulo } m_1 \cdot m_2 \cdots m_r)) = (\overline{a}(\text{módulo } m_1), \ldots,\ \overline{a}(\text{módulo } m_r))$$

es una biyección.

Notemos que este Corolario muestra que, dados enteros $a_1,\ a_2, \ldots\ a_r$, existe un entero n con $n = a_1$ (módulo m_1), $n \equiv a_2$ (módulo m_2), ..., $n \equiv a_r$ (módulo m_r).

Proposición: *Tenemos* $f((\mathbb{Z}/mn\mathbb{Z})^*) = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ *para la función* f *definida arriba.*

Demostración: Esto sigue del hecho de que a es primo con mn si y solo si a es primo con m, y a es primo con n.□

Corolario: $mdc(m,\ n) = 1 \Rightarrow \varphi(mn) = \varphi(m) \cdot \varphi(n)$.

Como consecuencia, si $n = p_1^{\alpha_1},\ p_2^{\alpha_2}, \ldots,\ p_k^{\alpha_k}$ donde $p_1,\ p_2, \ldots,\ p_k$ son primos distintos, $\alpha_1,\ \alpha_2, \ldots,\ \alpha_k \in \mathbb{N}^*$ entonces $\varphi(n) = n(1-1/p_1)(1-1/p_2)\cdots(1-1/p_k)$. En particular, si $n \geq 3$ entonces $\varphi(n)$ es par.

Mostraremos un problema cuya solución usa de modo no trivial el teorema chino de los restos:

Problema: Pruebe que dado $n \in \mathbb{N}$ existe un conjunto de n elementos $A \subset \mathbb{N}$ tal que para todo $B \subset A$, $B \neq \emptyset$, $\sum_{x \in B} x$ es una potencia no trivial (esto es, un número de la forma m^k, donde m, k son enteros mayores o iguales a 2), o sea, $A = \{x_1,\ x_2, \ldots,\ x_n\}$ tal que

$$x_1,\ x_2, \ldots,\ x_n,\ x_1 + x_2,\ x_1 + x_3, \ldots,\ x_{n-1} + x_n, \ldots,\ x_1 + x_2 + \ldots + x_n$$

son todos potencias no triviales.

Solución: $A = \{4\}$ es solución para $n = 1$, $A = \{9, 16\}$ es solución para $n = 2$. Vamos a probar la existencia de un tal conjunto por inducción en n. Suponga que $A = \{x_1, \ldots,\ x_n\}$ es un conjunto con n elementos y para todo $B \subset A$, $B \neq \emptyset$, $\sum_{x \in B} x = m_B^{k_B}$. Mostraremos que existe $c \in \mathbb{N}$ tal que el conjunto $\tilde{A} = \{cx_1,\ cx_2, \ldots,\ cx_n, c\}$ satisface el enunciado.

Sea $\ell = mmc\{k_B,\ B \subset A,\ B \neq \emptyset\}$ el mínimo común múltiplo de todos los exponentes k_B. Para cada $B \subset A$, $B \neq \emptyset$ asociamos un número primo $p_B > \ell$, de forma que $B_1 \neq B_2 \Rightarrow p_{B_1} \neq p_{B_2}$, y asociamos un natural r con $r_B \equiv 0$ (módulo p_x), $\forall X \neq B$, $\ell r_B + 1 \equiv 0$ (módulo p_B) (tal r_B existe por el teorema chino de los restos), y tomamos

$$c = \prod_{\substack{B \subset A \\ B \neq \emptyset}} (1 + m_B^{k_B})^{\ell r_B}$$

Como c es una potencia ℓ-ésima, c es una potencia k_B-ésima para todo $B \subset A$, $B \neq \emptyset$, por lo tanto, para $B' \subset \{cx_1,\ cx_2, \ldots,\ cx_n\}$, $B' \neq \emptyset$, tendremos $B' = \{cx : x \in B\}$ para algún $B \subset A$, $B \neq \emptyset$. Luego $\sum_{x \in B'} x$ será una potencia k_B-ésima.

