PROPEDÉUTICO DE MATEMÁTICAS

Generación 13

[2019]

Luis J. Dominguez Perez

GOBIERNO DE MÉXICO

Sesión 2

Contenido, sección 1

Divisibilidad y Euclides

Congruencias

Factorización

Divisibilidad

Un concepto central en la teoría de números es la *divisibilidad*. Sean $a, b \in \mathbb{Z}$, se dice que a **divide** b (denotado como: $a|b$) si $az = b$ para algún $z \in \mathbb{Z}$. Se dice que a es un **divisor** de b, que b es un **múltiplo** de a, o que b es **divisible por** a. Si a no divide b, entonces se escribe como: $a \nmid b$

Sobre la divisibilidad

Para todo $a, b, c \in \mathbb{Z}$, tenemos que:

- $a|a$, $1|b$, y $a|0$
- $0|b$ sí y solo si $b = 0$
- $a|b$ sí y solo si $-a|b$, sí y solo sí $a| - b$
- $a|b$ y $a|c$, implica que $a|(b + c)$
- $a|b$ y $b|c$, implica que $a|c$.

Observación> si $a|b$ y $b \nmid 0$, entonces $q \leq |a| \leq |b|$. De hecho, si $az = b \nmid 0$ para algún entero z, entonces $a \nmid 0$ y $z \nmid 0$; por lo que $|a| \geq 1, z \geq 1$, y $|a| \leq |a||z| = |b|$.

CIMAT

Teorema

Para todo $a, b \in \mathbb{Z}$, se tiene que $a|b$ y $b|a$ sí y sólo si $a = \pm b$. En particular, para todo $a \in \mathbb{Z}$, tenemos que $a|1$ sí y sólo si $a = \pm 1$

Proof.

Si $a = \pm b$, entonces $a|b$ y $b|a$. Asumamos que $a|b$ y que $b|a$ para probar que $a + \pm b$. Si a o b son cero, entonces el otro debe ser cero también. Asumamos que ninguno es cero. $a|b$ implica que $|a| \leq |b|$, y $b|a$ implica que $|b| \leq |a|$; por lo que $|a| = |b|$, entonces $a = \pm b$. Esto prueba la primera parte. La segunda parte viene de poner a $b = 1$, entonces $1|a$ $\square$

Números Primos

Sea n un número positivo y entero. Sabemos que 1 y n dividen n. Si $n > 1$ y ningún otro número además de 1 y n lo dividen, decimos que n es **primo**.Si $n > 1$ pero n no es primo, entonces decimos que n es **compuesto**. Nota: el número 1 no se considera primo, ni compuesto.

n es compuesto si y sólo si $n = ab$ para algún entero a, b con $1 < a < n$, y $1 < b < n$.

Normalmente, al hablar de un númro primo o compuesto, nos referimos a un número entero positivo.

CIMAT

Teorema

Todo entero n distinto de cero puede expresarse como:

$$n = \pm p_1^{e_1} \cdots p_r^{e_r}$$

donde $p_1, \ldots, p_r$ son primos distintos, y $e_1, \ldots, e_r$ son enteros positivos. Adicionalmente, esta expresión es única después de reordenar los primos.

CIMAT

Teorema - Propiedad de la división con residuo

Sea $a, b \in \mathbb{Z}$ con $b > 0$. Existen $q, r \in \mathbb{Z}$ únicos tales que $a = bq + r$, con $0 \leq r \leq b$.

Número liso

Si un número entero positivo es divisible solamente por números primos "pequeños", se dice que es un número *liso* (smooth).

Los números lisos son muy utilizados en el criptoanálisis para verificar un sistema (romperlo). Por otro lado, los números que solamente se pueden factorizar por dos números primos muy grandes son esenciales para la criptografía de clave pública.

CIMAT

Máximo común divisor

Dados dos números $a, b \in \mathbb{Z}$, distintos a cero, el Máximo común divisor (MCD), denotado como MCD(a, b), o en ocasiones símplemente como (a, b), es un número entero d que es el más grande que divide tanto a a como a b.

Mínimo común múltiplo

Dados dos números $a, b \in mathbbZ$, distintos a cero, el mínimo común múltiplo (mcm), denotado como mcm(a, b) es el número entero positivo más pequeño al cual a y b dividen.

Algoritmo de Euclides

El algoritmo de Euclides es una manera rápida de encontrar el MCD(a, b) aún cuando se desconozcan los factores primos de a y b.

