Teoría de Números I

José de Jesús Lavalle Martínez

Benemérita Universidad Autónoma de Puebla
Facultad de Ciencias de la Computación
Estructuras Discretas CCOS 009

Contenido

1. Motivación
2. Divisibilidad y Aritmética Modular
3. El Algoritmo de División
4. Aritmética Modular
5. Aritmética Módulo m
6. Ejercicios

Motivación I

- Las ideas que desarrollaremos en esta sección se basan en la noción de divisibilidad.

Motivación I

- La división de un número entero por un número entero positivo produce un cociente y un resto.

Motivación I

- Trabajar con estos restos conduce a la aritmética modular, que juega un papel importante en matemáticas y que se utiliza en todas las ciencias de la computación.

División I

- Cuando un número entero se divide por un segundo número entero distinto de cero, el cociente puede ser o no un número entero.

División I

- Por ejemplo, $12/3 = 4$ es un número entero, mientras que $11/4 = 2.75$ no lo es.

División I

Definición 1

Si a y b son números enteros con $a \neq 0$, decimos que a *divide* a b si hay un número entero c tal que $b = ac$ (o de forma equivalente, si $\frac{b}{a}$ es un número entero). Cuando a divide a b, decimos que a es un *factor* o *divisor* de b, y que b es un múltiplo de a. La notación $a|b$ denota que a divide a b. Escribimos $a \not| b$ cuando a no divide a b.

División II

Observación 1

Podemos expresar $a|b$ usando cuantificadores como $\exists c(ac = b)$, donde el universo de discurso es el conjunto de números enteros.

Observación 1

Podemos expresar $a|b$ usando cuantificadores como $\exists c(ac = b)$, donde el universo de discurso es el conjunto de números enteros.

En la Figura 1, una recta numérica indica qué enteros son divisibles por el entero positivo d.

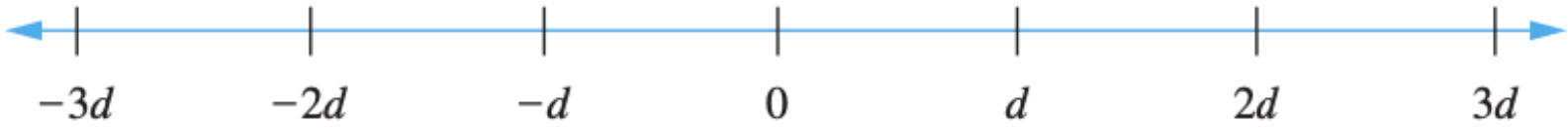

Figura 1: Enteros divisibles por el entero positivo d.

Ejemplo 1

Ejemplo 1

Determine si $3|7$ y si $3|12$.

Ejemplo 1

Determine si $3|7$ y si $3|12$.

Solución:

- Vemos que $3 \not| 7$, porque $7/3$ no es un número entero.

Ejemplo 1

Determine si $3|7$ y si $3|12$.

Solución:

- Por otro lado, $3|12$ porque $12/3 = 4$.

□

Ejemplo 2

Sean n y d enteros positivos. ¿Cuántos números enteros positivos que no exceden a n son divisibles por d?

Ejemplo 2

Sean n y d enteros positivos. ¿Cuántos números enteros positivos que no exceden a n son divisibles por d?

Solución:

- Los enteros positivos divisibles por d son todos los enteros de la forma dk, donde k es un entero positivo.

Ejemplo 2

Sean n y d enteros positivos. ¿Cuántos números enteros positivos que no exceden a n son divisibles por d?

Solución:

- Los enteros positivos divisibles por d son todos los enteros de la forma dk, donde k es un entero positivo.
- Así, el número de enteros positivos divisibles por d que no exceden a n es igual al número de enteros k con $0 < dk \leq n$, o con $0 < k \leq n/d$.

Ejemplo 2

Sean n y d enteros positivos. ¿Cuántos números enteros positivos que no exceden a n son divisibles por d?

