Introducción a la Teoría de Números

- Concepto
- Nros. naturales y números enteros
- Operaciones elementales en Z
- Esencialmente +
- Divisibilidad | en Z
- Teorema del resto
- Propiedades de |
- Números primos y compuestos
- Máximo común divisor (MDC)
- Mínimo común múltiplo (mcm)
- Algor. de Euclides
- Teorema fundamental de la aritmética
- Otros teoremas

Introducción a la Teoría de Números

Concepto

La teoría de números se refiere a los números enteros, sus operaciones elementales y las propiedades que de ellas se desprenden.

Números Naturales y Números Enteros

N = {0, 1, 2, 3, …}

Z = {…, -3, -2, -1, 0, 1, 2, 3, …}

Operaciones Elementales (aritméticas) en Z

• Adición	+	**a + b = c**	sumandos, suma
• Multiplicación	×	**a x b = c**	factores, producto
• Substracción	–	**a – b = c**	minuendo, sustraendo, resta
• División	**|**	**b | a = c**	divisor, dividendo, cociente

Debe notarse que +, ×, – (esencialmente +) son cerradas en **Z** (siempre la suma, el producto, la resta es un entero) pero **|** no es cerrada en **Z**.

Introducción a la Teoría de Números

Esencialmente +

La adición de una unidad, se define en los enteros como la operación que aplicada a cada entero produce como suma el siguiente número entero:

Si $n \in Z$ entonces $n + 1$ = siguiente número entero luego de n

Luego:

- Adición → reiteradas sumas de 1 — **$a + b = a + \overbrace{1 + 1 + \ldots + 1}^{b \text{ veces}}$**
- Multiplicación → sumas reiteradas — **$a \times b = a + a + a + \ldots + a$**
- Resta → suma condicionada — **$a - b = c$ si y solo si $a = c + b$**

Operativamente armamos una **tabla de sumas** para cada dígito de 0 a 9 y un **procedimiento** para obtener la suma de cualquier par de enteros.

Luego armamos también una **tabla de productos** para cada dígito de 0 a 9 y un **procedimiento** para obtener el producto de cualquier par de enteros.

- División → producto condicionado — **$b \mid a = c$ si y solo si $a = b \times c$**

Introducción a la Teoría de Números

Divisibilidad

Pero como la división no es cerrada en **Z**, ponemos especial atención a la operación:

División Entera: decimos que "b divide a a" y lo simbolizamos "b|a", si existe un entero único "c" tal que a = b x c.

Si ese entero **c** existe, lo denominamos "**cociente de la división de a en b**" y decimos que **"b es un factor de a"**, o que **"b es un divisor de a"** o que "**a es divisible por b"**, o que **"a es un múltiplo de b"**.

Si ese entero no existe, decimos que **"b no divide (exactamente) a a"** o que **"a no es divisible en b"**.

Esta operación goza de muchas propiedades; mencionaremos dentro de ésta unidad algunas de ellas con rango de **teoremas**.

Introducción a la Teoría de Números

Si **a no es divisible en b**, aún podemos realizar una división "aproximada" que resultará en un **resto** además del cociente aproximado de la división.

Algoritmo de la división euclídea (o Teorema del Resto): dados dos números enteros a y b, con b no nulo, existen dos enteros únicos q y r, denominados cociente y resto respectivamente tales que:

$$a = b \times q + r, \quad \text{con } 0 \leq r < |b|$$

En este caso, decimos que la división no es exacta, y que al querer dividir el dividendo **a** en el divisor **b**, se obtiene un cociente **q** y un resto **r**.
Nótese que el teorema afirma que esos enteros **q** y **r son los únicos** que verifican la igualdad con la condición de que el resto **r** sea positivo y menor que el valor absoluto del divisor **b**.
En los lenguajes de programación suele haber operaciones definidas para calcularlos: PASCAL: **q = a div b, r = a mod b – C/JAVA: q = a / b, r = a % b**.

Introducción a la Teoría de Números

Propiedades de la división en Z

Las propiedades de **|** en **Z** son afirmaciones **"demostrables"** por lo que se enuncian como **teoremas**.

- **Teorema 1**. Para cualquier entero **a** no nulo, esto es distinto de cero, se verifica que: **1 | a** **a | 0** **a | a**
- **Teorema 2**. Para cualesquiera números enteros **a**, **b**, **c**, si **a | b** y **b | c** entonces se verifica que **a | c**.
- **Teorema 3**. Todo entero que es divisor de otros, también es divisor de la suma de ellos: **Si** $a|b_1, a|b_2, \ldots, a|b_n$ **entonces** $a \mid (b_1+b_2+\ldots+b_n)$
- **Teorema 4**. Un entero divisor de otro, divide a todos sus múltiplos: **Si** $a|b$ **entonces** $a|(m\times b)$ **para todo** $m \in Z$.
- **Teorema 5.** Un entero que es divisor de otros dos, también es divisor de su diferencia: **Si** $a|b$ **y** $a|c$ **entonces** $a|(b-c)$ (del teorema 3).

