Aritmética Modular

1. Introducción

Definición. *Sean $a, b, n \in \mathbb{Z}$ con $n \neq 0$, diremos que $a \equiv b \pmod{n}$ (a es congruente a b módulo n) si y sólo si $n \mid a - b$.*

Ejemplo: $8 \equiv 23 \pmod{5}$, pues $23 - 8 = 15$ es divisible por 5.

Ejemplo: $42 \equiv 33 \pmod{9}$, pues $42 - 33 = 9$.

Propiedades:

Sean $a, b, c, d, n \in \mathbb{Z}$ con $n \neq 0$, entonces:

1. $a \equiv a \pmod{n}$
2. $a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$
3. $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$
4. $a \equiv 0 \pmod{n} \iff n \mid a$
5. Sean $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tales que $a = nq_1 + r_1, b = nq_2 + r_2$ con $0 \leq r_1, r_2 < |n|$, entonces $a \equiv b \pmod{n} \iff r_1 = r_2$
6. $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$
7. $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow ac \equiv bd \pmod{n}$
8. $a \equiv b \pmod{n} \Rightarrow ac \equiv bc \pmod{n}$
9. $a \equiv b \pmod{n} \Rightarrow a^c \equiv b^c \pmod{n}$

P1. *Pruebe que $4^n - 1$ es divisible por 3.*
Solución:

Tenemos que:

$$\begin{aligned} 4 &\equiv 1 \pmod{3} \\ 4^n &\equiv 1^n \pmod{3} \\ 4^n - 1 &\equiv 0 \pmod{3} \end{aligned}$$ ■

P2. *Demuestre que si $x, y \in \mathbb{Z}$, entonces $x - y \mid x^n - y^n$.*
Solución:

Veamos que:

$$\begin{aligned} x - y &\equiv 0 \pmod{x - y} \\ x &\equiv y \pmod{x - y} \\ x^n &\equiv y^n \pmod{x - y} \\ x^n - y^n &\equiv 0 \pmod{x - y} \end{aligned}$$ ■

P3. *Encontrar las dos últimas cifras de $7^{7^{7^7}}$.*
Solución:

Veamos que:

$$\begin{aligned} 7 &\equiv 7 \pmod{100} \\ 7^2 &\equiv 49 \pmod{100} \\ 7^3 &\equiv 43 \pmod{100} \\ 7^4 &\equiv 1 \pmod{100} \end{aligned}$$

Como aparece un 1, desde ese punto los restos se empezarán a repetir. Por lo tanto, nos interesa ahora, el resto módulo 4 de 7^{7^7}. Notemos que:

$$\begin{aligned} 7 \equiv 3 \equiv -1 \pmod{4} \\ 7^2 \equiv 1 \pmod{4} \end{aligned}$$

Luego, los restos de las potencias de 7 módulo 4 se repiten cada dos. Como 7^7 es impar, entonces $7^{7^7} \equiv 3 \pmod{4}$. Por lo tanto, $7^{7^{7^7}} \equiv 43 \pmod{100}$. ■

P4. *Alberto quiere invitar a Ximena a su casa. Como Alberto sabe que Ximena es aficionada a las matemáticas, en lugar de señalarme exactamente cuales son los buses del Transantiago que le sirven le dice:*

- *Los números de los buses que llevan a mi casa tienen tres dígitos, siendo el dígito de la izquierda no nulo.*
- *Además, estos números son múltiplos de* 13.
- *El segundo dígito de ellos es el promedio de los otros dos.*

¿Cuáles son las lineas de buses que llevan a la casa de Alberto?

Solución:

Sean a, b, c los dígitos, entonces los números de lo buses son de la forma $100a + 10b + c$. Tenemos que

$$\begin{aligned} 100a + 10b + c &\equiv 100a + 10\left(\frac{a+c}{2}\right) + c \pmod{13} \\ &\equiv 105a + 6c \pmod{13} \\ &\equiv a + 6c \pmod{13} \end{aligned}$$

Además, tenemos que $a + c$ tiene que ser par, es decir, que a y c deben tener la misma paridad. Ahora, analicemos por casos:

- $c = 1 \Rightarrow a \equiv 7 \pmod{13} \Rightarrow a = 7 \Rightarrow b = 4$.
- $c = 2 \Rightarrow a \equiv 1 \pmod{13} \Rightarrow a = 1$, que no sirve por que a y c tienen distinta paridad.
- $c = 3 \Rightarrow a \equiv 8 \pmod{13} \Rightarrow a = 8$.
- $c = 4 \Rightarrow a \equiv 2 \pmod{13} \Rightarrow a = 2 \Rightarrow b = 3$.
- $c = 5 \Rightarrow a \equiv 4 \pmod{13} \Rightarrow a = 4$.
- $c = 6 \Rightarrow a \equiv 10 \pmod{13}$, lo cual no puede ser porque a es dígito.
- $c = 7 \Rightarrow a \equiv 3 \pmod{13} \Rightarrow a = 3 \Rightarrow b = 5$.
- $c = 8 \Rightarrow a \equiv 9 \pmod{13} \Rightarrow a = 9$.
- $c = 9 \Rightarrow a \equiv 2 \pmod{13} \Rightarrow a = 2$.

Por lo tanto, sirven los buses $741, 234, 357$.

P5. *Demuestre que existen infinitos números de la forma* $2013\ldots2013$ *que son divisibles por* 2011.
Solución:

Tomemos los números

$$2013, 20132013, \ldots, \underbrace{2013\ldots2013}_{2012 \text{ veces}}$$

Como existen 2011 restos posibles módulo 2011 y tenemos 2012 números distintos, por Principio del palomar, entonces hay dos números con el mismo resto módulo 2011. Si los restamos, obtenemos un número de la forma

$$\underbrace{2013\ldots2013}_{n \text{ veces}}\ \underbrace{0\ldots0}_{m \text{ veces}}$$

Como 10^m es comprimo con 2011 para $m \in \mathbb{Z}$, entonces $2011 \mid \underbrace{2013\ldots2013}_{n \text{ veces}}$.

Ahora, basta pegar el número obtenido con sí mismo para obtener infinitos números que cumplan lo pedido.

2. Potencias

Una característica importante de la aritmética modular es lo que pasa con los restos de las potencias. Por ejemplo:

1. $x \equiv 0 \pmod 3 \Rightarrow x^2 \equiv 0 \pmod 3$
2. $x \equiv 1 \pmod 3 \Rightarrow x^2 \equiv 1 \pmod 3$
3. $x \equiv 2 \pmod 3 \Rightarrow x^2 \equiv 4 \equiv 1 \pmod 3$

De donde concluimos que un cuadrado perfecto sólo puede dejar resto 0 ó 1. De manera análoga, tenemos que los cuadrados perfectos dejan resto:

- 0 ó 1 módulo 4
- $0, 1$ ó 4 módulo 5
- $0, 1, 2$ ó 4 módulo 7
- $0, 1$ ó 4 módulo 8

P6. *Encuentre todas las soluciones enteras de* $x^2 + 3y^3 = 8$.
Solución:

Veamos que:

$$2 \equiv 8 \equiv x^2 + 3y^3 \equiv x^2 \pmod 3$$

Como los cuadrados perfectos no dejan resto 2 módulo 3, entonces no existen soluciones enteras. ■

P7. *Encuentre todos los* p *primos tales que* $p^2 + 2^p$ *es primo.*
Solución:

Empecemos probando casos:

1. Si $p = 2$, entonces $p^2 + 2^p = 4$, lo que no es primo.
2. Si $p = 3$, entonces $p^2 + 2^p = 17$, lo que es primo.

3. Si $p = 5$, entonces $p^2 + 2^p = 57$, lo que es divisible por 3.

4. Si $p = 7$, entonces $p^2 + 2^p = 177$, lo que es divisible por 3.

Ahora, nos gustaría probar que para todos los $p > 3$, $p^2 + 2^p$ es divisible por 3. Sea $p > 3$, entonces $p^2 \equiv 1 \pmod 3$. Como el único primo par es 2, entonces p es impar. Luego

$$\begin{aligned} 2 &\equiv -1 \pmod 3 \\ 2^p &\equiv (-1)^{2k+1} \pmod 3 \\ 2^p &\equiv -1 \pmod 3 \\ p^2 + 2^p &\equiv 0 \pmod 3 \quad \blacksquare \end{aligned}$$

P8. *Una terna (a, b, c) de números enteros se dice* ***pitagórica****, si pueden ser lados de un triángulo rectángulo, es decir, si $a^2 + b^2 = c^2$.*

Demuestre que:

1. *a o b es par.*

2. *a o b es múltiplo de 3.*

3. *a o b es múltiplo de 4.*

4. *a, b o c es múltiplo de 5.*

Solución:

1. Supongamos que a y b son impares, entonces $a^2 \equiv 1 \equiv b^2 \pmod 4 \Rightarrow c^2 \equiv 2 \pmod 4$, lo cual no es posible.