Además,

$$\sum_{X\in B'\cup\{c\}} x = c(1+m_B^{K_B}) = \left[\prod_{\substack{X\subset A\\ X\neq\emptyset,B}} (1+m_X^{K_X})^{\ell r_X}\right]\cdot(1+m_B^{K_B})^{\ell r_B+1},$$

que es una potencia p_B-ésima, pues r_X es múltiplo de p_B para $X \neq B$ y $\ell r_B + 1$ es múltiplo de p_B.□

Sección 3: Ordenes y raíces primitivas

Dados $n \in \mathbb{N}^*$ y $a \in \mathbb{Z}$ con $mcd(a,\ n) = 1$, definimos **el orden de** a módulo n, $ord_n a := min\{t \in \mathbb{N}^* : a^t \equiv 1(\text{módulo } n)\}$. Dado $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ definimos $ord\bar{a} = ord_n a$.

Proposición 3.0: $\{t \in \mathbb{N}^* : a^t \equiv 1(\text{módulo } n)\} = \{k \cdot ord_n a,\ k \in \mathbb{N}^*\}$.

Demostración: Como $a^{ord_n a} \equiv 1$ (módulo n), para todo $k \in \mathbb{N}$ se tiene $a^{k\cdot ord_n a} = (a^{ord_n a})^k \equiv 1^k \equiv 1$ (módulo n). Por otro lado, si $t \in \mathbb{N}$, $a^t \equiv 1$ (módulo n), existe $k \in \mathbb{N}$ con $t = k\cdot ord_n a + r, 0 \leq r < ord_n a \Rightarrow a^t = a^{k\cdot ord_n a}\cdot a^r \equiv 1\cdot a^r \equiv a^r$ (módulo n) $\Rightarrow a^r \equiv 1$ (módulo n), por lo tanto $r = 0$ (pues $0 < r < ord_n a$ contradiría la minimalidad de $ord_n a$), y $t = k \cdot ord_n a$.□

Corolario: $ord_n a | \varphi(n)$.

Definición: *Si* $ord_n a = \varphi(n)$, *decimos que* a *es* **raíz primitiva módulo** n.

Ejemplos: 2 es raíz primitiva módulo 5, pues $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, que es la primera potencia de 2 congruente a 1 módulo 5 y $4 = \varphi(5)$.

- 1 es raíz primitiva módulo 2, pues $ord_2 1 = 1 = \varphi(2)$.
- 3 es raíz primitiva módulo 4, pues $ord_4 3 = 2 = \varphi(4)$.

Proposición 3.1: a *es raíz primitiva* módulo $n \Leftrightarrow \{\overline{a^t},\ t \in \mathbb{N}\} = (\mathbb{Z}/n\mathbb{Z})^*$.

Demostración: Para todo $a \in \mathbb{Z}$ con $mdc(a,\ n) = 1$ tenemos $\{\overline{a^t},\ t \in \mathbb{N}\} \subset (\mathbb{Z}/n\mathbb{Z})^*$. Si a es raíz primitiva módulo n entonces los números $1, a, a^2, \ldots, a^{\varphi(n)-1}$ son distintos (módulo n) pues $a^i = a^j$ (módulo n), con $0 \leq i < j < \varphi(n) \Rightarrow a^{j-i} \equiv 1$ (módulo n) con $0 < j - i < \varphi(n)$, absurdo $\Rightarrow \{a^t,\ t \in \mathbb{N}\} = (\mathbb{Z}/n\mathbb{Z})^*$.

Por otro lado, $\#\{\overline{a^t},\ t \in \mathbb{N}\} \leq ord_n a$ (el argumento arriba muestra que de hecho vale la igualdad), y por lo tanto $\{\overline{a^t},\ t \in \mathbb{N}\} = (\mathbb{Z}/n\mathbb{Z})^* \Rightarrow ord_n a = \varphi(n)$. □

Corolario 1: *Si m divide n y a es raíz primitiva* módulo *n entonces a es raíz primitiva* módulo *m*.