Introducción a la Teoría de Números

Propiedades de la división en Z (continuación)

- **Teorema 6**. Un entero que es divisor de otros dos, es también divisor del resto de la división de ellos:

  Si $a|b$ y $a|c$ entonces $a|r$, donde $b = q \times c + r$ con $0 \leq r < |c|$

Notemos que el teorema 1, nos asegura que **todo número entero no nulo** es divisible por la unidad (1) y por sí mismo. Sin embargo, algunos enteros "**SOLO" son divisibles por la unidad y por sí mismos**; éstos son números muy especiales:

Número Primo: Un número entero $p > 1$ se dice que es primo si SÓLO es divisible por sí mismo y por la unidad.

Si el número no es primo, esto es, es un número entero mayor a uno y tiene más de dos divisores, se dice que es un **número compuesto**.

Introducción a la Teoría de Números

El siguiente teorema acelera la determinación de si es o no es, primo:

Teorema 7. Si **$n \in Z^+$ y $n > 1$** es un número compuesto (no primo) entonces tiene un divisor primo menor o igual a su raíz cuadrada.

Tomando este teorema en cuenta, podemos desarrollar un procedimiento para determinar si un número entero **n** es o no es primo:

1. Si **n = 2**, entonces es primo y se termina el procedimiento.
2. Si **2|n** (o sea, **n** es par) entonces no es primo y terminamos (o termina en cinco, o la suma de sus dígitos es tres, etcétera).
3. Si **n** no es par, entonces calculamos la parte entera de su raíz cuadrada $\boldsymbol{k = parte\ entera\ de\ \sqrt{n}.}$
4. Para todos los números primos **p** (o los impares > 1) menores o iguales que **k**, verificar si para algún **p**, ocurre que **p|n**. Según esto:

   SI $\Rightarrow$ COMPUESTO **NO $\Rightarrow$ PRIMO**

Teorema 8. Existen infinitos números primos.

Introducción a la Teoría de Números

Máximo Común Divisor (MCD)

Dados los números enteros **a, b, d** $\in$ **Z**, con **d** $\neq$ **0**, decimos que **d** es un divisor común de **a** y **b**, si **d|a** y **d|b**, esto es si **d** divide a ambos. Pero puede haber varios divisores comunes de **a** y **b**.

Máximo Común Divisor: Se denomina máximo común divisor de los enteros a y b, y se lo denota MCD(a, b), al mayor de sus divisores comunes.

Para determinar cuál es el **MCD(a, b)** para dos números enteros **a** y **b** dados, se pueden determinar todos los divisores de **a** y luego todos los divisores de **b**; luego se buscan los comunes a ambos, y el mayor será el máximo común divisor (**método exhaustivo o de la fuerza bruta**).

Debe notarse que siempre existe este número, ya que en el peor de los casos, el número uno (1) siembre dividirá a ambos según el teorema 1.

Si el **MCD(a, b) = 1** entonces se dice que **a** y **b** son **primos relativos**.

Introducción a la Teoría de Números

Mínimo común múltiplo (mcm)

Dados los números enteros **a, b, d** $\in$ **Z**, con **d** $\neq$ **0**, decimos que **d** es un múltiplo común de **a** y **b**, si **d=a×n** y **d=b×m**, para dos enteros **m** y **n** elegidos adecuadamente. Pero siempre habrá varios múltiplos comunes de **a** y **b**, ya que si **d** es un múltiplo común, también lo será **k×d** con **k**$\in$**Z**.

Mínimo Común Múltiplo: Se denomina mínimo común múltiplo de los enteros a y b, y se lo denota mcm(a, b), al menor de sus múltiplos comunes.

Para determinar cuál es el **mcm(a, b)** para dos números enteros **a** y **b** dados, se pueden determinar algunos múltiplos de **a** y luego algunos múltiplos de **b** hasta conseguir uno en común; luego el primero que se encuentre será el mínimo común múltiplo (**método de la fuerza bruta**).

Debe notarse que siempre existe este número, ya que en el peor de los casos el producto **a×b** es tanto un múltiplo de **a** como de **b**.

Introducción a la Teoría de Números

Algoritmo de Euclides (preliminares)

Sean **a, b ∈ Z** dos números enteros positivos, con **a > b** (en caso de ser al revés, se invierte el orden de los mismos, y en caso de **ser iguales**, es claro que **si a = b entonces MCD(a, b)=a=b**).

El método de la fuerza bruta para calcular el **MCD(a, b)** puede ser muy lento para números suficientemente grandes. Sin embargo, desde el siglo III A.C. se conoce un algoritmo para calcular el máximo común divisor de forma eficiente, descripto en los **Elementos** del matemático griego Euclides. Primero Euclides demostró el siguiente:

Lema: Dados a, b ∈ Z dos números enteros positivos con **a ≥ b**, el **MCD(a, b) = MCD(b, r)**, donde **r** es el resto de dividir **a** en **b**.