2. Usando el mismo argumento anterior, c^2 tendría que ser 2 módulo 3.

3. Sea $d = (a, b)$, entonces $d^2 \mid a^2 + b^2 = c^2 \Rightarrow d \mid c$. Ahora, definimos $a' = \frac{a}{d}, b' = \frac{b}{d}$ y $c' = \frac{c}{d}$. Tenemos que $a'^2 + b'^2 = c'^2$. Supongamos que a' y b' no son divisibles por 4. Por la primera parte, tenemos que uno de ellos es par, por lo que tenemos que uno deja resto 1 y el otro, 4. Luego, $c'^2 = a'^2 + b'^2 \equiv 5 \pmod 8$, lo cual no es posible. Por lo tanto, a' o b' es divisible por 4, y finalmente, a o b es divisible por 4.

4. Supongamos que a y b no son divisibles por 5. Entonces, los cuadrados dejan resto 1 o 4 en módulo 5. Por lo tanto, c^2 deja resto $2, 3$ o 0. Los dos primeros casos no son posibles, y en el tercero, c es múltiplo de 5.

   $\blacksquare$

De igual manera, los cubos perfectos dejan resto $-1, 0$ ó 1 módulo 7, y las potencias cuartas dejan resto 0 ó 1 módulo 16.

P9. *Demuestre que* 2005 *no puede escribirse como diferencia de los cubos de dos enteros positivos.*

(Clasificación ONM 2005, Nivel Menor)

Solución:

Veamos que $2005 \equiv 3 \pmod 7$, lo que no se puede obtener con la diferencia de los restos de cubos. $\blacksquare$

P10. *Encuentre todas las soluciones enteras de* $x_1^{2012} + \cdots + x_{10}^{2012} = \underbrace{2011\ldots2011}_{2011 \text{ veces}}$

Solución:

Veamos que:

$$\underbrace{2011\ldots2011}_{2011 \text{ veces}} \equiv 2011 \equiv 11 \pmod{16}$$

Como los x_i^{2012} son potencias cuartas, entonces dejan resto 0 ó 1 módulo 16. Por lo que la suma deja resto entre 0 y 10, por lo que no existen soluciones. ■

3. Invertibilidad

Si tuviéramos la ecuación $2x \equiv 4 \pmod 6$, nos gustaría decir que la única solución módulo 6 es 2. Sin embargo, 5 también es solución, pues $2 \cdot 5 \equiv 10 \equiv 4 \pmod 6$. Ahora, estudiaremos el caso en que si podemos cancelar un número a ambos lados de una ecuación.

Tomemos la ecuación:

$$ax \equiv ab \pmod n \iff n \mid ax - ab = a(x-b)$$

Si $(a,n) = 1$, entonces $x \equiv b \pmod n$.

Ejemplo: $2x \equiv 3 \pmod 7 \Rightarrow 2x \equiv 10 \pmod 7 \Rightarrow x \equiv 5 \pmod 7$.

Ejemplo: $8x \equiv 12 \pmod 7 \Rightarrow 2x \equiv 3 \Rightarrow x \equiv 5 \pmod 7$.

Definición. *Sea $n \in \mathbb{Z}^+$, definiremos $\mathbb{Z}_n = 0, 1, \ldots, n-1$, es decir al conjunto de los restos módulo n.*

Definición. *Sea $a \in \mathbb{Z}_n$, diremos que es **invertible** en $\mathbb{Z}_n$ si y sólo si existe $b \in \mathbb{Z}_n$ tal que $ab \equiv 1 \pmod n$. A b lo llamaremos el **inverso** de a.*

Proposición: *$a \in \mathbb{Z}_n$ es invertible si y sólo si $(a,n) = 1$.*
Demostración:

$a \in \mathbb{Z}_n$ es invertible si y sólo si $\exists b \in \mathbb{Z}_n$ tal que

$$ab \equiv 1 \pmod n \iff n \mid ac - 1 \iff \exists k : ac - 1 = kn \iff ac - kn = 1$$

Por Identidad de Bezout, lo anterior ocurre si y sólo si $(a,n) = 1$. ■

Definición. *Sea $m \in \mathbb{Z}_n$, definiremos $m\mathbb{Z}_n$ como los restos módulo n de $\{m \cdot 0, m \cdot 1, \ldots, m \cdot (n-1)\}$*