Corolario 2: *Se* $k \geq 3$, *entonces no existe ninguna raíz primitiva* módulo 2^k.

Prueba: Por el corolario anterior, basta probar que no existe raíz primitiva módulo 8, y esto sigue del hecho que si a es impar,

$$a = 2r + 1,\ r \in \mathbb{Z} \Rightarrow a^2 = 4r(r+1) + 1 \equiv 1 \text{ (módulo 8)}.\square$$

Proposición 3.2: *Sean p un número primo, y* $a \in \mathbb{Z}$ *raíz primitiva* módulo p. *Entonces a ó* $a + p$ *es raíz primitiva* módulo p^2.

Demostración: Por hipótesis,

$$ord_p a = ord_p(a+p) = \varphi(p) = p - 1.$$

Por lo tanto $p - 1 | ord_{p^2} a$ (pues $a^t \equiv 1$ (módulo p^2) $\Rightarrow a^t \equiv 1$ (módulo p)), y, como $ord_{p^2} a | \varphi(p^2) = p(p-1)$, debemos tener

$$ord_{p^2} a = p - 1 \text{ ó } ord_{p^2} a = p(p-1) = \varphi(p^2).$$

Del mismo modo,

$$ord_{p^2}(a+p) = p - 1 \text{ ó } ord_{p^2}(a+p) = p(p-1) = \varphi(p^2).$$

Basta probar, por lo tanto, que $ord_{p^2} a \neq p - 1$ ó $ord_{p^2}(a+p) \neq p - 1$. Suponga que $ord_{p^2} a = p - 1$. Por lo tanto, $a^{p-1} \equiv 1$ (módulo p^2), y entonces

$$(a+p)^{p-1} = a^{p-1} + (p-1)pa^{p-2} + C_{p-1}^2 a^{p-3} \cdot p^2 + \ldots \equiv 1 + (p-1)pa^{p-2} \text{ (módulo } p^2),$$

por lo tanto $(a+p)^{p-1}$ no es congruente a 1 (módulo p^2), pues p^2 no divide $(p-1)pa^{p-2}$,de donde obtenemos $ord_{p^2}(a+p) \neq p - 1.\square$

Proposición 3.3: *Si p es un número primo impar y a es raíz primitiva* módulo p^2 *entonces a es raíz primitiva* módulo p^k *para todo* $k \in \mathbb{N}$.

Demostración: Tenemos $a^{p-1} \equiv 1$ (módulo p), pero a^{p-1} no es congruente a 1 (módulo p^2), por lo tanto $a^{p-1} = 1 + b_1 p$, donde p no divide b_1. Vamos a mostrar por inducción que $a^{p^{k-1}(p-1)} = 1 + b_k p^k$, donde p no divide b_k, para todo $k \geq 1$: Tenemos

$$a^{p^k(p-1)} = (a^{p^{k-1}(p-1)})^p = (1 + b_k p^{k-1})^p = 1 + b_k p^{k+1} + C_p^2 b_k^2 p^{2k} + \cdots \equiv 1 + b_k p^{k+1} \text{ (módulo } p^{k+2}).$$

Luego $a^{p^k(p-1)} = 1 - b_k p^{k+1}$, con $b_{k+1} \equiv b_k$ (módulo p). Sigue que p no divide b_{k+1}.