El algoritmo funciona así:

- Reordene para que $a > b$
- Divida a sobre b, y guarde el cociente q_1, y el residuo $r_1 : a = q_1 b + r_1$
- Reordene para que $a > b$: b es el nuevo a, y r_1 es el nuevo b
- Divida b sobre r_1 y guarde q_2 y $r_2 : b = q_2 r_1 + r_2$
- Reordene para que $a > b \ldots$
- Se detiene el algorimto cuando el último residuo divide al anterior: $r_n | r_{n-1}$

Ejemplo:

Encontrar el MCD(1547, 560):

$$1547 = 2 \cdot 560 + 427$$
$$560 = 1 \cdot 427 + 133$$
$$427 = 3 \cdot 133 + 28$$
$$133 = 4 \cdot 28 + 21$$
$$28 = 1 \cdot 21 + 7$$

Dado que $7|21$ hemos terminado: $\text{MCD}(1547, 560) = 7$.

Ejercicio

- Genere un programa en Sage para calcular el MCD.

Propiedades

- Por definición $\text{MCD}(0,0) = 0$
- $\text{MCD}(a,b) = \text{MCD}(b,a)$
- $\text{MCD}(a,b) = \text{MCD}(-a,b)$
- $\text{MCD}(-a,0) = |a|$
- $\text{MCD}(a,b) \cdot c = \text{MCD}(ac,bc)$, si $c \geq 0$
- $\text{mcm}(a,b) \cdot c = \text{mcm}(ac,bc)$, si $c \geq 0$
- $ab = \text{MCD}(a,b)\text{mcm}(a,b)$, si $a,b \geq 0$
- $\text{MCD}(\text{mcm}(a,b), \text{mcm}(a,c)) = \text{mcm}(a, \text{MCD}(b,c))$
- $\text{mcm}(\text{MCD}(a,b), \text{MCD}(a,c)) = \text{MCD}(a, \text{mcm}(b,c))$

Propiedades binarias

- Si a, b son pares, entonces:
  - $\text{MCD}(a, b) = 2 \cdot \text{MCD}(a/2, b/2)$
- Si a es par, y b es impar, entonces:
  - $\text{MCD}(a, b) = \text{MCM}(a/2, b)$
  - $\text{MCD}(a, b) = \text{MCM}(a - b, b)$
- Si a, b son impares, entonces:
  - $a - b$ es par
  - $|a - b| < \max(a, b)$

Ejercicio

- Genere un programa en Sage para calcular los números primos menores a 10000.

- Si contamos a 2 como el primer número primo, 3 el segundo, ¿cuál es el 100mo. primo?

Contenido, sección 2

Divisibilidad y Euclides

Congruencias

Factorización

CIMAT

Propiedades básicas

Dados tres enteros a, b, y m, decimos que *a es congruente a b módulo m*, denotado: $a \equiv b \bmod m$, si la diferencia $a - b$ es divisible por m.

A m se le conoce como el *módulo* de la congruencia.

Propiedades

Propiedades de la congruencia:

1.
   - $a \equiv a \bmod m$
   - $a \equiv b \bmod m$ sí y solo sí $b \equiv a \bmod m$
   - Si $a \equiv b \bmod m$, y $b \equiv c \bmod m$, entonces $a \equiv c \bmod m$

   Para una m fija, esto significa que la congruencia módulo m es una *relación de equivalencia*.

Propiedades. . .

2.
- Para una m fija, cada *clase de equivalencia* con respecto a un módulo m tiene 1 y sólo 1 representante entre 0 y $m-1$.
- El conjunto de clases de equivalencia (*clases residuales*) se denota como $\mathbb{Z}/m\mathbb{Z}$
- Cualquier conjunto de representantes para las clases residuales es llamado *conjunto completo de residuos módulo m*.

Propiedades. . .

3. Si $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then $a \pm c \equiv b \pm d \bmod m$ and $ac \equiv bd \bmod m$.

En otras palabras, las congruencias (con el mismo módulo) se pueden sumar, restar, o multiplicar.

- El conjunto de clases de equivalencia $\mathbb{Z}/m\mathbb{Z}$ es un anillo conmutativo (lo veremos en la siguiente unidad). Esencialmente, las clases residuales se pueden sumar, restar, o multiplicar, y los axiomas básicos aplican (asociatividad, conmutabilidad, inversos aditivos, etc.)

Propiedades. . .