Y luego, desarrolló un procedimiento iterativo (un **algoritmo**, que además puede plantearse en forma *recursiva*) para el cálculo del máximo común divisor, aplicando reiteradamente el resultado de este lema.

Algoritmo de Euclides

Sean dos números enteros positivos **a, b** $\in \mathbf{Z^+}$, con **a > b**. Entonces:

1. Se intenta dividir **a** en **b** (el mayor en el menor).
2. Si la división es exacta, entonces **MCD(a, b) = b** y se termina.
3. Si la división no es exacta se obtendrá un **cociente** y un **resto**, y se procederá a aplicar el lema anterior y el algoritmo de la división reiteradamente **hasta que el resto se haga cero**:

$$a = b \times q_1 + r_1 \qquad 0 \leq r_1 < b \qquad \Rightarrow MCD(a, b) = MCD(b, r_1)$$
$$b = r_1 \times q_2 + r_2 \qquad 0 \leq r_2 < r_1 \qquad \Rightarrow MCD(b, r_1) = MCD(r_1, r_2)$$
$$r_1 = r_2 \times q_3 + r_3 \qquad 0 \leq r_3 < r_2 \qquad \Rightarrow MCD(r_1, r_2) = MCD(r_2, r_3)$$
$$\ldots \qquad \ldots$$
$$r_n = r_{n+1} \times q_{n+2} + r_{n+2} \qquad 0 \leq r_{n+2} < r_{n+1} \qquad \Rightarrow MCD(r_n, r_{n+1}) = MCD(r_{n+1}, r_{n+2})$$
$$r_{n+1} = r_{n+2} \times q_{n+3} + 0 \qquad 0 = r_{n+3} < r_{n+2} \qquad \Rightarrow MCD(r_{n+1}, r_{n+2}) = MCD(r_{n+2}, 0) = r_{n+2}$$

Así, el MCD(a, b) es igual al último resto no nulo del algoritmo.

Introducción a la Teoría de Números

Teorema Fundamental de la Aritmética (factoreo)

Todo número entero positivo mayor a uno, o es un número primo, o puede ser expresado como producto de números primos de forma **única**, salvo el orden de los factores. En símbolos:

Si $a \in Z^+$ y $a > 1$ entonces $$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_n^{a_n}$$

donde los p_i son números primos y los a_j números naturales.

Éste es el resultado **más importante** de la teoría de números que veremos, y en él se basan casi todos los sistemas de claves de seguridad mundiales.

Ya desde la enseñanza media aprendemos a "factorear" un número entero positivo, esto es, descomponerlo en sus factores primos p_i mediante el procedimiento de hacer divisiones sucesivas por los primos menores a él.

Esto siempre se puede hacer, y como asegura el teorema, los factores que se obtienen son únicos.

Introducción a la Teoría de Números

Euclides demostró también que existen una infinidad de números primos.

Teorema 9. Sean **a, b** $\in \mathbf{Z^+}$ dos números enteros positivos y, aplicando el Teorema Fundamental de la Aritmética, supongamos que han sido factoreados de la siguiente forma:

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_n^{a_n} \qquad b = p_1^{b_1} \times p_2^{b_2} \times \cdots \times p_n^{b_n}$$

Entonces se pueden calcular utilizando esta factorización:

$$\mathbf{MCD(a, b)} = p_1^{min(a_1,b_1)} \times p_2^{min(a_2,b_2)} \times \cdots \times p_n^{min(a_n,b_n)}$$

$$\mathbf{mcm(a, b)} = p_1^{máx(a_1,b_1)} \times p_2^{máx(a_2,b_2)} \times \cdots \times p_n^{máx(a_n,b_n)}$$

Esto lleva a la conocidas reglas: **el MCD de dos números es el producto de los factores primos comunes a ambos al menor exponente**, y **el mcm de dos números es el producto de los factores primos comunes y no comunes a ambos, al mayor exponente**.

Introducción a la Teoría de Números

Del teorema 9 provine el nombre de **primos relativos** o **coprimos**, dado a dos números **a** y **b** cuyo **MCD(a, b) = 1**. Si esto ocurre, significa que **NO TIENEN** factores primos en común.

Teorema 10. Sean **a, b** $\in$ $\mathbf{Z^+}$ dos números enteros positivos. Entonces se cumple que: **a × b = MCD(a, b) × mcm(a, b)**.

Este teorema nos brinda nuevas formas de calcular el **mcm(a, b)**. Por ejemplo, podríamos utilizar el Algoritmo de Euclides para calcular el máximo común divisor de **a** y **b**, y luego despejar el **mcm(a, b)**.

Esto puede resultar sumamente útil si los números en cuestión son muy grandes, ya que el proceso de factorización siempre existe, pero para números grandes es extremadamente lento.