# ARITMÉTICA DE GAUSS

Luis Joel C. Castillo

# CONTENIDO

*Este artículo tiene el propósito de abarcar todo lo relacionado con la Aritmética Modular, introducida por Carl Friedrich Gauss en 1801.*

# ÍNDICE



Luis Joel C. Castillo

# ARITMÉTICA MODULAR

La aritmética modular es un sistema que se ocupa de estudiar las propiedades y relaciones de los números enteros. Pero para entender más a fondo la aritmética modular, necesitamos saber qué es el módulo y residuo.

El residuo, no es más que el resto de una división:

$$\begin{array}{r|l} 15 & 5 \\ \hline 15 & 3 \\ \hline 0 & \end{array}$$

En este ejemplo el residuo es *0*, ya que es el primer cociente que se obtiene al dividir $15 \div 5$.

$$\begin{array}{r|l} 10 & 3 \\ \hline 9 & 3 \\ \hline 1 & \end{array}$$

Podemos observar que este caso nos dió resto *1*, debido a que si dividimos $10 \div 3$, nos sobra *1*, osea, no alcanza para repartir el valor entre *3*.

El módulo no es más que una notación del resto de una división, tal que:

$$\begin{array}{r|l} 45 & 8 \\ \hline 45 & 5 \\ \hline 0 & \end{array}$$

Se denominaría:

$$45 \bmod 8 = 0$$

Lo mismo ocurre aquí:

$$\begin{array}{r|l} 34 & 7 \\ \hline 28 & 4 \\ \hline 6 & \end{array} \qquad 34 \bmod 7 = 6$$

Ahora, pasemos a definir la congruencia, esta es la parte principal para comprender la aritmética modular. La congruencia se define como la relación entre dos números bajo una operación de módulo.

$$A \equiv B \ (mod\ C)$$

En esta notación Gauss representó este simbolo "≡" como congruencia, pero la congruencia anterior es equivalente a:

$$A \bmod C = B$$

Se dice que dos números son congruentes, si se cumple:

$$A \equiv B\ (mod\ C) \Leftrightarrow A\ mod\ C = B$$

Por ejemplo:

$$30 \equiv 0\ (mod\ 10) \Leftrightarrow 30\ mod\ 10 = 0$$
$$28 \equiv 0\ (mod\ 7) \Leftrightarrow 28\ mod\ 7 = 0$$
$$41 \equiv 9\ (mod\ 16) \Leftrightarrow 41\ mod\ 16 = 9$$
$$63 \equiv 3\ (mod\ 10) \Leftrightarrow 63\ mod\ 10 = 3$$
$$17 \equiv 2\ (mod\ 15) \Leftrightarrow 17\ mod\ 15 = 2$$

Cabe recalcar esta propiedad: siempre que se haga:

$$A \equiv B\ (mod\ C)$$

*B* siempre será igual a *A,* si, y solo si *A* es menor que *C*, osea:

$$\forall A < C \Rightarrow B = A$$

Ejemplo:

$$6 \equiv 6\ (mod\ 21) \because 6 < 21$$

Se lee: seis es congruente con seis a módulo de veinte y uno, porque seis es menor que veinte y uno.

# ECUACIONES DIOFÁNTICAS

Las ecuaciones diofánticas, no son más que ecuaciones de dos o más incógnitas, cuyas incógnitas pertenecen al conjunto de números enteros.

$$3x+7y = 1$$

Hay varias formas de resolver este tipo de ecuaciones, pero en este caso todas las ecuaciones diofánticas que veamos de aquí en adelante la resolveremos por aritmética modular. Para resolver este tipo de ecuaciones necesitamos convertirlas de una ecuación a una congruencia. Para eso, tomemos en cuenta esta definición:

$$\begin{array}{r|l} x & y \\ \hline -b & a \\ \hline z & \end{array} \qquad x = a \cdot y + z$$

