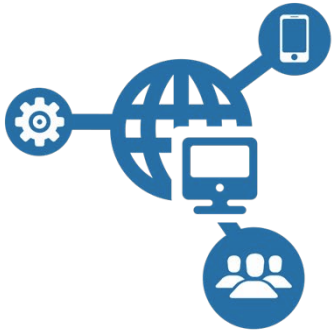

MAESTRÍA EN CIENCIAS EN INGENIERÍA Y TECNOLOGÍAS COMPUTACIONALES

Tema:

Resolución de Problemas

Teoría de Números

Cinvestav Tamaulipas

Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional
Cinvestav - Tamaulipas

Contenido

Temas a desarrollar de Teoría de Números

a. Números naturales

b. Divisibilidad

c. Máximo común divisor

d. Números primos

e. El teorema fundamental de la aritmética

Números primos

- El fundamento de este concepto es la divisibilidad
- El número 1 sólo tiene un divisor positivo, el mismo 1
- El número 1 no se toma como primo solo por conveniencia. No perjudica en nada
- Todo entero mayor de 1 tiene al menos dos divisores, precisamente el número 1 y él mismo. Si estos son los únicos divisores positivos del número entero, éste entero se denomina **primo**
- Si p es primo, -p también es primo, pero sólo se usan los positivos. Todo primo tiene un asociado primo negativo
- Todo entero mayor de 1 que tenga como divisores, además del número 1 y sí mismo, otros divisores positivos, se denomina **compuesto**

Números primos

- Los números primos son la base sobre las que se construyen todos los demás números enteros
- Lema. Si **p** es primo, entonces

$$\text{mcd}(p,a) = \begin{cases} 1 & \text{si } p \nmid a \\ p & \text{si } p \mid a \end{cases}$$

- El divisor menor, distinto de la unidad, de un entero mayor que la unidad, es un número primo

  Sea **q** el divisor menor, distinto de la unidad, de un entero **a** > 1. Si **q** es compuesto tendría un divisor $\mathbf{q_1}$ con la condición $1 < q_1 < q$, pero **a**, siendo divisible por **q**, tendría que ser divisible también por $\mathbf{q_1}$, lo que contradice la hipótesis sobre el número **q**.

Números primos

- Si **p** es primo y **p|ab**, entonces **p|a** o **p|b**.
- Si **a|c** y **b|c** y **mcd(a, b)** = 1, entonces **ab|c**. a y b coprimos
- El divisor menor, distinto de 1, de un número compuesto **a** (debe ser primo) y no es superior a $\sqrt{a}$

  Sea **q** el divisor menor, entonces $\mathbf{a = qa_1}$, $a_1 \geq q$, de donde multiplicando y simplificando por a_1, se tiene $a \geq q^2$ y $q \leq \sqrt{a}$
- La cantidad de números primos es infinita.

  Sean los números primos distintos $p_1, p_2, p_3, \ldots, p_k$, se puede obtener un nuevo número primo que no esté en la lista sumando $p_1, p_2, p_3, \ldots, p_k + 1$, el cual dividiendo a toda la suma, no puede coincidir con ninguno de los primos $p_1, p_2, p_3, \ldots, p_k$

Números primos

- El único primo par es 2
- ¿Cómo decidir si n es primo?
- Si **n** es un número muy grande, probar que **n** sólo es divisible por **1** y **n** involucra muchos cálculos
- Teorema. Sean **a**, **b**, **n ∈ N**, a > 1, b > 1 y n > 1

  a) Si **n = ab**, entonces (**a ≤ √n**) o (**b ≤ √n**)

  b) Si **n** no tiene (divisores primos **≤ √n**)

  entonces n es primo
- Para determinar si un número **n** es primo o no, basta con probar con los divisores primos inferiores a √n
- Corolario. Si **n** es compuesto, **n** tiene un divisor primo **p** ≤ √n

Números primos

Ejemplo

- ¿103 es primo?
- SI, pues no es divisible por ningún primo inferior a

  $\sqrt{103} \approx 10.1$
- Los primos inferiores a 10 son 2, 3, 5 y 7
- Para probar que **n** no es divisible por alguno de los primos se calculan los residuos:

  $r(103,2) = 1$, $r(103,3) = 1$,

  $r(103,5) = 3$, $r(103,7) = 5$

Números primos

- Teorema. Existen arbitrariamente grandes vacíos en la serie de números primos.
- Dado cualquier entero positivo **k**, existen k enteros compuestos consecutivos
- Demostración. Considérense los enteros

  $(k+1)! + 2, (k+1)! + 3, \ldots, (k+1)! + k, (k+1)! + k+1$

  Cada uno es compuesto porque **j** divide a $(k+1)! + j$ si $2 \leq j \leq k + 1$
- Los números primos están espaciados irregularmente
- $\Pi(x)$ denota la cantidad de números primos que no exceden a **x**

Números primos

¿Cuántos primos hay ≤ x

- $\Pi(x)$ denota la cantidad de números primos inferiores o iguales a x
- Hasta 2008, se conocen los primos inferiores a $x = 10^{23}$