Solución:

- Los enteros positivos divisibles por d son todos los enteros de la forma dk, donde k es un entero positivo.
- Así, el número de enteros positivos divisibles por d que no exceden a n es igual al número de enteros k con $0 < dk \leq n$, o con $0 < k \leq n/d$.
- Por lo tanto, hay $\lfloor n/d \rfloor$ enteros positivos que no exceden a n y son divisibles por d.

□

Teorema 1

Sean a, b y c números enteros, donde $a \neq 0$. Entonces

I. si $a|b$ y $a|c$, entonces $a|(b+c)$;

II. si $a|b$, entonces $a|bc$ para todos los enteros c;

III. si $a|b$ y $b|c$, entonces $a|c$.

Teorema 1

Sean a, b y c números enteros, donde $a \neq 0$. Entonces

I. si $a|b$ y $a|c$, entonces $a|(b+c)$;

II. si $a|b$, entonces $a|bc$ para todos los enteros c;

III. si $a|b$ y $b|c$, entonces $a|c$.

Demostración:

- Daremos una prueba directa de I.

Teorema 1

Sean a, b y c números enteros, donde $a \neq 0$. Entonces

I. si $a|b$ y $a|c$, entonces $a|(b+c)$;

II. si $a|b$, entonces $a|bc$ para todos los enteros c;

III. si $a|b$ y $b|c$, entonces $a|c$.

Demostración:

- Suponga que $a|b$ y $a|c$.

Teorema 1

Sean a, b y c números enteros, donde $a \neq 0$. Entonces

I. si $a|b$ y $a|c$, entonces $a|(b+c)$;

II. si $a|b$, entonces $a|bc$ para todos los enteros c;

III. si $a|b$ y $b|c$, entonces $a|c$.

Demostración:

- Suponga que $a|b$ y $a|c$.
- Entonces, de la definición de divisibilidad, se deduce que hay números enteros s y t con $b = as$ y $c = at$.

Teorema 1

Sean a, b y c números enteros, donde $a \neq 0$. Entonces

I. si $a|b$ y $a|c$, entonces $a|(b+c)$;

II. si $a|b$, entonces $a|bc$ para todos los enteros c;

III. si $a|b$ y $b|c$, entonces $a|c$.

Demostración:

- Suponga que $a|b$ y $a|c$.
- Entonces, de la definición de divisibilidad, se deduce que hay números enteros s y t con $b = as$ y $c = at$.
- Por tanto, $b + c = as + at = a(s + t)$.

Teorema 1

Sean a, b y c números enteros, donde $a \neq 0$. Entonces

I. si $a|b$ y $a|c$, entonces $a|(b+c)$;

II. si $a|b$, entonces $a|bc$ para todos los enteros c;

III. si $a|b$ y $b|c$, entonces $a|c$.

Demostración:

- Suponga que $a|b$ y $a|c$.
- Entonces, de la definición de divisibilidad, se deduce que hay números enteros s y t con $b = as$ y $c = at$.
- Por tanto, $b + c = as + at = a(s + t)$.
- Por ello, a divide $b + c$.

Corolario 1

Si a, b y c son números enteros, donde $a \neq 0$, tal que $a|b$ y $a|c$, entonces $a|mb + nc$ siempre que m y n sean números enteros.

Corolario 1

Si a, b y c son números enteros, donde $a \neq 0$, tal que $a|b$ y $a|c$, entonces $a|mb + nc$ siempre que m y n sean números enteros.

Demostración:

- Daremos una prueba directa.

Corolario 1

Si a, b y c son números enteros, donde $a \neq 0$, tal que $a|b$ y $a|c$, entonces $a|mb + nc$ siempre que m y n sean números enteros.

Demostración:

- Por la parte II del Teorema 1 vemos que $a|mb$ y $a|nc$ siempre que m y n son números enteros.

Corolario 1

Si a, b y c son números enteros, donde $a \neq 0$, tal que $a|b$ y $a|c$, entonces $a|mb + nc$ siempre que m y n sean números enteros.