Vamos ahora a mostrar por inducción que a es raíz primitiva módulo p^k para todo $k \geq 2$. Suponga que a sea raíz primitiva módulo p^k. Entonces tenemos

$$p^{k-1}(p-1) = \varphi(p^k) = ord_{p^k} a | ord_{p^{k+1}} a | \varphi(p^{k+1}) = p^k(p-1).$$

Por lo tanto,

$$ord_{p^{k+1}} a = p^{k-1}(p-1) \text{ ó } ord_{p^{k+1}} a = p^k(p-1) = \varphi(p^{k+1}),$$

pero el primer caso es imposible, pues $a^{p^{k-1}(p-1)} = 1 + b_k p^k$, que no es congruente a 1 módulo p^{k+1}, pues p no divide b_k. Por lo tanto $ord_{p^{k+1}} a = \varphi(p^{k+1})$ y a es raíz primitiva módulo p^{k+1}.□

Ejemplo: 2 es raíz primitiva módulo 5^k, $\forall k \in \mathbb{N}$. De hecho, 2 es raíz primitiva módulo 5, y, como $2^4 = 16 \neq 1$ (módulo 25), 2 es raíz primitiva módulo $25 = 5^2$ (como en la proposición 3.2). Por lo tanto, por la proposición 3.3, 2 es raíz primitiva módulo 5^k, $\forall k \in \mathbb{N}$.

Ejercicio: Muestre que existe n natural tal que los mil últimos dígitos de 2^n pertenecen a $\{1, 2\}$.

Solución: Observamos inicialmente que para todo $k \in \mathbb{N}$ existe un número m_k de k dígitos, todos 1 ó 2, divisible por 2^k. De hecho, $m_1 = 2$ y $m_2 = 12$ satisfacen el enunciado.

Sea $m_k = 2^k \cdot r_k$, $r_k \in \mathbb{N}$. Si r_k es par, tome

$$m_{k+1} = 2 \cdot 10^k + m_k = 2^{k+1}(5^k + r_k/2),$$

y si r_k es impar, tome

$$m_{k+1} = 10^k + m_k = 2^{k+1}(5^k + r_k)/2.$$

Como $m_{1000} \equiv 2$ (módulo 10), 5 no divide $r_{1000} = m_{1000}/2^{1000}$. Como 2 es raíz primitiva módulo 5^{1000}, existe $k \in \mathbb{N}$ con $2^k \equiv r_{1000}$ (módulo 5^{1000}). Luego $2^k = b \cdot 5^{1000} + r_{1000}$, para algún $b \in \mathbb{N}$. Por lo tanto,

$$2^{k+1000} = b \cdot 10^{1000} + 2^{1000} \cdot r_{1000} = b \cdot 10^{1000} + m_{1000},$$

y las 1000 últimas casas de 2^{k+1000} son las 1000 casas de m_{1000}, que pertenecen todas a $\{1, 2\}$.□

Observación: *Si p es primo impar, $k \in \mathbb{N}$ y a es un entero impar tal que a es raíz primitiva* módulo p^k *entonces a es raíz primitiva* módulo $2p^k$, *pues*

$$\varphi(p^k) = ord_{p^k} a | ord_{2p^k} a | \varphi(2p^k) = \varphi(p^k) \Rightarrow ord_{2p^k} a = \varphi(2p^k).$$

Esto implica que si a es raíz primitiva módulo p^k *entonces a ó* $a+p^k$ *es raíz primitiva* módulo $2p^k$ *(pues a y* $a+p^k$ *son raíces primitivas* módulo p^k *y uno de ellos es impar).*

Proposición 3.4: *Si* $n = ab$, *con* $a \geq 3$ *y* $b \geq 3$ *enteros tales que* $mdc(a,\ b) = 1$, *entonces no existe raíz primitiva* módulo n.

Demostración: Tenemos $\varphi(n) = \varphi(a) \cdot \varphi(b)$ y, como $a \geq 3$ y $b \geq 3$, $\varphi(a)$ y $\varphi(b)$ son pares. Si $mdc(k,\ n) = 1$ entonces tenemos

$$k^{\varphi(n)/2} = (k^{\varphi(b)/2})^{\varphi(a)} \equiv 1 \text{ (módulo } a\text{), y } k^{\varphi(n)/2} = (k^{\varphi(a)/2})^{\varphi(b)} \equiv 1 \text{ (módulo } b\text{).}$$

Así, $k^{\varphi(n)/2} = 1$ (módulo n), y por lo tanto $ord_n k | \varphi(n)/2 < \varphi(n)$.□

Teorema: *Existe algúna raíz primitiva* módulo n *si, y solo si,* $n = 2$, $n = 4$, $n = p^k$ *ó* $n = 2p^k$ *donde p es primo impar.*

Prueba: Por los resultados anteriores, basta probar que si p es primo impar entonces existe raíz primitiva módulo p, o sea, existe $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ con $ord_p a = p - 1$.

