Aritmética Modular.

Héctor Raúl Fernández Morales
hectorraulfm@gmail.com

Diciembre 19, 2020

En este documento desarrollamos los temas más relevantes relacionados con aritmética modular:

- Inversos
- Teorema chino del resto(CRT)
- Función de euler y pequeño teorema de Fermat
- Orden

Background: Se asume que el lector está familiarizado con los conceptos esenciales de divisibilidad: algoritmo de euclides, teorema de Bezout, teorema fundamental de la aritmética, congruencias.

1 Inversos

Definition 1. *Decimos que b es el **inverso** de a módulo m si:*

- $\text{mcd}(a, m) = 1$ *y*
- $ab \equiv 1 \pmod{m}$.

Definition 2. *Sea n un entero positivo. La función $\varphi(n)$ es llamada **Función φ de Euler(Euler's totient function)** y denota el número de enteros positivos menores que n que son primos relativos con n.*

$$\varphi(n) = |\{m \in \mathbb{N} | m < n \wedge \text{mcd}(m, n) = 1\}|$$

Theorem 1. *Sean a y m primos relativos. Sea R el conjunto de los números enteros positivos menores que m y primos relativos con m, $R = \{a_1, a_2, \ldots a_{\varphi(m)}\}$. El conjunto $S = \{aa_1, aa_2, \ldots aa_{\varphi(m)}\}$ reducido módulo m es igual a R.*

Proof. Primeramente notemos que cada elemento de S es primo relativo con m y que S y R tienen el mismo cardinal. Solo necesitamos probar que cuando reducimos S modulo m sigue teniendo $\varphi(m)$ elementos. Supongamos lo contrario, esto es, existen $1 \leq i < j \leq \varphi(m)$ tales que $aa_i \equiv aa_j \pmod{m}$, de donde

$$aa_i \equiv aa_j \pmod{m} \Rightarrow a(a_i - a_j) \equiv 0 \pmod{m} \Rightarrow a_i \equiv a_j \pmod{m}$$

lo que implica que $i = j$, contradicción. □

Theorem 2. *Sean a y m primos relativos, entonces a tiene un único inverso módulo m.*

Proof. Notemos que $1 \in R$, donde R es el conjunto definido previamente. Como $R = S$ tenemos que existe un único $a_k \in R$ tal que $aa_k \equiv 1 \pmod{m}$. □

Corollary 2.1. *Sean a y m primos relativos, entonces la ecuación $ax \equiv b \pmod{m}$ siempre tiene solución.*

Proof. Tomemos $x \equiv a^{-1}b \pmod{m}$. □

Example 1. *Sean a y b enteros positivos primos relativos. Consideremos la progresión aritmética $a, a+b, a+2b \ldots$. Entonces existe infinitos pares de primos relativos en dicha progresión.*

Solution. Usemos inducción. El caso base es elemental $\text{mcd}(a, a+b) = 1$. Supongamos que tenemos un conjunto de m elementos de la progresión primos relativos dos a dos, $S = \{a + k_1 b, a + k_2 b \ldots a + k_m b\}$. Sea $P_S = \{p_1, p_2, \ldots p_n\}$ el cojunto de primos que dividen a algun elemento de S. Sabemos que $p_i | a + k_j b$ para algun j, por tanto $p_i | b \Rightarrow p_i | a$ lo que contradice que $\text{mcd}(a, b) = 1$, de donde $p_i \nmid b$ para todo i. Usando el corolario anterior sabemos que existe x tal que

$$xb \equiv 1 - a \pmod{p_1 p_2 \ldots p_m} \Rightarrow a + xb \equiv 1 \pmod{p_1 p_2 \ldots p_m}$$

Sea ahora $x = k_{m+1}$. Como $a + k_{m+1} b$ no es divisible por ningún elemento de P_S tenemos que $\text{mcd}(a + k_{m+1} b, a + k_i b)$ para todo $1 \leq i \leq m$, y añadiendo $a + k_{m+1} b$ a S tenemos un subconjunto de la progresión de $m + 1$ elementos todos primos relativos dos a dos. □

