Enteros y División
Matemáticas Discretas
Docente: Esteban Andrés Díaz Mina

2.4 ENTEROS Y DIVISION

La teoría de números es la parte de las matemáticas discretas que estudia los enteros y sus propiedades. En esta sección se abordará algunos conceptos básicos, entre los que se incluyen la divisibilidad, el máximo común divisor y la aritmética modular. Un concepto importante basado en la divisibilidad es el número primo, determinar si un número es primo es importante en las aplicaciones a la criptografía.

DIVISION

Cuando un entero se divide por otro entero no nulo, el cociente puede ser entero. Por ejemplo, 12/4 = 3 es un entero, mientras que 11/4= 2.75 no lo es. Esto conduce a la siguiente definición:

Definición. Si a y b son enteros con a≠0, decimos que a divide a b si existe un entero c talque b=ac. 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. Escribiremos a $\nmid$ b cuando a no divide a b.

Ex. Determinar si son ciertas las siguientes afirmaciones: $6 \nmid 605$ y $3 \mid 150$.

Definición. Un entero positivo p mayor que 1 es llamado primo si los únicos factores positivos de p son 1 y p. Un entero positivo que sea mayor que 1 y no sea primo es llamado compuesto.

Ex. El número 21 es un número compuesto. Mientras que 23 es un número primo.

TEOREMA FUNDAMENTAL DE LA ARITMÉTICA. Todo entero positivo mayor que 1 se puede escribir de una única forma, como un primo o como el producto de dos o más primos en el que los factores primos se escriben en orden no decreciente.

Ex. Las factorizaciones de 99 son $3^2 * 11$.

ALGORITMO DE LA DIVISIÓN

La división de un entero entre un entero positivo da un cociente y un residuo, como muestra el algoritmo de la división.

ALGORITMO DE LA DIVISIÓN. Sea a un entero y d un entero positivo. Entonces, existen enteros q y r únicos, con $0 \leq r < d$, tal que $a = dq + r$.

En la igualdad dada en el algoritmo de la división, d es llamado el *divisor*, a es llamado el *dividendo*, q es llamado el *cociente*, y r es llamado el *residuo*. La siguiente notación es usada para expresar el cociente y el residuo: $q = a \ \boldsymbol{div}\ d$, $r = a \ \boldsymbol{mod}\ d$.

Ex. ¿Cuál es el cociente y el residuo cuando 102 es dividido por 11?

Sol. 102=9(11)+3. Luego el cociente es 9 y el residuo es 3

Ex. ¿Cuál es el cociente y el residuo de –22 dividido por 4?

Sol. -22=4(-6)+2. Luego el cociente es –6 y el residuo es 2 (positivo según definición).

MÁXIMO COMÚN DIVISOR Y MÍNIMO COMÚN MÚLTIPLO

El mayor entero que divide a dos enteros se llama máximo común divisor de estos enteros

Definición. Sean a y b enteros diferentes a 0. El entero más grande d tal que d | a y d | b es llamado el **Máximo Común Divisor** de a y b. Es denotado como mcd(a, b).

Definición 4. Sean a y b enteros diferentes a 0. El entero más grande d tal que d | a y d | b es llamado el **Máximo Común Divisor** de a y b. Es denotado como mcd(a, b).

Ex. ¿Cuál es el máximo común divisor de 24 y 36?

Ex. ¿Cuál es el máximo común divisor de 17 y 22?

El mcd de dos números se puede hallar a partir de su factorización prima. Ya que si:

$$\begin{cases} a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \\ b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n} \end{cases}, \text{ entonces } mcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

Ex14. ¿Cuál es el mcd de 120 y 500?

$120=2^3.3^1.5^1$ y $500=2^2.5^3$. Luego $mcd(120,500) = 2^{\min(3,2)}. 3^{\min(1,0)}.5^{\min(1,3)} = 2^2. 3^0.5^1 = 20$

La factorización de un numero se puede utilizar también para obtener el mínimo común múltiplo de dos enteros:

El *mínimo común múltiplo* de los enteros positivos a y b es el menor entero positivo que es divisible tanto por a como por b. El *mínimo común múltiplo* de a y b se denota por mcm(a,b).

El mcm de dos enteros puede hallarse a partir de su factorización prima. Ya que si:

$$\begin{cases} a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \\ b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n} \end{cases}$$. Entonces $mcm(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$

Ex15. ¿Cuál es el mcd de 120 y 500?

$120=2^3.3^1.5^1$ y $500=2^2.5^3$. Luego mcm(120,500) = $2^{\max(3,2)}.\ 3^{\max(1,0)}.5^{\max(1,3)} = 2^3.\ 3^1.5^3=3000$.

APLICACIONES DE LAS CONGRUENCIAS

La teoría de números tiene aplicaciones en un amplio abanico de áreas. En esta sesión presentamos un sistema de cifrado basado en aritmética modular.