Demostración:

- Por la parte II del Teorema 1 vemos que $a|mb$ y $a|nc$ siempre que m y n son números enteros.
- Por la parte I del Teorema 1 se deduce que $a|mb + nc$.

■

El Algoritmo de División I

Teorema 2

EL ALGORITMO DE DIVISIÓN Sea a un número entero y d un entero positivo. Entonces hay enteros únicos q y r, con $0 \leq r < d$, tales que $a = dq + r$. ■

El Algoritmo de División I

Teorema 2

EL ALGORITMO DE DIVISIÓN Sea a un número entero y d un entero positivo. Entonces hay enteros únicos q y r, con $0 \leq r < d$, tales que $a = dq + r$. ■

Observación 2

El teorema 2 no es realmente un algoritmo. (¿Por qué no?) Sin embargo, usaremos su nombre tradicional.

El Algoritmo de División II

Definición 2

En la igualdad dada en el algoritmo de división, d se llama *divisor*, a se llama *dividendo*, q se llama *cociente* y r se llama *residuo (resto)*. Esta notación se usa para expresar, respectivamente, el cociente y el residuo:

$$q = a \text{ div } d, \qquad r = a \text{ mod } d.$$

El Algoritmo de División II

Observación 3

Tenga en cuenta que tanto a div d como a mod d para un d fijo son funciones en el conjunto de números enteros. Además, cuando a es un número entero y d es un número entero positivo, tenemos a div $d = \lfloor a/d \rfloor$ y a mod $d = a - d\lfloor a/d \rfloor$.

Ejemplo 3

¿Cuáles son el cociente y el resto cuando 101 se divide entre 11?

Ejemplo 3

¿Cuáles son el cociente y el resto cuando 101 se divide entre 11?

Solución:

- Tenemos que

$$101 = 11 \cdot 9 + 2.$$

Ejemplo 3

¿Cuáles son el cociente y el resto cuando 101 se divide entre 11?

Solución:

- Tenemos que
$$101 = 11 \cdot 9 + 2.$$
- Por lo tanto, el cociente cuando 101 se divide entre 11 es $9 = 101 \text{ div } 11$,

Ejemplo 3

¿Cuáles son el cociente y el resto cuando 101 se divide entre 11?

Solución:

- Tenemos que
$$101 = 11 \cdot 9 + 2.$$
- Por lo tanto, el cociente cuando 101 se divide entre 11 es $9 = 101 \text{ div } 11$,
- y el resto es $2 = 101 \text{ mod } 11$.

□

Ejemplo 4

¿Cuáles son el cociente y el residuo cuando -11 se divide entre 3?

Ejemplo 4

¿Cuáles son el cociente y el residuo cuando -11 se divide entre 3?

Solución:

- Tenemos

$$-11 = 3(-4) + 1.$$

Ejemplo 4

¿Cuáles son el cociente y el residuo cuando -11 se divide entre 3?

Solución:

- Tenemos
$$-11 = 3(-4) + 1.$$
- Por lo tanto, el cociente cuando -11 se divide por 3 es $-4 = -11$ div 3,

Ejemplo 4

¿Cuáles son el cociente y el residuo cuando -11 se divide entre 3?

Solución:

- Tenemos
$$-11 = 3(-4) + 1.$$
- Por lo tanto, el cociente cuando -11 se divide por 3 es $-4 = -11 \text{ div } 3$,
- y el residuo es $1 = -11 \bmod 3$.

Ejemplo 4

¿Cuáles son el cociente y el residuo cuando -11 se divide entre 3?

Solución:

- Tenemos
$$-11 = 3(-4) + 1.$$
- Por lo tanto, el cociente cuando -11 se divide por 3 es $-4 = -11$ div 3,
- y el residuo es $1 = -11$ mod 3.
- Tenga en cuenta que el resto no puede ser negativo.

Ejemplo 4

¿Cuáles son el cociente y el residuo cuando -11 se divide entre 3?