2 Teorema chino del resto

Theorem 3. *[CRT] Sean $m_1, \ldots, m_k$ enteros positivos primos relatiovos dos a dos, y sea $M = m_1 m_2 \ldots m_k$. Entonces para cada k-tupla $(x_1, x_2 \ldots, x_k)$ de enteros, existe exactamente una clase de residuo $x \pmod{M}$ tal que*

$$\begin{aligned} x &\equiv x_1 \pmod{m_1} \\ x &\equiv x_2 \pmod{m_2} \\ &\vdots \\ x &\equiv x_k \pmod{m_k}. \end{aligned}$$

Proof. El teorema se demuestra por inducción en k. Demostremos el caso $k = 2$,

$$\begin{aligned} x &\equiv x_1 \pmod{m_1} \\ x &\equiv x_2 \pmod{m_2} \end{aligned}$$

Consideremos $0 \leq x \leq m_1 m_2 - 1$. De la primera equación sabemos que x pertenece al conjunto

$$S = \{k m_1 + x_1, \quad 0 \leq k \leq b_2 - 1\}$$

Según el corolario 2.1 sabemos que la ecuación $km_1 + x_1 \equiv x_2 \pmod{b_2}$ tiene una única solución módulo b_2. De donde x existe y es único.
Asumamos que existe solución única para $k = n$ y cosideremos

$$\begin{aligned} x &\equiv x_1 \pmod{m_1} \\ x &\equiv x_2 \pmod{m_2} \\ &\vdots \\ x &\equiv x_n \pmod{m_n} \\ x &\equiv x_{n+1} \pmod{m_{n+1}}. \end{aligned}$$

Por hipótesis de inducción este sistema es equivalente a

$$\begin{aligned} x &\equiv y \pmod{m_1 m_2 \dots m_n} \\ x &\equiv x_{m+1} \pmod{m_{n+1}} \end{aligned}$$

y este sistema se resuelve igual que el caso base. □

Problem 1 (IMO 1989)**.** *Prueba que para cada entero positivo n existen n enteros positivos consecutivos ninguno de los cuales es potencia de un primo.*

Solution. Consideremos dos colleciones de primos todos distintos $\{p_1, p_2, \dots p_n\}$ y $\{q_1, q_2, \dots q_n\}$. El sistema

$$\begin{aligned} x &\equiv -1 \pmod{p_1 q_1} \\ x &\equiv -2 \pmod{p_2 q_2} \\ &\vdots \\ x &\equiv -n \pmod{p_n q_n}. \end{aligned}$$

tiene solucion por el CRT, de donde cada elemento de la colección $\{x+1, x+2 \dots, x+n\}$ es divisible por al menos dos primos. □

Problem 2 (IMO 2009)**.** *Sea n un entero positivo y sean $a_1, a_2, \dots, a_k$ $(k \geq 2)$ enteros distintos del conjunto $\{1, 2, \dots, n\}$ tales que n divide a $a_i(a_{i+1} - 1)$ para $i = 1, 2 \dots k-1$. Prueba que n no divide a $a_k(a_1 - 1)$.*

Solution. Sea $n = p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$ y supongamos que $n | a_k(a_1 - 1)$.
Ahora, si $p | a_i$ para cierto i, entonces $p^r | a_{i-1}(a_i - 1) \Rightarrow p^r | a_{i-1}$ e inductivamente $p^r | a_i$ para todo i.
Si $p \nmid a_i$ para cierto i, entonces $p^r | a_i(a_{i-1} - 1) \Rightarrow p^r | a_{i-1} - 1 \Rightarrow p \nmid a_{i-1}$ e inductivamente $p^r | a_i - 1$ para todo i.
En ambos casos los a_i son iguales $\pmod{p^r}$. Por el CRT todos los a_i son iguales $\pmod{n}$ lo que implica que son iguales, contradicción. □

3 Función de euler y pequeño teorema de Fermat

Theorem 4 (Euler's totient theorem)**.** *Sean a y m primos relativos, entonces* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Proof. Usando el teorema 1 sabemos que los conjuntos $\{a_1, a_2, \dots a_{\varphi(m)}\}$ y $S = \{aa_1, aa_2, \dots aa_{\varphi(m)}\}$ son iguales módulo m. Entonces el producto de sus elementos es el mismo módulo m

$$a^{\varphi(m)} a_1 a_2 \dots a_{\varphi(m)} \equiv a_1 a_2 \dots a_{\varphi(m)} \pmod{m} \Longrightarrow a^{\varphi(m)} \equiv 1 \pmod{m}.$$

□

Corollary 4.1 (Pequeño teorema de Fermat)**.** *Sea p primo relativo con a, entonces* $a^{p-1} \equiv 1 \pmod{m}$.