  $\Pi(10^{23}) = 1925320391606803968923$
- Una manera de calcular $\Pi(x)$ es la fórmula de Legendre

$$\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum_{1 \le i \le s} \lfloor n/p_i \rfloor + \sum_{i<j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor$$

$$- \sum_{i<j<k} \lfloor n/(p_i p_j p_k) \rfloor + \cdots + (-1)^s \left\lfloor \frac{n}{p_1 p_2 * s p_s} \right\rfloor$$

Números primos

Calcular cuántos primos hay ≤ 64? = $\Pi(64)$ con la fórmula de Legendre

$$\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum_{1 \le i \le s} \lfloor n/p_i \rfloor + \sum_{i<j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor$$

$$- \sum_{i<j<k} \lfloor n/(p_i p_j p_k) \rfloor + \cdots + (-1)^s \left\lfloor \frac{n}{p_1 p_2 * s p_s} \right\rfloor$$

n = 64, $\sqrt{64}$ = 8, los primos ≤ 8 son {2, 3, 5, 7} y $\Pi(\sqrt{64}) = 4$. Por tanto,

$\Pi(64)$ = 64 – 1 + 4 – (⌊64/2⌋ + ⌊64/3⌋ + ⌊64/5⌋ + ⌊64/7⌋) +

+ (⌊64/2*3⌋ + ⌊64/2*5⌋ + ⌊64/2*7⌋ + ⌊64/3*5⌋ + ⌊64/3*7⌋ + ⌊64/5*7⌋)

- (⌊64/2*3*5⌋ + ⌊64/2*3*7⌋ + ⌊64/2*5*7⌋ + ⌊64/3*5*7⌋)

+ ⌊64/2*3*5*7⌋ = 24

Números primos

$$\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum_{1 \le i \le s} \lfloor n/p_i \rfloor + \sum_{i<j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor$$

$$- \sum_{i<j<k} \lfloor n/(p_i p_j p_k) \rfloor + \cdots + (-1)^s \left\lfloor \frac{n}{p_1 p_2 * s p_s} \right\rfloor$$

$\Pi(64) = \Pi(64) = 64 - 1 + 4 - (\lfloor 64/2 \rfloor + \lfloor 64/3 \rfloor + \lfloor 64/5 \rfloor + \lfloor 64/7 \rfloor) +$

64 - 1 + 4 -(32+21+12+9) = 64 - 1 + 4 - 74 = **-7**

+ (|64/2*3| + |64/2*5| + |64/2*7| + |64/3*5| + |64/3*7| + |64/5*7|)

+ (10+6+4+4+3+1) = **28**

(|64/2*3*5| + |64/2*3*7| + |64/2*5*7| + |64/3*5*7|)

+ (2+1+0+0) = **3**

+ |64/2*3*5*7| = **0**

= -7 + 28 + 3 + 0 = 24

$\Pi(64) = 24$

Números primos

La criba de Eratóstenes

- Es un método para determinar los números primos menores que un número natural dado (supongamos d)
  1) Se listan los números que van desde 2 hasta d
  2) Se eliminan de la lista los múltiplos de 2
  3) Se toma el primer primo después de 2 que no fue eliminado (el 3) y se eliminan de la lista sus múltiplos, y así sucesivamente.
  4) El proceso termina cuando el cuadrado del mayor número confirmado como primo es menor que el número final de la lista.
  5) Los números que permanecen en la lista son los primos menores a d

Números primos

La criba de Eratóstenes

- Obtener los números primos menores a 30

	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	27	28	29	30

- Eliminar los múltiplos de 2

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	

Números primos

La criba de Eratóstenes

- El siguiente número es 3. Como $3^2 < 30$, se eliminan sus múltiplos

	2	3		5		7			
11		13				17		19	
		23		25				29	

- El siguiente número es 5. Como $5^2 < 30$ se eliminan sus múltiplos

	2	3		5		7			
11		13				17		19	
		23						29	

Números primos

La criba de Eratóstenes

- El siguiente número es 7. Como $7^2 > 30$, el método termina y los números que quedan son los números primos menores a 30

	2	3		5		7			
11		13				17		19	
		23						29	

Números primos

- Todo entero mayor que 1 se descompone de forma recursiva en un producto de factores primos y, además, de modo único, si no se toma en cuenta el orden de los factores

Sea $a > 1$ y sea p_1 su divisor primo menor, se tiene $a= p_1a_1$. Si $a_1 > 1$ y sea p_2 su divisor primo menor, se tiene $a_1= p_2a_2$. Si $a_2 > 1$ y sea p_3 su divisor primo menor, se tiene $a_2= p_3a_3$. Y así sucesivamente hasta llegar a que $a_n = 1$, entonces $a_{n-1}= p_n$

Multiplicando todas las igualdades obtenidas, a se descompone en factores primos como:

$$a= p_1 p_2 p_3 \dots p_n$$

Ejercicios

...