CRIPTOGRAFIA

Las congruencias tienen muchas aplicaciones en matemáticas discretas y ciencias de la computación. Una de las aplicaciones más importantes de las congruencias está relacionada con la criptografía, que es el estudio de los mensajes secretos. Uno de los primeros usos conocidos de la criptografía se debe a Julio Cesar.; que construía mensajes secretos moviendo la posición de cada letra tres posiciones hacia delante en el alfabeto. Este es un ejemplo de codificación o cifrado; es decir, el proceso de construir un mensaje secreto.

Para expresar matemáticamente el proceso de cifrado de Cesar, primero se reemplaza cada letra por un entero de 0 a 26, basada en su posición en el alfabeto español.

El método de cifrado de Cesar se puede representar por la función f que asigna a un entero no negativo p, $p \leq 26$, el entero f(p) del conjunto {0, 1, 2, …, 26} con f(p) = (p + 3) mod 27.

Ex20. ¿Cuál es el mensaje cifrado obtenido usando el cifrado de Cesar a partir del mensaje "VOY AL PARQUE MAÑANA"?

Solución. Primero se reemplaza las letras del mensaje por números. Esto produce

22 15 25 - 0 11 - 16 0 18 17 21 4 - 12 0 14 0 13 0

Números asociados a cada una de las letras del alfabeto español.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Ahora, se reemplaza cada número p, por f(p) = (p + 3) mod 27. Esto da:

25 18 1 - 3 14 - 19 3 21 20 24 7 - 15 3 17 3 16 3

Pasando de nuevo a letras, se produce el mensaje codificado:

"YRB - DÑ - SDUTXH - ODQDPD"

Para recuperar el mensaje original a partir de un mensaje cifrado por el método Cesar se usa la función f^{-1}, la inversa de f. Tenga en cuenta que la función f^{-1} asigna a un entero p de {0, 1, 2, …, 26} el elemento $f^{-1}(p) = (p - 3) \bmod 27$. Este proceso de obtención del mensaje original a partir del codificado se llama decodificación o descifrado.

Hay varias formas de generalizar el cifrado de Cesar. Por ejemplo, en vez de desplazar cada letra tres puestos, se puede desplazar un número k, de tal forma que

$f(p) = (p + k) \bmod 27$

Tal codificación se llama cifrado por traslación. Observe que se descifra usando $f^{-1}(p) = (p - k) \bmod 27$

Obviamente, el cifrado de Cesar y el cifrado por desplazamiento no tienen un nivel de seguridad alto. Hay varias formas de mejorar este método. Una modificación que aumenta ligeramente la seguridad es usar una función de la forma $f(p) = (ap + b) \bmod 27$ donde a y b son enteros elegidos de forma que f sea biyectiva.

Esto proporciona un gran número de codificaciones distintas. A continuación, se presenta un ejemplo:

Ex21. ¿Qué letra reemplaza a la letra K cuando se utiliza la función de cifrado $f(p) = (7p + 3) \bmod 27$?

Solución. Como K se representa por el número 10. Utilizando la función de cifrado, se tiene que $f(10) = (7 \cdot 10 + 3) \bmod 27 = 19$. Como 19 representa la letra S, K se reemplaza por S en el mensaje cifrado.

Para recuperar la letra K, se realiza el siguiente procedimiento.

73 | 27
-54 | 2
19

$div = 2 \quad a = 7$
$mod = 19 \quad b = 3$

$$f^{-1}(p) = \frac{div * 27 + mod - b}{a} \qquad f^{-1}(19) = \frac{2 * 27 + 19 - 3}{7} = 10$$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Enteros y Algoritmos
Matemáticas Discretas
Docente: Esteban Andrés Díaz Mina

2.5 ENTEROS Y ALGORITMOS

REPRESENTACIONES DE NUMEROS ENTEROS

En nuestra vida cotidiana utilizamos la notación decimal para expresar números enteros. Por ejemplo, 965 se usa para denotar $9 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0$. No obstante, a veces es conveniente usar otras bases diferentes a 10. En particular, los ordenadores utilizan notación binaria (con 2 como base) para realizar cálculos aritméticos y octal (base 8) o hexadecimal (base 16) para expresar caracteres, como letras o dígitos.

Sea b un entero positivo mayor que 1. Entonces, si n es un entero positivo, se puede expresar como $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$ de una única forma, donde k es un entero no negativo, $a_0, a_1, \ldots, a_k$ son enteros no negativos menores que b y $a_k \neq 0$.

EXPRESIONES BINARIAS. La elección de 2 como base da la expresión binaria de los números enteros. En notación binaria cada digito es 0 o 1. En otras palabras, la expresión binaria de un entero no es más que una cadena de bits. Las expresiones binarias son las que utilizan los ordenadores para representar y desarrollar la aritmética con enteros.

Ejemplo 1. ¿Cuál es la expresión decimal del entero cuya expresión binaria es $(1\ 0101\ 1111)_2$?

EXPRESIONES HEXADECIMALES. Dieciséis es otra base utilizada en informática. La expresión en base 16 de un entero se llama expresión hexadecimal. Para esta expresión se requieren 16 dígitos. Los dígitos hexadecimales usados generalmente son 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, donde las letras de la A a la F representan los números del 10 al 16 (en notación decimal).