Proposición: *Sean p primo y $m \in \mathbb{Z}_p$ con $m \neq 0$. Entonces $m\mathbb{Z}_p = \mathbb{Z}_p$.*
Demostración:

Como $m\mathbb{Z}_p$ está formados por restos módulo p, entonces $m\mathbb{Z}_p \subseteq \mathbb{Z}_p$. Sean i, j tales que

$$mi \equiv mj \pmod p \Rightarrow i \equiv j \pmod p \text{ , pues } (m,p) = 1$$

Por lo tanto, $m\mathbb{Z}_p$ y $\mathbb{Z}_p$ tienen la misma cantidad de elementos. Finalmente, $m\mathbb{Z}_p = \mathbb{Z}_p$. ■

Pequeño teorema de Fermat. *Sea $a \in \mathbb{Z}_p$, entonces $a^p \equiv 1 \pmod p$.*
Demostración:

Si $a = 0$, entonces $a^p \equiv 0 \equiv a \pmod p$. Si no, entonces $a\mathbb{Z}_p = \mathbb{Z}_p$. Ahora, multiplicaremos los términos no nulos de ambos conjuntos:

$$\begin{aligned} a \cdot 1 \cdot a \cdot 2 \cdot \cdots \cdot a(p-1) &\equiv 1 \cdot 2 \cdot \cdots \cdot (p-1) \pmod p \\ a^{p-1} &\equiv 1 \pmod p \text{ pues } (i,p) = 1, \forall i \in \mathbb{Z}_p, i \neq 0 \\ a^p &\equiv a \pmod p \quad ■ \end{aligned}$$

P11. *Encontrar todas las soluciones enteras positivas de* $1 + 2^x + 3^y = z^3$ *(Olimpiada Rioplatense 2000)*

Solución:

Como $x, y > 0$, entonces:

$$2|2^x \text{ y } 2|1 + 3^y \Rightarrow 2|1 + 2^x + 3^y = z^3$$

Como 2 es primo, tenemos que:

$$2|z \Rightarrow 8|z^3$$

Veamos que $3^y \equiv 1$ *ó* $3 \pmod 3$ según la paridad de y. Luego, para que $8|1 + 2^x + 3^y$ es necesario que $2^x \equiv 6$ *ó* $4 \pmod 8$. Claramente, $x = 1$ no cumple con lo anterior, y $x \geq 3 \Rightarrow 2^x \equiv 0 \pmod 8$. Luego, el único caso posible es $x = 2$.

Entonces, $5 + 3^y = z^3$. Utilizando el pequeño teorema de Fermat para $p = 3$, obtenemos:

$$z \equiv z^3 = 5 + 3^y \equiv 2 \pmod 3$$

Ahora, escribimos $z = 3k + 2$:

$$5 + 3^y = (3k + 2)^3 = 27k^3 + 54k^2 + 36k + 8$$

$$\Rightarrow 3^y = 27k^3 + 54k^2 + 36k + 3$$

Como el lado derecho es divisible por 3 pero no por 9, entonces $y < 2$, es decir, $y = 1$.

Por lo tanto, la solución a la ecuación es $(x, y, z) = (2, 1, 2)$. ■

Con el fin de generalizar el resultado anterior, haremos las siguientes definiciones

Definición. *Sea* $n \in \mathbb{Z}^+$, *llamaremos* $\mathbb{Z}_n^* = \{a \in \mathbb{Z} : (a, n) = 1\}$, *es decir, el conjunto de los números invertibles en* $\mathbb{Z}_n$.

Definición. *Llamaremos* $\varphi(n) = \#(\mathbb{Z}_n^*)$, *es decir, es la cantidad de números coprimos con* n, *menores que* n.

Ejemplo:

$$\varphi(1) = 1, \quad \varphi(2) = 1 \quad \varphi(3) = 2, \quad \varphi(4) = 2, \quad \varphi(5) = 4, \quad \varphi(6) = 2$$

Proposición: *Sean* $a, b \in \mathbb{Z}_n^*$, *entonces el resto de* ab *módulo* n *está en* $\mathbb{Z}_n^*$.

Demostración:

Si $a, b \in \mathbb{Z}_n^*$, entonces $\exists c, d \in \mathbb{Z}_n$ tales que

$$ac \equiv bd \equiv 1 \pmod n \Rightarrow acbd \equiv (ab) \cdot (cd) \equiv 1 \pmod n$$

Luego, ab es invertible módulo n, es decir, su resto está en $\mathbb{Z}_n^*$. ■

Proposición: *Sea* $m \in \mathbb{Z}_n^*$, *entonces* $m\mathbb{Z}_n^* = \mathbb{Z}_n^*$.