Solución:

- Tenemos
$$-11 = 3(-4) + 1.$$
- Por lo tanto, el cociente cuando -11 se divide por 3 es $-4 = -11 \text{ div } 3$,
- y el residuo es $1 = -11 \bmod 3$.
- Tenga en cuenta que el resto no puede ser negativo.
- En consecuencia, el resto no es -2, aunque $-11 = 3(-3) - 2$, porque $r = -2$ no satisface $0 \leq r < 3$.

□

Aritmética Modular I

- En algunas situaciones, solo nos preocupamos por el resto de un número entero cuando se divide por algún número entero positivo especificado.

Aritmética Modular I

- Por ejemplo, cuando preguntamos qué hora será (en un reloj de 24 horas) dentro de 50 horas, solo nos preocupamos por el resto cuando 50 más la hora actual se divide por 24.

Aritmética Modular I

- Debido a que a menudo solo nos interesan los restos, tenemos notaciones especiales para ellos.

Aritmética Modular I

- Ya hemos introducido la notación a mod m para representar el resto cuando un entero a se divide por el entero positivo m.

Aritmética Modular I

- Introducimos ahora una notación diferente, pero relacionada, que indica que dos enteros tienen el mismo resto cuando se dividen por el entero positivo m.

Definición 3

Si a y b son números enteros y m es un número entero positivo, entonces a es *congruente con* b *módulo* m si m divide a $a - b$. Usamos la notación $a \equiv b (\text{mod } m)$ para indicar que a es congruente con b módulo m. Decimos que $a \equiv b (\text{mod } m)$ es una **congruencia** y que m es su **módulo**. Si a y b no son congruentes módulo m, escribimos $a \not\equiv b (\text{mod } m)$.

Aritmética Modular II

- Aunque ambas notaciones $a \equiv b (\text{mod } m)$ y $a \text{ mod } m = b$ incluyen "mod", representan conceptos fundamentalmente diferentes.

Aritmética Modular II

- Aunque ambas notaciones $a \equiv b (\text{mod } m)$ y $a \text{ mod } m = b$ incluyen "mod", representan conceptos fundamentalmente diferentes.
- El primero representa una relación en el conjunto de números enteros, mientras que el segundo representa una función.

Aritmética Modular II

- Sin embargo, la relación $a \equiv b (\text{mod } m)$ y la función mod m están estrechamente relacionadas, como se describe en el Teorema 3.

Teorema 3

Sean a y b números enteros y m un número entero positivo. Entonces $a \equiv b (\text{mod } m)$ si y sólo si $a \text{ mod } m = b \text{ mod } m$.

Teorema 3

Sean a y b números enteros y m un número entero positivo. Entonces $a \equiv b (\text{mod } m)$ si y sólo si $a \text{ mod } m = b \text{ mod } m$.

■

- La demostración del Teorema 3 se deja como ejercicio.

Teorema 3

Sean a y b números enteros y m un número entero positivo. Entonces $a \equiv b (\text{mod } m)$ si y sólo si $a \text{ mod } m = b \text{ mod } m$.

■

- Recuerde que por la Definición 2 a mod m y b mod m son los residuos cuando a y b se dividen por m, respectivamente.

Teorema 3

Sean a y b números enteros y m un número entero positivo. Entonces $a \equiv b (\text{mod } m)$ si y sólo si $a \text{ mod } m = b \text{ mod } m$.

■

- En consecuencia, el Teorema 3 también dice que $a \equiv b (\text{mod } m)$ si y sólo si a y b tienen el mismo resto cuando se dividen por m.

Ejemplo 5

Determine si 17 es congruente con 5 módulo 6 y si 24 y 14 son congruentes módulo 6.

Ejemplo 5

Determine si 17 es congruente con 5 módulo 6 y si 24 y 14 son congruentes módulo 6.

Solución:

- Como 6 divide a $17 - 5 = 12$, vemos que $17 \equiv 5 (\text{mod } 6)$.

Ejemplo 5

Determine si 17 es congruente con 5 módulo 6 y si 24 y 14 son congruentes módulo 6.