Ejemplo 2. ¿Cuál es la expresión decimal del entero con expresión hexadecimal $(2AE0B)_{16}$?

CONVERSION DE BASE. Algoritmo para obtener la expresión en base b de un numero n. Primero, se divide n por b para obtener el cociente y el resto, esto es,

$$n = bq_0 + a_0 \quad 0 \leq a_0 < b.$$

Es resto, a_0 , es el digito situado más a la derecha en la expresión en base b de n. Luego, se divide q_0 por b para obtener

$$q_0 = bq_1 + a_1 \quad 0 \le a_1 < b.$$

Ahora a_1 es el segundo digito por la derecha de la expresión de n en base b. Este proceso continúa dividiendo sucesivamente el cociente por b, obteniendo como restos los dígitos de la representación en base b. El proceso concluye cuando obtenemos un cociente igual a cero.

EXPONENCIACIÓN MODULAR

En criptografía es importante calcular de forma eficiente $b^n \bmod m$, donde b, n y m son enteros grandes. No es práctico calcular primero b^n y posteriormente hallar el resto de dividirlo por m, porque b^n puede ser un número excesivamente grande. En lugar de esto, podemos usar el algoritmo que emplea la expansión binaria del exponente n, es decir, $n=(a_{k-1}a_{k-2}\ldots a_1a_0)_2$.

El algoritmo calcula sucesivamente b mod m, $b^2 \bmod m$, $b^4 \bmod m$,..,$b^r \bmod m$ (donde $r=2^{k-1}$) y multiplica todos los términos $b^s \bmod m$ ($s=2^j$) cuando $a_j=1$, calculando el resto de la división por m tras cada multiplicación. El pseudocódigo

```
Procedimiento Exponenciación modular (b: entero, n=(ak-1... a1a0)2,  m: entero positivo)
x := 1
potencia := b mod m
Para i:=0 hasta k-1
begin
   Si ai=1 Entonces  x := (x * potencia) mod m
   potencia := (potencia * potencia) mod m
Fin para //finalmente x es igual a bn mod m
Fin procedimiento
```

Ex. Utiliza procedimiento anterior para hallar $2^{644} \bmod 645$

i=0: Como $a_0 = 0$, tenemos que x=1 y potencia = $2^2 = 4 \bmod 645 = 4$

i=1: Como $a_1 = 0$, tenemos que x=1 y potencia = $4^2 = 16 \bmod 645 = 16$

i=2: Como $a_2 = 1$, tenemos que x=1·16 y potencia = $16^2 = 256 \bmod 645 = 256$

i=3: Como $a_3 = 0$, tenemos que x=16 y potencia = $256^2 = 65536 \bmod 645 = 391$

i=4: Como $a_4 = 0$, tenemos que x=16 y potencia = $391^2 = 152881 \bmod 645 = 16$

i=5: Como $a_5 = 0$, tenemos que x=16 y potencia = $16^2 = 256 \bmod 645 = 256$

i=6: Como $a_6 = 0$, tenemos que x=16 y potencia = $256^2 = 65536 \bmod 645 = 391$

i=7: Como $a_8 = 1$, tenemos que $x=(16 \cdot 391) \mod 645 = 451$ y potencia $= 391^2 = 152881 \mod 645=16$

i=8: Como $a_8 = 0$, tenemos que $x=451$ y potencia $= 16^2 = 256 \mod 645 = 256$

i=9: Como $a_9 = 1$, tenemos que $x=(451 \cdot 256) \mod 645 = 1$

ALGORTIMO DE EUCLIDES

El método para calcular el máximo común divisor de dos enteros usando la descomposición en productos de factores primos no es eficiente. La razón es que la Factorización es un proceso que consume mucho tiempo. Daremos un método más eficiente para hallar el máximo común divisor, llamado algoritmo de Euclides. Este algoritmo se ha utilizado desde la antigüedad. Se denomina así por el matemático de la Grecia antigua Euclides, quien incluyó una descripción de este algoritmo en su obra Los elementos.

Sea a=bq+r, donde a, b, q y r son enteros. Entonces, mcd(a, b)=mcd(b, r).

Sea a = 2322, b = 654. Calcular el máximo común divisor de a y b.

2322 = 654*3 + 360	mcd(2322, 654) = mcd(654, 360)
654 = 360*1 + 294	mcd(654, 360) = mcd(360, 294)
360 = 294*1 + 66	mcd(360, 294) = mcd(294, 66)
294 = 66*4 + 30	mcd(294, 66) = mcd(66, 30)
66 = 30*2 + 6	mcd(66, 30) = mcd(30, 6)
30 = 6*5	mcd(30, 6) = 6

Entonces, mcd(2322,654) = 6.

Ex. Calcular el mcd de 120 y 500 usando el algoritmo de Euclides

Sol. 500=120*4+20 120=20*6. Luego mcd(120, 500)=mcd(20,120)=20