Proof. Trivial. □

Lemma 1 (φ es multiplicativa)**.** *Sean m, n primos relativos, entonces*

$$\varphi(m)\,\varphi(n) = \varphi(mn).$$

Proof. Consideremos el siguiente arreglo

$$\begin{array}{cccccc} 1 & m+1 & 2m+1 & \dots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \dots & (n-1)m+2 \\ \vdots & & \ddots & \vdots & \\ m & 2m & 3m & \dots & nm \end{array}$$

todas las filas son de la forma $km + r$ por tanto un elemento de la fila es primo relativo con m si y solo si $\text{mcd}(m, r) = 1$ y en ese caso m es primo relativo con toda la columna.En total hay $\varphi(m)$ de estas columnas.
Ahora, es fácil probar que $\{km + r\}_{k=0}^{n-1}$ es un sistema completo de residuos módulo n, entonces en dicha columna hay exactamente $\varphi(n)$ elementos primos relativos a n, de donde se deduce que el total de primos relativos a mn es $\varphi(m)\,\varphi(n)$. □

Se deja al lector calcular $\varphi(p^r)$ y usar este lema para obtener una fórmula general de $\varphi(n)$ en función de la descomposición en factores de n.

Problem 3 (AIME 1983)**.** *Sea $a_n = 6^n + 8^n$. Determine el resto de a_{83} en la división por* 49*.*

Solution. Notemos que $\varphi(49) = 42$, de donde $6^{84} \equiv 8^{84} \equiv 1 \pmod{49}$, de donde,

$$6^{83} + 8^{83} \equiv 6^{84}6^{-1} + 8^{84}8^{-1} \equiv 6^{-1} + 8^{-1} \pmod{49}$$

ahora,

$$6^{-1} + 8^{-1} \equiv (6+8)6^{-1}8^{-1} \equiv (14)48^{-1} \equiv (14)(-1)^{-1} \equiv -14 \equiv 35 \pmod{49}.$$

□

Problem 4. *Demuestra que para cada $c \in \mathbb{Z}$ y cada primo p, la ecuación $x^x \equiv c \pmod{p}$ tiene solución.*

Solution. Si $p|c$ tomamos $x = p$. Supongamos que $\mathrm{mcd}(p, c) = 1$ y que x satisface

$$\begin{aligned} x &\equiv c \pmod{p} \\ x &\equiv 1 \pmod{p-1} \end{aligned}$$

entonces,

$$x^x \equiv x^{(p-1)k+1} \equiv (x^{p-1})^k x \equiv x \equiv c \pmod{p}.$$

El sistema anterior siempre tiene solución por el CRT. □

4 Orden

Definition 3. *El **orden** de a módulo m, con $\mathrm{mcd}(a, m) = 1$, es el menor entero positivo x tal que $a^x \equiv 1 \pmod{m}$. Denotamos $x = ord_m(a)$.*

Nota: El orden de a módulo m, con $\mathrm{mcd}(a, m) = 1$, siempre está bien definido debido al teorema 4.

Theorem 5. *Sean a, m primos relativos. Entonces se cumple que*

$$a^n \equiv 1 \pmod{m} \Leftrightarrow ord_m(a)|n$$

.

Proof. Si $ord_a(m)|n$ entonces $n = ord_a(m)\, k$ para algún entero k, lo que implica que $a^n = a^{ord_m(a)\, k} = (a^{ord_m(a)})^k \equiv 1 \pmod{m}$.
Sea ahora n tal que $a^n \equiv 1 \pmod{m}$. Escribamos $n = ord_m(a)\, k + r$ con $k \in \mathbb{Z}$ y $0 \leq r \leq ord_m(a) - 1$. Veamos que,

$$a^n = a^{ord_m(a)\, k + r} = (a^{ord_m(a)})^k a^r \equiv a^r \equiv 1 \pmod{m}$$

Si $r > 0$ entonces $ord_m(a)$ no es el menor entero solución de $a^x \equiv 1 \pmod{m}$. De donde $r = 0$ que implica $ord_m(a)|n$. □

Corollary 5.1. *Sean a, m primos relativos. Entonces se cumple que $ord_m(a) |\, \varphi(m)$.*

Proof. Se deriva del teorema de Euler. □

Theorem 6 (Truco del MCD)**.** *Sean a, m, n enteros positivos. Entonces se cumple que* $\mathrm{mcd}(a^m - 1, a^n - 1) = a^{\mathrm{mcd}(m,n)} - 1$.

