Estructuras Discretas INF-313

Sergio Hernández, Mónica Acevedo
shernandez@ucm.cl, macevedo@ucm.cl

Facultad de Ciencias de la Ingeniería

UNIVERSIDAD CATOLICA DEL MAULE

Introducción

- La teoría de números es una rama de las matemáticas que estudia las propiedades de los números enteros.

Introducción

- La teoría de números es una rama de las matemáticas que estudia las propiedades de los números enteros.
- Desde el punto de vista práctico, existen muchas aplicaciones en criptografía y compresión de datos y estructuras de datos (hashing).

Definición

Sea $\mathbb{N} = \{1, 2, 3\}$ el conjunto de enteros positivos (números naturales) y $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ el conjunto de enteros.

Divisibilidad

Definición

Sean a y $b \neq 0$ dos números enteros en $\mathbb{Z}$. Se dice que a divide a b (denotado por $a|b$) si existe un entero c tal que $b = ac$

Divisibilidad

Definición

Sean a y $b \neq 0$ dos números enteros en $\mathbb{Z}$. Se dice que a divide a b (denotado por $a|b$) si existe un entero c tal que $b = ac$

- Si $a|b \wedge 0 < a < b \Rightarrow a$ es un divisor propio de b.

Divisibilidad

Definición

Sean a y $b \neq 0$ dos números enteros en $\mathbb{Z}$. Se dice que a divide a b (denotado por $a|b$) si existe un entero c tal que $b = ac$

- Si $a|b \wedge 0 < a < b \Rightarrow a$ es un divisor propio de b.
- Si $a|b \wedge b|c \Rightarrow a|c$.

Divisibilidad

Definición

Sean a y $b \neq 0$ dos números enteros en $\mathbb{Z}$. Se dice que a divide a b (denotado por $a|b$) si existe un entero c tal que $b = ac$

- Si $a|b \wedge 0 < a < b \Rightarrow a$ es un divisor propio de b.
- Si $a|b \wedge b|c \Rightarrow a|c$.
- Si $a|b \wedge a|c \Rightarrow a|(b + c)$

Divisibilidad

Definición

Sean a y $b \neq 0$ dos números enteros en $\mathbb{Z}$. Se dice que a divide a b (denotado por $a|b$) si existe un entero c tal que $b = ac$

- Si $a|b \wedge 0 < a < b \Rightarrow a$ es un divisor propio de b.
- Si $a|b \wedge b|c \Rightarrow a|c$.
- Si $a|b \wedge a|c \Rightarrow a|(b + c)$
- Si $a|b \wedge a|c \Rightarrow a|(b - c)$

Cociente y Residuo

Definición

Sean a y $b \neq 0$ dos enteros positivos en $\mathbb{N}$. Si $b = ac + r$ con c y r enteros en $\mathbb{Z}$, entonces c es el cociente y r el residuo.

Cociente y Residuo

Definición

Sean a y $b \neq 0$ dos enteros positivos en $\mathbb{N}$. Si $b = ac + r$ con c y r enteros en $\mathbb{Z}$, entonces c es el cociente y r el residuo.

- Si $a|b \Rightarrow c = \lfloor a|b \rfloor$.

Cociente y Residuo

Definición

Sean a y $b \neq 0$ dos enteros positivos en $\mathbb{N}$. Si $b = ac + r$ con c y r enteros en $\mathbb{Z}$, entonces c es el cociente y r el residuo.

- Si $a|b \Rightarrow c = \lfloor a|b \rfloor$.
- Si $a|b \Rightarrow r = a - bc$

Python modulo y cociente

```
>>> a=4461
>>> b=16
>>> r=a%b
>>> print r
13
>>> c=a/b
>>> print c
278
>>> a-b*c
13
```

Números primos

Definición

Un entero positivo $p > 1$ es un número **primo** si sus únicos divisores son ± 1 y $\pm p$. Un entero positivo n que no es primo es llamado **compuesto**.

Números primos

Definición

Un entero positivo $p > 1$ es un número **primo** si sus únicos divisores son ± 1 y $\pm p$. Un entero positivo n que no es primo es llamado **compuesto**.

- Existe una infinidad de primos.

Números primos

Definición

Un entero positivo $p > 1$ es un número **primo** si sus únicos divisores son ± 1 y $\pm p$. Un entero positivo n que no es primo es llamado **compuesto**.

- Existe una infinidad de primos.
- Cada número compuesto tiene un factor primo.

Números primos

Definición

Un entero positivo $p > 1$ es un número **primo** si sus únicos divisores son ± 1 y $\pm p$. Un entero positivo n que no es primo es llamado **compuesto**.

- Existe una infinidad de primos.
- Cada número compuesto tiene un factor primo.
- Si n es un número compuesto entonces n tiene un divisor primo p, tal que $p \leq \sqrt{n}$.

Números primos

Definición

Un entero positivo $p > 1$ es un número **primo** si sus únicos divisores son ± 1 y $\pm p$. Un entero positivo n que no es primo es llamado **compuesto**.

- Existe una infinidad de primos.
- Cada número compuesto tiene un factor primo.
- Si n es un número compuesto entonces n tiene un divisor primo p, tal que $p \leq \sqrt{n}$.
- los números primos son los ladrillos con los que se construyen todos los números.

Números primos

Definición

Un entero positivo $p > 1$ es un número **primo** si sus únicos divisores son ± 1 y $\pm p$. Un entero positivo n que no es primo es llamado **compuesto**.

- Existe una infinidad de primos.
- Cada número compuesto tiene un factor primo.
- Si n es un número compuesto entonces n tiene un divisor primo p, tal que $p \leq \sqrt{n}$.
- los números primos son los ladrillos con los que se construyen todos los números.
- Otros los denominan simplemente como los átomos de las matemáticas.

Teorema Fundamental de la Aritmética

Definición

Cualquier entero $n > 1$ se puede escribir como un producto de primos, tal que:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \tag{1}$$

$$= \prod_{i=1}^{k} p_i^{\alpha_i} \tag{2}$$

con p_i y p_j números primos distintos para todo $i \neq j$ y $\alpha_i \in \mathbb{N}$ para todo $i = 1 \ldots k$.

Teorema Fundamental de la Aritmética

Definición

Cualquier entero $n > 1$ se puede escribir como un producto de primos, tal que:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad (1)$$

$$= \prod_{i=1}^{k} p_i^{\alpha_i} \quad (2)$$

con p_i y p_j números primos distintos para todo $i \neq j$ y $\alpha_i \in \mathbb{N}$ para todo $i = 1 \ldots k$.

- Si $p_1 < p_2 < \cdots p_k$ entonces la factorización $n = \prod_{i=1}^{k} p_i$ es única.

Ejemplos

- Encuentre todos los primos entre 50 y 100.

Ejemplos

- Encuentre todos los primos entre 50 y 100.
- Encuentre la factorización única de cada número:
  1. 135
  2. 1330
  3. 3105
  4. 211

Ejemplos

- Encuentre todos los primos entre 50 y 100.
- Encuentre la factorización única de cada número:
  1. 135
  2. 1330
  3. 3105
  4. 211
- Encuentre el m.c.d y m.c.m entre los siguientes números 1048, 786 y 3930.