4. Si $a \equiv b \bmod m$, entonces $a \equiv b \bmod d$ para cualquier $d|m$
5. Si $a \equiv b \bmod m$, $a \equiv \bmod n$, y m y n son primos relativos, entonces $a \equiv b \bmod mn$

CIMAT

Teorema

Sea p un primo. Cualquier entero a satisface $a^p \equiv a \bmod p$, y cualquier entero a no divisible por p satisface $a^{p-1} \equiv 1 \bmod p$

Corolario

Si a no es divisible por p y si $n \equiv m \bmod (p-1)$, entonces $a^n \equiv a^m \bmod p$.

CIMAT

Definición

La función ϕ de Euler, también llamada totient, es la función definida por la siguiente regla:

$$\phi(m) = \#\mathbb{Z}/m\mathbb{Z} = \#\{0 \leq a < m : \text{MCM}(a, m) = 1\}$$

Podemos calcular el valor con:

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Ejemplo

Calcular para 100:

- Factores: 2, 5
- $\phi(100) = 100 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right) = 40$

Ejemplo

Calcular para 100:

- Factores: 2, 5
- $\phi(100) = 100 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right) = 40$

En el caso de números primos, $\phi(p) = p - 1$.

Ejercicio

- Genere un programa en Sage para calcular la función ϕ de Euler.

Observaciones

- Euler demostró que: $a^{\phi(n)} \equiv 1 \bmod n$
- Pregunta: ¿$\phi(n)|n-1$?

Contenido, sección 3

Divisibilidad y Euclides

Congruencias

Factorización

CIMAT

Proposición

Para todo entero b y cualquier entero positivo n, $b^n - 1$ es divisible por $b - 1$ con cociente $b^{n-1} + b^{n-2} + \cdots + b^2 + b + 1$

Corolario

Para todo entero b y todo entero positivo m y n, tenemos que $b^{mn} - 1 = (b^m - 1)(b^{m(n-2)} + b^{m(n-2)} + \cdots + b^{2m} + b^m + 1)$

CIMAT

Proposición

Suponga que b es primo con respecto a m, y que a y c son enteros positivos. Si $b^a \equiv 1 \bmod m$ y $b^c \equiv 1 \bmod m$, y si $d = \text{MCM}(a, c)$, entonces $b^d \equiv 1 \bmod m$.

Proposición

Si p es un primo que divide $b^n - 1$, entonces: $p | b^d - 1$ para algún *factor propio* d de n, o $p \equiv 1 \bmod n$. Si $p > 2$ y n es impar, entonces $p \equiv 1 \bmod 2n$.

Ejemplos

- Factorizar $2^{11} - 1 = 2407$. Si $p|2^{11} - 1$, entonces $p \equiv 1 \bmod 22$, así que probamos con 23, 67, 89, ... (primos). Obtenemos la factorización con estos primos: $2047 = 23 \cdot 89$. Similarmente, sabemos que $2^{13} - 1 = 8191$ es primo (factores cercanos: 53, 79, y 131).

Si el número de esta forma es primo, se le conoce como *primo Mersenne*, en honor a su descubridor.

Ejemplos

- Factorizar $3^{12} - 1 = 531440$. Intentamos primeramente con los valores menores a $d = 12$: $3^1 - 1$, $3^2 - 1$, $3^3 - 1$, $3^4 - 1$, y el factor especial $3^6 - 1 = (3^3 - 1)(3^3 + 1)$, que no se repite. Tenemos 2, 2^4, $2 \cdot 13$, $2^4 \cdot 5$, y $2^2 \cdot 7$; que son: $2^4 \cdot 5 \cdot 7 \cdot 13$, valor que es un factor propio de 531440. Así que, tenemos: $531440/(2^4 \cdot 5 \cdot 7 \cdot 13) = 73)$, el cual es primo, y lo agregamos a la cadena de factores: $\{2^4, 5, 7, 13, 73\}$.

Note que el valor que no proviene de un $3^d - 1$, es congruente a 1 modulo $d = 12$; en este caso, $73 \equiv 1 \bmod 12$.

Ejemplos

- Factorizar $2^{35} - 1 = 34359738367$. Consideramos los factores de $2^d - 1$ para $d = \{1, 5, 7\}$. Esto nos da 31 y 127: $(2^{35} - 1)/(31 \cdot 127) = 8727391$. Siendo $d = 35$, $p \equiv 1 \bmod 70$. Así que deberemos de checar $71, 211, 281, \ldots$, afortunadamente, $71|8727391$, $8727391/70 = 122921$, así que seguimos con el 211 para el $122921\ldots$, el cual es un número primo. Así que: $2^{35} - 1 = 31 \cdot 71 \cdot 127 \cdot 122921$.