Esto quiere decir, que si tenemos la siguiente congruencia con incógnita:

$$x \equiv 2 \pmod 7$$

Para convertirla a una ecuación, sería:

$$x = 7n+2$$

Siendo $7 = a$, $n = y$, $2 = z$, respectivamente, según la definición

Para resolver este tipo de ecuaciones se hace lo siguiente:

$$3x+7y = 1$$

Acá tenemos la ecuación del principio, que anteriormente habíamos planteado que teníamos que convertirla a una congruencia, entonces quedaría:

$$3x \equiv 1 \ (mod\ 7)$$

Ahora al número 1 tenemos que ir sumándole o restándole el módulo, en este caso es el *7*, hasta que el número *1* sea divisible entre *3x*, se hace esto para así poder despejar a la *x*:

$$3x \equiv 15 \ (mod\ 7)$$

Aquí podemos observar que pudimos encontrar el valor mas próximo, que fue el *15*, de manera desarrollada:

$$3x \equiv 1+7+7 \ (mod\ 7)$$

Entonces, ya que ahora *15* se puede dividir por *3x*, hacemos lo siguiente:

$$\frac{3x}{3} \equiv \frac{15}{3} \ (mod\ 7)$$

Ahora transformamos la congruencia en ecuación, siguiendo la definición dada anteriormente:

$$x = 7n+5,\ n \in \mathbb{Z} \therefore x = 5$$

Se lee: *x* es igual a siete *n* más cinco, perteneciendo *n* al conjunto de números enteros, por tanto, *x* es igual a cinco. *x*, sea cualquier letra, siempre será igual al residuo, en este caso: +5, debido a que es el menor valor posible de *x*

Ya que tenemos que $x = 5$, para encontrar el valor de $y$, simplemente resolvemos la ecuación lineal:

$$3(5)+7y = 1$$
$$15+7y = 1$$
$$7y = -14$$
$$\frac{7y}{7} = \frac{-14}{7}$$

Entonces, tenemos que $y = -2$. Podemos verificar la ecuación:

$$3(5)+7(-2) = 1$$
$$15-14 = 1$$
$$1 = 1$$

Hagamos otro ejemplo, ahora con tres incógnitas:

$$7x+5y+3z = 1$$

El proceso es el mismo, solo que tenemos tres variables, osea, hay que hacerlo dos veces, para $x$, $y$, y luego para $z$ resolver la ecuación lineal que queda.

$$7x \equiv 1 \pmod 5$$

Cabe recalcar que el módulo siempre será la variable siguiente, en este caso el coeficiente de $y$

Entonces, se hace el mismo proceso:

$$7x \equiv 1+5+5+5+5 \ (mod\ 5)$$

$$\frac{7x}{7} \equiv \frac{21}{7} \ (mod\ 5)$$

$$x = 5n+3,\ n \in \mathbb{Z} \therefore x = 3$$

Ya que se tiene el valor de $x$, seguimos haciendo el proceso, pero ahora con $y$

$$5y \equiv 1 \ (mod\ 3)$$

$$5y \equiv 1+3+3+3 \ (mod\ 3)$$

$$\frac{5y}{5} \equiv \frac{10}{5} \ (mod\ 3)$$

$$y = 3n+2,\ n \in \mathbb{Z} \therefore y = 2$$

Ahora resolvemos la ecuación lineal:

$$7(3)+5(2)+3z = 1$$
$$31+3z = 1$$
$$3z = -30$$
$$\frac{3z}{3} = \frac{-30}{3}$$
$$z = -10$$

$$7(3)+5(2)+3(-10) = 1$$
$$21+10-30 = 1$$
$$31-30 = 1$$
$$1 = 1$$

Lo mismo se haría sin importar la cantidad de incógnitas que hubiese en la ecuación. Hagamos un último ejemplo, un poco distinto:

$$7x^2-2y+z = 30$$

Es similar, lo único distinto es que en este ejemplo tenemos *x* al cuadrado:

$$7x^2 \equiv 30 \ (mod\ -2)$$

$$7x^2 \equiv 30+2+2+2+2+2+2 \ (mod\ -2)$$

$$\frac{7x^2}{7} \equiv \frac{42}{7} \ (mod\ -2)$$

$$\sqrt{x^2} \equiv \sqrt{6} \ (mod\ -2)$$

$$x = -2n+\sqrt{6},\ n \in \mathbb{Z} \therefore \boxed{x = 2.449489742783178}$$

$$\frac{-2y}{-2} \equiv \frac{30}{-2} \ (mod\ 1)$$

$$y = n-15,\ n \in \mathbb{Z} \therefore \boxed{y = -15}$$

$$7(2.449489742783178)^2-2(-15)+z = 30$$

$$72+z = 30$$

$$\boxed{z = -42}$$

# SISTEMAS DE CONGRUENCIAS

Un sistema de congruencia hace referencia a un conjunto de congruencias que comparten los mismos valores incógnitos:

$$\begin{cases} x \equiv 2 \ (mod\ 5) \\ 2x \equiv 1 \ (mod\ 7) \\ 3x \equiv 4 \ (mod\ 11) \end{cases}$$

El propósito radica en buscar un valor que pueda satisfacer las tres congruencias. A continuación, vamos a resolver el anterior sistema de congruencia. Antes que nada, hay que verificar que si exista solución, para ello buscamos que el máximo común divisor del coeficiente de la incógnita y el módulo divida al residuo (que de un número entero):

$$mcd(1,5) = 1;\ 2 \div 1 = 2$$
$$mcd(2,7) = 1;\ 1 \div 1 = 1$$
$$mcd(3,11) = 1\ ;\ 4 \div 1 = 4$$

El segundo paso para verificar si tiene solución vamos a hacer uso del Teorema Chino del Resto, que dice que un sistema de congruencia tiene solución si sus módulos son coprimos o primos relativos entre sí.

Para ello primero hay que entender qué son los números coprimos o primos relativos. Los números coprimos o primos relativos, son aquellos números cuyo máximo común divisor es uno:

$$mcd(\alpha,\beta) = 1$$

Ya habiendo definido lo que son los números coprimos, vamos a seguir verificando si tiene solución:

$$mcd(5,7) = 1$$
$$mcd(11,7) = 1$$
$$mcd(5,11) = 1$$

Y efectivamente, son coprimos, es decir, que el sistema de congruencia tiene solución. Ya sabiendo que tiene solución, lo que sigue es ir resolviendo cada congruencia en orden creciente, tenemos la primera congruencia:

$$x \equiv 2 \ (mod\ 5)$$

La cual ya podemos sacarle el valor a *x:*

$$x = 5n+2,\ n \in \mathbb{Z}$$

Como ya sabemos lo que vale *x*, en la demas congruencias reemplazamos la *x* por su valor, y resolvemos:

$$2(5n+2) \equiv 1 \ (mod\ 7)$$

$$10n+4 \equiv 1 \pmod 7$$
$$10n \equiv -3 \pmod 7$$
$$10n \equiv -3+7+7+7+7+7+7+7+7+7 \pmod 7$$
$$\frac{10n}{10} \equiv \frac{60}{10} \pmod 7$$
$$n = 7p+6,\ p \in \mathbb{Z}$$

Ahora, como sabemos lo que vale *n*, retrocedemos al valor de *x*, y reemplazamos la *n* por su valor, y así sera todo el proceso, hasta haber resuelto cada congruencia:

$$x = 5n+2$$
$$x = 5(7p+6)+2$$
$$x = 35p+32$$

Acá tenemos un nuevo valor de *x*, ahora solo falta resolver la última congruencia:

$$3x \equiv 4 \pmod{11}$$
$$3(35p+32) \equiv 4 \pmod{11}$$
$$105p+96 \equiv 4 \pmod{11}$$
$$105p \equiv -92 \pmod{11}$$
$$105p \equiv -92+37x11 \pmod{11}$$
$$\frac{105p}{105} \equiv \frac{315}{105} \pmod{11}$$

$$p = 11r+3,\ r \in \mathbb{Z}$$

Como ahora hemos completado cada congruencia del sistema, vamos a reemplazar la $p$ por su valor en $x$:

$$x = 35p+32$$
$$x = 35(11r+3)+32$$
$$x = 385r+137 \Rightarrow x = 137$$

Ahora que tenemos el valor final de $x$, vamos a verificar si este valor de $x$ satisface cada congruencia:

$$\begin{cases} 137 \equiv 2 \pmod 5 \checkmark \\ 2(137) \equiv 1 \pmod 7 \checkmark \\ 3(137) \equiv 4 \pmod{11} \checkmark \end{cases}$$