Proof. Sea $d = \mathrm{mcd}(a^m - 1, a^n - 1)$, sabemos que $a^{\mathrm{mcd}(m,n)} - 1$ divide a $a^m - 1$ y a $a^n - 1$, de donde $a^{\mathrm{mcd}(m,n)} - 1|d$.
Sabemos, por Bezout, que existen x, y tal que $mx + ny = \mathrm{mcd}(m, n)$, entonces $a^n \equiv 1 \pmod{d}$ y $a^m \equiv 1 \pmod{d}$ implican que

$$a^{mx+ny} \equiv (a^m)^x (a^n)^y \equiv 1 \pmod{d}$$

de donde $d|a^{\mathrm{mcd}(m,n)} - 1$.
Combinando ambos resultados obtenemos que

$$\mathrm{mcd}(a^m - 1, a^n - 1) = a^{\mathrm{mcd}(m,n)} - 1.$$

□

Problem 5. *Prueba que si p es primo, entonces cada divisor primo de $2^p - 1$ es mayor que p.*

Solution. Sea q tal que $q|2^p - 1$, esto implica que $ord_q(2)|p$, de donde $ord_q(2) \in \{1, p\}$, si $ord_q(2) = 1 \Rightarrow q|1$ que es absurdo, de donde $ord_q(2) = p$.
Por el pequeño teorema de Fermat $ord_q(2)|\,\varphi(q) = q - 1$, lo que implica que $p|q - 1$ y se deduce que $q > p$. □

Problem 6. *Sea $a > 1$ y n enteros positivos. Si p es un primo impar que divide a $a^{2^n} + 1$, prueba que $2^{n+1}|p - 1$*

Solution. Como p es impar sabemos que $p \nmid a^{2^n} - 1$, además $p|(a^{2^n} + 1)(a^{2^n} - 1) = a^{2^{n+1}} - 1$. Por tanto

$$ord_p(a)|2^{n+1}$$

Si $ord_p(a)|2^n$ tendríamos que $p|a^{2^n} - 1$, por tanto $ord_p(a) \nmid 2^n$ y se deduce que $ord_p(a) = 2^{n+1}$.
El problema finaliza viendo que por el pequeño teorema de Fermat

$$ord_p(a)|\,\varphi(p) = p - 1$$

. □

Problem 7 (Clásico)**.** *Sea $n \geq 2$ un entero. Prueba que $n \nmid 2^n - 1$.*

Solution. Sea p el menor primo tal que $p|n$, tenemos que

$$p|n|2^n - 1.$$

Sabemos que $ord_p(2)|n$ y que $ord_p(2) \leq \varphi(p) = p - 1$, lo que contradice la minimalidad de p. □

5 Lista de Problemas

Problem 1 (AIME 2001)**.** *Cuánto enteros positivos múltiplos de* 1001 *pueden ser expresados de la forma* $10^j - 10^i$*, donde* $0 \leq i < j \leq 99$*.*

Problem 2. *Sea* p *un primo impar, y sean* q *y* r *primos tales que* $p|q^r + 1$*. Prueba que* $2r|p-1$ *o* $p|q^2 - 1$*.*

Problem 3 (APMO 2009/P4)**.** *Prueba que para cada entero positivo* k *existe una progresión aritmética* $\{\frac{a_1}{b_1}, \frac{a_1}{b_1}, \ldots \frac{a_k}{b_k}\}$ *de números racionales, donde* $mcd(a_i, b_i) = 1$ *para* $1 \leq i \leq k$ *y además los* $2k$ *números* $a_1, a_2, \ldots a_k, b_1, b_2, \ldots, b_k$ *son todos distintos.*