Para cada $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$, se tiene $ord_p a | (p-1)$. Sea d un divisor de $p-1$. Definimos

$$N(d) = \#\{\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^* : ord_p a = d\}.$$

Tenemos por lo tanto $p - 1 = \sum_{d|p-1} N(d)$. El resultado seguirá de los dos lemas siguientes:

Lema 1: $N(d) \leq \varphi(d)$ *para todo d divisor de* $p - 1$.

Prueba: Si $N(d) > 0$ entonces existe $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ con $ord_p a = d$. Si $ord_p a = d$, entonces $\overline{a^d} = \overline{1}$ y, para $0 \leq k < d$, las clases de a^k son todas distintas módulo p, y $(\overline{a^k})^d = \overline{1}$. Como la ecuación $x^d - \overline{1} = 0$ tiene a lo sumo d raíces distintas en $\mathbb{Z}/p\mathbb{Z}$ (pues $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo), sus raíces son exactamente $\overline{a^k}$, $0 \leq k < d$. Por otro lado, $ord_p a^k = d \Rightarrow mcd(k,\ d) = 1$, pues si $r > 1$ es tal que $r|k$ y $r|d$ entonces $(a^k)^{d/r} = (a^d)^{k/r} \equiv 1$ (módulo p), luego $ord_p(a^k) \leq d/r < d$. De esta forma,

$$\{\overline{b} \in (\mathbb{Z}/p\mathbb{Z})^* : ord_p b = d\} \subset \{\overline{a^k},\ 0 \leq k < d \text{ y } mcd(k,\ d) = 1\},$$

por lo tanto $N(d) \leq \varphi(d)$.□

Lema 2: $\sum_{d|n} \varphi(d) = n$, *para todo* $n \in \mathbb{N}$.

Prueba del Lema 2: Considere los n números racionales $1/n$, $2/n$, ..., n/n. Al simplificarlos, aparecen exactamente $\varphi(d)$ de ellos con denominador d, para cada divisor d de n. Por lo tanto, $\sum_{d|n} \varphi(d) = n$.□

Fin de la prueba del teorema: Del Lema 2 sigue que $\sum_{d|p-1} \varphi(d) = p-1$ y, como $p-1 = \sum_{d|p-1} N(d)$ y $N(d) \leq \varphi(d)$ para todo d, debemos tener $N(d) = \varphi(d)$ para todo d. En particular, $N(p-1) = \varphi(p-1) > 0 \Rightarrow$ existen raíces primitivas módulo p.□

PROBLEMAS

1. Pruebe que existen infinitos números primos congruentes a 3 módulo 4.

2. Determine todos los n naturales tales que $(2^n - 1)/n$ es entero.

3. Determine todos los n naturales tales que $(2^n + 1)/n^2$ es entero. (Propuesto en la XXXI Olimpíada Internacional de Matemática, realizada en China, en 1990)

4. Pruebe que si a y b son naturales y $(a^2 + b^2)/(ab + 1)$ es entero entonces $(a^2 + b^2)/(ab + 1)$ es cuadrado perfecto. (Propuesto en la XXIX Olimpíada Internacional de Matemática, realizada en Australia en 1988)

5. Sean a, $n \in \mathbb{N}^*$. Considere la sucesión (x_n) definida por $x_1 = a$, $x_{k+1} = a^{x_k}$, $\forall k \in \mathbb{N}$. Muestre que existe $N \in \mathbb{N}$ tal que $x_{k+1} \equiv x_k$ (módulo n), para todo $k \geq N$.