Solución:

- Sin embargo, debido a que $24 - 14 = 10$ no es divisible entre 6, vemos que $24 \not\equiv 14 (\text{mod } 6)$.

□

Teorema 4

Sea m un entero positivo. Los enteros a y b son congruentes módulo m si y sólo si hay un entero k tal que $a = b + km$.

Teorema 4

Sea m un entero positivo. Los enteros a y b son congruentes módulo m si y sólo si hay un entero k tal que $a = b + km$.

Prueba:

- Si $a \equiv b (\text{mod } m)$, por la definición de congruencia (Definición 3), sabemos que $m|(a - b)$.

Teorema 4

Sea m un entero positivo. Los enteros a y b son congruentes módulo m si y sólo si hay un entero k tal que $a = b + km$.

Prueba:

- Si $a \equiv b (\text{mod } m)$, por la definición de congruencia (Definición 3), sabemos que $m|(a - b)$.
- Esto significa que hay un entero k tal que $a - b = km$, de modo que $a = b + km$.

Teorema 4

Sea m un entero positivo. Los enteros a y b son congruentes módulo m si y sólo si hay un entero k tal que $a = b + km$.

Prueba:

- Si $a \equiv b (\text{mod } m)$, por la definición de congruencia (Definición 3), sabemos que $m|(a - b)$.
- Esto significa que hay un entero k tal que $a - b = km$, de modo que $a = b + km$.
- Por el contrario, si hay un número entero k tal que $a = b + km$, entonces $km = a - b$.

Teorema 4

Sea m un entero positivo. Los enteros a y b son congruentes módulo m si y sólo si hay un entero k tal que $a = b + km$.

Prueba:

- Si $a \equiv b (\text{mod } m)$, por la definición de congruencia (Definición 3), sabemos que $m|(a - b)$.
- Esto significa que hay un entero k tal que $a - b = km$, de modo que $a = b + km$.
- Por el contrario, si hay un número entero k tal que $a = b + km$, entonces $km = a - b$.
- Por tanto, m divide a $a - b$, de modo que $a \equiv b (\text{mod } m)$.

■

Aritmética Modular III

- El conjunto de todos los números enteros congruentes con un número entero módulo m se denomina la clase de congruencia de un módulo m.

Aritmética Modular III

- En el capítulo 2 mostramos que hay m clases de equivalencia disjuntas por pares módulo m y que la unión de estas clases de equivalencia es el conjunto de enteros.

Aritmética Modular III

- El teorema 5 muestra que las sumas y multiplicaciones preservan las congruencias.

Teorema 5

Sea m un entero positivo. Si $a \equiv b (\text{mod } m)$ y $c \equiv d (\text{mod } m)$, entonces

$$a + c \equiv b + d (\text{mod } m)$$

y

$$ac \equiv bd (\text{mod } m).$$

Teorema 5 II

Prueba:

- Haremos una prueba directa.

Teorema 5 II

Prueba:

- Haremos una prueba directa.
- Debido a que $a \equiv b (\text{mod } m)$ y $c \equiv d (\text{mod } m)$, según el Teorema 4 hay números enteros s y t con $b = a + sm$ y $d = c + tm$.

Teorema 5 II

Prueba:

- Haremos una prueba directa.
- Debido a que $a \equiv b (\text{mod } m)$ y $c \equiv d (\text{mod } m)$, según el Teorema 4 hay números enteros s y t con $b = a + sm$ y $d = c + tm$.
- Por lo tanto,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

Teorema 5 II

Prueba:

- Haremos una prueba directa.
- Debido a que $a \equiv b (\text{mod } m)$ y $c \equiv d (\text{mod } m)$, según el Teorema 4 hay números enteros s y t con $b = a + sm$ y $d = c + tm$.
- Por lo tanto,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

- y

$$bd = (a + sm)(c + tm) = ac + m(at + cs + stm).$$

Teorema 5 II

Prueba:

- Haremos una prueba directa.
- Debido a que $a \equiv b(\text{mod } m)$ y $c \equiv d(\text{mod } m)$, según el Teorema 4 hay números enteros s y t con $b = a + sm$ y $d = c + tm$.
- Por lo tanto,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

- y

$$bd = (a + sm)(c + tm) = ac + m(at + cs + stm).$$

- Por ello,

$$a + c \equiv b + d(\text{mod } m)$$

y

$$ac \equiv bd(\text{mod } m).$$

Ejemplo 6

Dado que $7 \equiv 2 (\text{mod } 5)$ y $11 \equiv 1 (\text{mod } 5)$, del Teorema 5 se sigue que

$$18 = 7 + 11 \equiv 2 + 1 = 3 (\text{mod } 5)$$

y que

$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 (\text{mod } 5).$$

□

Aritmética Modular IV

- Debemos tener cuidado al trabajar con congruencias.

Aritmética Modular IV

- Algunas propiedades que podemos esperar que sean verdaderas no son válidas.

Aritmética Modular IV

- Por ejemplo, si $ac \equiv bc (\text{mod } m)$, la congruencia $a \equiv b (\text{mod } m)$ puede ser falsa.

Aritmética Modular IV

- De manera similar, si $a \equiv b (\text{mod } m)$ y $c \equiv d (\text{mod } m)$, la congruencia

$$a^c \equiv b^d (\text{mod } m)$$

puede ser falsa.

Aritmética Modular IV

- El corolario 2 muestra cómo encontrar los valores de la función mod m para la suma y el producto de dos enteros usando los valores de esta función en cada uno de estos enteros.

Corolario 2 I

Corolario 2

Sea m un entero positivo y sean a y b enteros. Entonces

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

y

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$$

Corolario 2 II

Prueba:

- Por las definiciones de mod m y de congruencia módulo m, sabemos que $a \equiv (a \bmod m) (\bmod m)$ y $b \equiv (b \bmod m) (\bmod m)$.

Corolario 2 II

Prueba:

- Por las definiciones de mod m y de congruencia módulo m, sabemos que $a \equiv (a \text{ mod } m)(\text{mod } m)$ y $b \equiv (b \text{ mod } m)(\text{mod } m)$.
- Por lo tanto, el Teorema 5 nos dice que

$$a + b \equiv (a \text{ mod } m) + (b \text{ mod } m)(\text{mod } m)$$

Corolario 2 II

Prueba:

- Por las definiciones de mod m y de congruencia módulo m, sabemos que $a \equiv (a \bmod m) (\bmod m)$ y $b \equiv (b \bmod m) (\bmod m)$.
- Por lo tanto, el Teorema 5 nos dice que

$$a + b \equiv (a \bmod m) + (b \bmod m) (\bmod m)$$

- y

$$ab \equiv (a \bmod m)(b \bmod m) (\bmod m).$$

Corolario 2 II

Prueba:

- Por las definiciones de mod m y de congruencia módulo m, sabemos que $a \equiv (a \bmod m) (\bmod m)$ y $b \equiv (b \bmod m) (\bmod m)$.
- Por lo tanto, el Teorema 5 nos dice que

$$a + b \equiv (a \bmod m) + (b \bmod m) (\bmod m)$$

- y

$$ab \equiv (a \bmod m)(b \bmod m) (\bmod m).$$

- Las igualdades en este corolario se derivan de estas dos últimas congruencias del Teorema 3. ■

Ejemplo 7

Encuentre el valor de $(19^3 \bmod 31)^4 \bmod 23$.

Ejemplo 7

Encuentre el valor de $(19^3 \bmod 31)^4 \bmod 23$.

Solución:

- Para poder calcular $(19^3 \bmod 31)^4 \bmod 23$, primero evaluaremos $19^3 \bmod 31$.

Ejemplo 7

Encuentre el valor de $(19^3 \bmod 31)^4 \bmod 23$.