Nota: Como ya se había mencionado, si un número primo es de la forma: $2^d - 1$, se le conoce como primo de Mersenne $(3, 7, 31, 127, \ldots)$; sin embargo, si es de la forma: $2^d + 1$, entonces se le conoce como *primo de Fermat* $(3, 5, 17, 257, \ldots)$.

Ejercicios

- Dado $m = 24$, $2^m + 1 = 16777217$:
  - Encuentre su factorización
  - Encuentre un primo de Fermat que divida m.
- Factorice:
  - $3^{15} - 1$, $3^{24} - 1$
  - $5^{12} - 1$
  - $10^5 - 1$, $10^6 - 1$, y $10^8 - 1$
  - $2^{33} - 1$, y $2^{21} - 1$
  - $2^{15} - 1$, $2^{30} - 1$, y $2^{60} - 1$.

Caso RSA

- Ronal Rivest, Adi Shamir, y Len Adleman en 1977 descubrieron el método RSA para cifrado de información.
- El algoritmo se basa en la dificultad para descomponer factores primos muy grandes
- Se utiliza ampliamente como base para la criptografía de llave pública.
- Ganaron el premio Túrin en 2002 por esta aportación

Caso RSA

- Ronal Rivest, Adi Shamir, y Len Adleman en 1977 descubrieron el método RSA para cifrado de información.
- El algoritmo se basa en la dificultad para descomponer factores primos muy grandes
- Se utiliza ampliamente como base para la criptografía de llave pública.
- Ganaron el premio Túrin en 2002 por esta aportación

- Documentos desclasificados por el gobierno Británico en 1997 hacen referencia a un sistema equivalente descubierto por Clifford Cocks en 1973 (Sí, es agencia de inteligencia británica.)

Funcionamiento RSA

- Sean p y q dos números primos secretos “muy grandes”, $n = pq$
- e es un coprimo a $(p-1)(q-1)$
- d es un secreto $ed \equiv 1 \bmod (p-1)(q-1)$
- m es un mensaje en texto
- c es el mensaje cifrado

Remitente		Destinatario
	Datos públicos: e, n	
m – mensaje Cifrado: $c = m^e \bmod n$		
	c–texto cifrado $\longrightarrow$	
		Descifrado: $m = c^d \bmod n$

Ejemplo

- $p = 11, q = 13$
- $n = pq = 143$
- $(p-1)(q-1) = 130$
- $e = (2^3 - 1) = 7$
- $de \equiv 1 \bmod (p-1)(q-1)$:
  - $7d \equiv 1 \bmod 130$
  - $7 \cdot 103 = 721$
  - $d = 103$

Ejemplo

- $p = 11, q = 13$
- $n = pq = 143$
- $(p-1)(q-1) = 130$
- $e = (2^3 - 1) = 7$
- $de \equiv 1 \bmod (p-1)(q-1)$:
  - $7d \equiv 1 \bmod 130$
  - $7 \cdot 103 = 721$
  - $d = 103$

- j en ASCII $= 74$
- $c = m^e \bmod n$
- $c = 74^7 \bmod 143$
- $c = 12151280273024 \bmod 143$
- $c = 35$
  - $12151280273024 - (143 \cdot 84973987923) = 35$
  - $12151280273024 - 12151280272989 = 35$

Ejemplo

- $c = 35$
- $d = 103$, $n = 143$
- $m = c^d \bmod n = 35^{103} \bmod 143$
- $m = 109397794885431131912169431274237206964441402117990370352407937564807665869703731456055005181949245448691766438796795900961766889736281882505863904953002929687 5 \bmod 143$
- $m = 74$
- 74 en ASCII es j

Ejercicio

- Haga un programa para cifrar y descifrar texto en RSA para primos pequeños:
  - Utilice los valores del ejemplo
  - Utilice su programa generador de números primos, y seleccione los valores.

Discusión

- ¿Qué pasa si se obtiene la factorización de n?

Discusión

- ¿Qué pasa si se obtiene la factorización de n?

- Tome los valores públicos de un compañero, y rompa su esquema (recupere el texto en plano a partir del cifrado)

- Fin de la unidad 2