Demostración:

Denotemos $\mathbb{Z}_n^* = \{a_1, \ldots, a_{\varphi(n)}\}$. Por la proposición anterior, $ma_i \in \mathbb{Z}_n^*$, por lo que $m\mathbb{Z}_n^* \subseteq \mathbb{Z}_n^*$. Sean a_i, a_j tales que

$$ma_i \equiv ma_j \pmod n \Rightarrow a_i \equiv a_j \pmod n \text{ , pues } m \in \mathbb{Z}_n^*$$

Por lo tanto, $m\mathbb{Z}_n^*$ y $\mathbb{Z}_n^*$ tienen la misma cantidad de elementos. Finalmente, $m\mathbb{Z}_n^* = \mathbb{Z}_n^*$. ■

Teorema de Euler. *Sea* $a \in \mathbb{Z}_n^*$, *entonces* $a^{\varphi(n)} \equiv 1 \pmod n$.

Demostración:

Por la proposición anterior, tenemos que $a\mathbb{Z}_n^* = \mathbb{Z}_n$. Entonces

$$\begin{aligned} a \cdot a_1 \cdot a \cdot \dots \cdot a \cdot a_{\varphi(n)} &\equiv a_1 \cdot \dots a_{\varphi(n)} \pmod{n} \\ a^{\varphi(n)} &\equiv 1 \pmod{n}\text{ , pues } a_i \in \mathbb{Z}_n^* \end{aligned}$$ ■

Ahora, para poder usar este teorema, veremos como calcular $\varphi(n)$.

Proposición: *La función φ cumple las siguientes propiedades:*

- *Si p es primo, entonces $\varphi\left(p^k\right) = p^k\left(1 - \frac{1}{p}\right)$.*
- *Si m, n coprimos, entonces $\varphi(mn) = \varphi(m)\varphi(n)$.*
- *Si $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$, entonces $\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_m}\right)$*

Solución:

- Veamos que sólo los múltiplos de p no son coprimos con p^k. Veamos que los múltiplos de p menores que p^k son $\frac{p^k}{p}$. Por lo tanto

$$\varphi\left(p^k\right) = p^k - \frac{p^k}{p} = p^k\left(1 - \frac{1}{p}\right)$$

- La demostración de esto quedará pendiente.
- Como $p_i \neq p_j$ si $i \neq j$, entonces todos los $p_i^{k_i}$ son coprimos, por lo que

$$\begin{aligned} \varphi(n) &= \varphi\left(p_1^{k_1} \dots p_m^{k_m}\right) = \varphi\left(p_1^{k_1}\right) \dots \varphi\left(p_m^{k_m}\right) \\ &= p_1^{k_1} \dots p_m^{k_m}\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_m}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_m}\right) \quad ■ \end{aligned}$$

Ejemplo: Como $1000 = 2^3 \cdot 5^3$, entonces $\varphi(1000) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400$.

P12. *Calcule los últimos tres dígitos de* 13^{398}.
Solución:

Como $(13, 100) = 1$, entonces

$$\begin{aligned} 13^{\varphi(1000)} &\equiv 1 \pmod{1000} \\ 13^{400} &\equiv 1 \pmod{1000} \end{aligned}$$

Ahora, necesitamos encontrar el inverso de 13 módulo 1000. Recordemos que $1001 = 7 \cdot 11 \cdot 13$, por lo tanto, el inverso buscado es 77. Luego

$$13^{398} \equiv 77^2 \equiv 929 \pmod{1000}$$ ■

P13. *Sea $n \in \mathbb{N}$. Demuestre que*

- *n impar $\Rightarrow \varphi(2n) = \varphi(n)$.*
- *n par $\Rightarrow \varphi(2n) = 2\varphi(n)$.*
- *$3 \mid n \Rightarrow \varphi(3n) = 3\varphi(n)$.*
- *$3 \nmid n \Rightarrow \varphi(3n) = 2\varphi(n)$.*

- $\varphi(n) = \frac{n}{2} \iff n = 2^k$.

P14. *Sean $n, m \in \mathbb{N}$. Pruebe que*

- $n \mid m \Rightarrow \varphi(n) \mid \varphi(m)$.
- $(n, m)\varphi(n)\varphi(m) = \varphi(nm)\varphi((n, m))$.
- $\varphi(n)\varphi(m) = \varphi((n, m)\varphi([n, m])$.