# CLASES DE EQUIVALENCIA Y ESPACIOS COCIENTES

Una clase de equivalencia se define como: conjunto de números que son congruentes entre sí, bajo una operación de módulo específica:

$$[\alpha]n = \{x: x \in \mathbb{Z}\}$$

Siempre y cuando se cumpla la condición:

$$\forall \lambda \in [\alpha]n \Rightarrow \lambda \equiv \alpha \ (mod\ n)$$

Se lee: Para todo *Lambda* que pertenezca a la clase de equivalencia: [*α*]*n*, entonces *Lambda* es congruente a *alpha* a módulo *n*. Esto quiere decir que para que exista una clase de equivalencia, todos sus elementos deben ser congruentes a *alpha* a módulo de *n*.

Ejemplo:

$$[1]5 = \{-\infty...6,11,16,21,26...\infty\}$$

En este caso, la clase de equivalencia [*1*]*5*, hace referencia a todos los números que a módulo de *5* dan como resto/residuo *1*.

Aquí hay más ejemplos:

$$[0]7 = \{-\infty...7,14,21,28,35...\infty\}$$
$$[0]2 = \{-\infty...2,4,6,8,10...\infty\}$$
$$[3]15 = \{-\infty...3,18,33,48,63...\infty\}$$
$$[-7]2 = \varnothing$$

Dada una clase de equivalencia de residuo negativo:

$$[-1]13 = \varnothing \because \nexists\, x \equiv -1 \ (mod\ 13)$$

Esto quiere decir que la clase de equivalencia $[-1]13$ está vacía, ya que no existe un número que a módulo de *13* de como resto *-1*. Lo mismo pasaría con cualquier número negativo:

$$[\alpha]n = \varnothing \Leftrightarrow \alpha \in \mathbb{Z} \wedge \alpha < 0$$

Dicho esto, las clases de equivalencia sirven para almacenar el conjunto de valores que bajo a una operación de módulo en específico, dan un resto específico.

Ahora, definamos qué son los espacios concientes. Un espacio conciente no es más que el conjunto de todas la clases de equivalencia que se les denote:

$$[a]n = \{x: x \in \mathbb{Z}\}$$
$$[\mathrm{b}]p = \{\mathrm{y}: y \in \mathbb{Z}\}$$
$$[\mathrm{c}]m = \{\mathrm{z}: z \in \mathbb{Z}\}$$
$$X/\sim = \{[a]n,[b]m,[c]p\}$$

La notación de los espacios concientes es una letra cualquiera acompañada por "/~". Por tanto, el espacio cociente $X/\sim$, contiene a todos los elementos de las clases de equivalencia: $[a]n$, $[b]p$, $[c]m$, entonces:

$$[a]n,\ [\mathrm{b}]p,\ [\mathrm{c}]m \subseteq X/\sim$$

Ejemplo en $\mathbb{N}$:

$$[1]7 = \{1,8,15,22,29...\infty\}$$
$$[12]67 = \{12,79,146,213,280...\infty\}$$
$$[0]10 = \{10,20,30,40,50...\infty\}$$
$$Z/\sim = \{[1]7,[12]67,[0]10\}$$

$$[1]7,\ [12]67,\ [0]10 \subseteq Z/\sim$$

# TEOREMA DE FERMAT Y TEOREMA DE EULER

El teorema de Fermat y el teorema de Euler son los teoremas principales de la teoría de números. Ambos teoremas se enfocan en los números primos cuando son involucrados en una congruencia. Para comenzar, veamos primero el teorema de Fermat, que formula:

Si $p$ es un número primo, y $a$ un número natural, entonces:

$$a^p \equiv a \ (mod\ p)$$

A lo que es equivalente decir:

$$a^{p-1} \equiv 1 \ (mod\ p)$$

Por tanto, Euler en su teorema planteó que:

$$\forall n,\ a \in \mathbb{Z} \wedge mcd(a,n) = 1 : a^{\Phi(n)} \equiv 1 \ (mod\ n)$$