Problem 4 (USA TST)**.** *Prueba que para cada entero positivo* n *existe un un conjunto* S *de* n *enteros positivos tales que para cualesquiera dos elementos distintos de* S*,* a *y* b*, se tiene que* $a - b$ *divide a* a *y a* b *pero a ningun otro elemento de* S*.*

Problem 5. *Decimos que un punto latice es "visible" si el máximo común divisor de sus coordenadas es* 1*. Prueba que existe un cuadrado de* 100×100 *donde ninguno de sus puntos es visible.*

Problem 6. *Prueba que para* $n > 1$ *se cumple que* $n \nmid 2^{n-1} + 1$*.*

Problem 7. *Sean* a *y* b *primos relativos. Prueba que cualquier divisor impar de* $a^{2^n} + b^{2^n}$ *es de la forma* $2^{n+1}m + 1$*.*

Problem 8 (Canadá 2003)**.** *Encuentra los* 3 *últimos dígitos de* $2003^{2002^{2001}}$*.*

Problem 9 (IMO 2005/P4)**.** *Determine todos los enteros positivos primos relativos a todos los términos de la sucesión* $a_n = 2^n + 3^n + 6^n - 1$*, con* $n \geq 1$*.*

Problem 10 (Ibero 2004/P3)**.** *Sean* n *y* k *enteros positivos tales que o bien* n *es impar o bien* n *y* k *son pares. Prueba que existen enteros* a *y* b *tales que* $\text{mcd}(a, n) = \text{mcd}(b, n) = 1$ *y* $k = a + b$*.*

Problem 11 (ISL 2005/N6)**.** *Sean* a, b *enteros positivos tales que* $a^n + n|b^n + n$ *para todo entero positivo* n*. Prueba que* $a = b$*.*

Problem 12 (ISL 2002/N3)**.** *Sean* $p_1, p_2, \ldots p_n$ *primos distintos mayores que* 3*. Prueba que* $2^{p_1, p_2, \ldots p_n} + 1$ *tiene al menos* 4^n *divisores.*

Problem 13 (Bulgaria 1996)**.** *Encuentra todos los pares de primos* p, q *tales que* $pq|(5^p - 2^p)(5^q - 2^q)$

Problem 14 (Ibero 2019/P6)**.** *Sean* $a_1, a_2, \ldots, a_{2019}$ *enteros positivos y sea* P *un polinomio con coeficientes enteros tal que, para todo entero positivo* n*,*

$$P(n) \text{ divides } a_1^n + a_2^n + \cdots + a_{2019}^n.$$

Prueba que P *es constante.*

Hint: *Teorema de Schur. Dado un polinomio de coeficientes enteros* P *no constante, existen infinitos primos* p *tales que* $p|P(n)$ *para algun* $n \in \mathbb{Z}$*.*

Problem 15 (USA TST 2003)**.** *Encuentra todos las ternas ordenadas de primos* p, q, r *tales que* $p|q^r + 1$*,* $q|r^p + 1$ *y* $r|p^q + 1$*.*

Problem 16 (China 2009)**.** *Encuentra todos los pares de primos* p, q *tales que* $pq|5^p + 5^q$*.*

Problem 17 (IMO 1999/P4)**.** *Encuentra todos los pares de enteros positivos* x, p*, con* p *primo, tales que* $x \leq 2p$ *y* $x^{p-1}|(p-1)^x + 1$*.*

Problem 18 (IMO 1990/P3)**.** *Encuentra todos los enteros positivos* n *tales que* $n^2|2^n + 1$*.*

Problem 19 (IMO 2003/P6)**.** *Sea* p *un número primo. Prueba que existe un primo* q *tal que para todo entero positivo* n*, el número* $n^p - p$ *no es divisible por* q*.*

References

[1] Justin Stevens, Olympiad Number Theory Through Challenging Problems.

[2] Aditya Khurmi, Modern Olympiad Number Theory

[3] Yufei Zhao, Modular arithmetic: Divisibility, Fermat, Euler, Wilson, residue classes, order, https://yufeizhao.com/olympiad/mod2.pdf

[4] Evan Chen, Orders Modulo a Prime,https://web.evanchen.cc/handouts/ORPR/ORPR.pdf

[5] Evan Chen, The Chinese Remainder Theorem ,https://web.evanchen.cc/handouts/CRT/CRT.pdf

[6] https://artofproblemsolving.com