Solución:

- Para poder calcular $(19^3 \bmod 31)^4 \bmod 23$, primero evaluaremos $19^3 \bmod 31$.
- Como $19^3 = 6859$ y $6859 = 221 \cdot 31 + 8$, tenemos $19^3 \bmod 31 = 6859 \bmod 31 = 8$.

Ejemplo 7

Encuentre el valor de $(19^3 \bmod 31)^4 \bmod 23$.

Solución:

- Para poder calcular $(19^3 \bmod 31)^4 \bmod 23$, primero evaluaremos $19^3 \bmod 31$.
- Como $19^3 = 6859$ y $6859 = 221 \cdot 31 + 8$, tenemos $19^3 \bmod 31 = 6859 \bmod 31 = 8$.
- Entonces, $(19^3 \bmod 31)^4 \bmod 23 = 8^4 \bmod 23$.

Ejemplo 7

Encuentre el valor de $(19^3 \bmod 31)^4 \bmod 23$.

Solución:

- Para poder calcular $(19^3 \bmod 31)^4 \bmod 23$, primero evaluaremos $19^3 \bmod 31$.
- Como $19^3 = 6859$ y $6859 = 221 \cdot 31 + 8$, tenemos $19^3 \bmod 31 = 6859 \bmod 31 = 8$.
- Entonces, $(19^3 \bmod 31)^4 \bmod 23 = 8^4 \bmod 23$.
- A continuación, tenga en cuenta que $8^4 = 4096$.

Ejemplo 7

Encuentre el valor de $(19^3 \bmod 31)^4 \bmod 23$.

Solución:

- Para poder calcular $(19^3 \bmod 31)^4 \bmod 23$, primero evaluaremos $19^3 \bmod 31$.
- Como $19^3 = 6859$ y $6859 = 221 \cdot 31 + 8$, tenemos $19^3 \bmod 31 = 6859 \bmod 31 = 8$.
- Entonces, $(19^3 \bmod 31)^4 \bmod 23 = 8^4 \bmod 23$.
- A continuación, tenga en cuenta que $8^4 = 4096$.
- Como $4096 = 178 \cdot 23 + 2$, tenemos $4096 \bmod 23 = 2$.

Ejemplo 7

Encuentre el valor de $(19^3 \bmod 31)^4 \bmod 23$.

Solución:

- Para poder calcular $(19^3 \bmod 31)^4 \bmod 23$, primero evaluaremos $19^3 \bmod 31$.
- Como $19^3 = 6859$ y $6859 = 221 \cdot 31 + 8$, tenemos $19^3 \bmod 31 = 6859 \bmod 31 = 8$.
- Entonces, $(19^3 \bmod 31)^4 \bmod 23 = 8^4 \bmod 23$.
- A continuación, tenga en cuenta que $8^4 = 4096$.
- Como $4096 = 178 \cdot 23 + 2$, tenemos $4096 \bmod 23 = 2$.
- Por lo tanto, $(19^3 \bmod 31)^4 \bmod 23 = 2$.

Aritmética Módulo m I

- Podemos definir operaciones aritméticas en $\mathbb{Z}_m$, el conjunto de enteros no negativos menores que m, es decir, el conjunto $\{0, 1, \ldots, m-1\}$.

Aritmética Módulo m I

- En particular, definimos la suma de estos números enteros, denotados por $+_m$ por

$$a +_m b = (a + b) \bmod m,$$

donde la suma en el lado derecho de esta ecuación es la suma ordinaria de enteros,

- y definimos la multiplicación de estos enteros, denotada por $\cdot_m$ por

$$a \cdot_m b = (a \cdot b) \bmod m,$$

donde la multiplicación del lado derecho de esta ecuación es la multiplicación ordinaria de números enteros.

Aritmética Módulo m I

- Las operaciones $+_m$ y $\cdot_m$ se llaman suma y multiplicación módulo m y cuando usamos estas operaciones, se dice que estamos haciendo **aritmética módulo m**.

Ejemplo 8

Use la definición de suma y multiplicación en $\mathbb{Z}_m$ para hallar $7 +_{11} 9$ y $7 \cdot_{11} 9$.