Tal que la función $\Phi(n)$:

$$\Phi(n) = \exists q : q \in \mathbb{Z},\ q \leq n \wedge mcd(q,n) = 1$$

# CLASES DE EQUIVALENCIA POTENCIAL

Las clases de equivalencia potencial, las inventé como una extensión de las clases de equivalencia, y las defino como: conjunto de todos los números enteros *x*, que satisfacen:

$$[a|b]n = \{x: x \in \mathbb{Z} \wedge b^x \bmod n = a\}$$

Ejemplo:

$$[1|2]7 = \{3,6,9,12,15,18,21,24...\infty\}$$

$$[4|8]5 = \{2,6,10,14,18,22,26,28...\infty\}$$

Ya que:

$$\forall \alpha \in [1|2]7 \Rightarrow 2^{\alpha} \bmod 7 = 1$$

Como puedes observar, cada clase de equivalencia potencial se componen por una serie, por ejemplo en la clase [*1*|*2*]*7*, los números van de tres en tres, en la clase [*4*|*8*]*5*, los números van de cuatro en cuatro. Una notación en serie de ambas clases, sería:

$$[1|2]7 = \sum_{k=0}^{\infty} k+3 \qquad [4|8]5 = \sum_{l=2}^{\infty} l+4$$

Una clase de equivalencia potencial aparte de poder representarse como una serie, también podemos verla como una función recursiva, tal que:

$$\zeta(x) = \zeta(x+4) \quad \Leftrightarrow x \neq \infty \Rightarrow x$$
$$\delta(x) = \delta(x+3) \Leftrightarrow x \neq \infty \Rightarrow x$$
$$[4|8]5 = \zeta(2)$$
$$[1|2]7 = \delta(0)$$

A continuación, veremos las propiedades de las clases de equivalencia potencial, que denominé: <u>propiedades naturales</u>:

1. $[a|b]n = \mathbb{N} \Leftrightarrow a = 0,\ b \geq n \wedge mcd(b,n) = n$

La primera propiedad dice: una clase de equivalencia potencial será igual al conjunto de números naturales, si, y solo si *a* es igual a cero, *b* mayor o igual a *n* y el máximo común divisor de *b* y *n* sea *n*.

2. $[a|b]n = \mathbb{N} \Leftrightarrow \nexists d\colon 2 \leq d < b,\ b \bmod d = 0,\ n = 2 \cdot b \wedge a = b$

La segunda propiedad dice: una clase de equivalencia potencial será igual al conjunto de números naturales, si, y solo si no existe *d*, tal que *d* sea mayor o igual *2* y menor que *b*, donde el módulo de *b* y *d* sea cero. Osea, que *b* sea primo, *n* sea igual al doble de *b* y *a* igual a *b*

Aquí hay unos ejemplos que muestran las propiedades de manera más clara:

1. $[a|b]n = \mathbb{N} \Leftrightarrow a = 0,\ b \geq n \wedge mcd(b,n) = n$

$[0|4]2 = \{1,2,3,4,5,6,7,8,9...\infty\} = \mathbb{N}$

---

2. $[a|b]n = \mathbb{N} \Leftrightarrow \nexists d: 2 \leq d < b,\ b\ mod\ d = 0,\ n = 2b \wedge a = b$

$[7|7]14 = \{1,2,3,4,5,6,7,8,9...\infty\} = \mathbb{N}$

Por tanto:

$[0|4]2 \cup [7|7]14 = \mathbb{N}$

$[0|4]2 \cap [7|7]14 = \mathbb{N}$

$[0|4]2 - [7|7]14 = \varnothing$

$[7|7]14 - [0|4]2 = \varnothing$

$[0|4]2 \Delta [7|7]14 = \varnothing$

Usos de las clases de equivalencia potencial:

**• Criptografía:**

Pueden usarse para representar el conjunto de todas las posibles claves privadas que podrían descifrar un mensaje cifrado en un sistema criptográfico basado en exponenciación modular.

**• Teoría de Números:**

Las clases de equivalencia son una herramienta fundamental en la teoría de números. Por tanto, las clases de equivalencia potencial pueden usarse para estudiar las propiedades de las ecuaciones de exponenciación modular y proporcionar una nueva forma de entender las soluciones a estas ecuaciones.

---

**Carl Friedrich Gauss:** *"La matemática es la reina de las ciencias y la teoría de números es la reina de las matemáticas"*