Ejemplo 8

Use la definición de suma y multiplicación en $\mathbb{Z}_m$ para hallar $7 +_{11} 9$ y $7 \cdot_{11} 9$.

Solución:

- Usando la definición de suma módulo 11, encontramos que

$$7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5,$$

Ejemplo 8

Use la definición de suma y multiplicación en $\mathbb{Z}_m$ para hallar $7 +_{11} 9$ y $7 \cdot_{11} 9$.

Solución:

- y

$$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8.$$

Ejemplo 8

Use la definición de suma y multiplicación en $\mathbb{Z}_m$ para hallar $7 +_{11} 9$ y $7 \cdot_{11} 9$.

Solución:

- Por tanto, $7 +_{11} 9 = 5$ y $7 \cdot_{11} 9 = 8$.

□

Propiedades de la Aritmética Módulo m

Cerradura Si a y b pertenecen a $\mathbb{Z}_m$, entonces $a +_m b$ y $a \cdot_m b$ pertenecen a $\mathbb{Z}_m$.

Propiedades de la Aritmética Módulo m

Asociatividad Si a, b y c pertenecen a $\mathbb{Z}_m$, entonces

$$(a +_m b) +_m c = a +_m (b +_m c) \text{ y } (a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c).$$

Propiedades de la Aritmética Módulo m

Conmutatividad Si a y b pertenecen a $\mathbb{Z}_m$, entonces $a +_m b = b +_m a$ y $a \cdot_m b = b \cdot_m a$.

Propiedades de la Aritmética Módulo m

Elementos identidad Los elementos 0 y 1 son los elementos identidad para la suma y la multiplicación módulo m, respectivamente. Es decir, si a pertenece a $\mathbb{Z}_m$, entonces $a +_m 0 = 0 +_m a = a$ y $a \cdot_m 1 = 1 \cdot_m a = a$.

Propiedades de la Aritmética Módulo m

Inversos aditivos Si $a \neq 0$ pertenece a $\mathbb{Z}_m$, entonces $m - a$ es un inverso aditivo de a módulo m y 0 es su propio inverso aditivo, es decir, $a +_m (m - a) = 0$ y $0 +_m 0 = 0$.

Propiedades de la Aritmética Módulo m

Distributividad Si a, b y c pertenecen a $\mathbb{Z}_m$, entonces

$$a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c) \text{ y}$$
$$(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c).$$

Ejercicios I

1. ¿17 divide a cada uno de estos números?
   1. 68
   2. 84
   3. 357
   4. 1001
2. Demuestre las partes II y III del Teorema 1.
3. Demuestre que si a, b, c y d son enteros, con $a \neq 0$ y $b \neq 0$, tal que $a|c$ y $b|d$ entonces $ab|cd$.
4. ¿Cuál es el cociente y el residuo cuando
   1. 19 es dividido por 7?
   2. -111 es dividido por 11?
   3. 789 es dividido por 23?
   4. 0 es dividido por 19?
   5. -1 es dividido por 3?
   6. 1001 es dividido por 13?
   7. 3 es dividido por 5?
   8. 4 es dividido por 1?
5. ¿Qué hora marcará un reloj de 12 horas
   1. 80 horas después de que marca las 11:00?
   2. 40 horas después de que marca las 12:00?

Ejercicios II

3. 100 horas después de que marca las 6:00?

6. Decida si cada uno de estos números enteros es congruente con 3 módulo 7.
   1. 37
   2. 66
   3. -17
   4. -67

7. Encuentre cada uno de los siguientes valores.
   1. $(19^2 \bmod 41) \bmod 9$
   2. $(32^3 \bmod 13)^2 \bmod 11$
   3. $(7^3 \bmod 23)^2 \bmod 31$
   4. $(21^2 \bmod 15)^3 \bmod 22$

8. Escriba las tablas de adición y multiplicación para $\mathbb{Z}_6$ (donde por adición y multiplicación queremos decir $+_6$ y $\cdot_6$).