2019-09-16

Teoría de Números

- orientada a C.S.

- def. el estudio de los enteros y sus propiedades
  - def. divisibilidad: dados dos enteros a, b decimos "a" divide a "b" $(a \mid b)$, si existe un entero q tal que:

$$b = a \cdot q$$

! entendemos a la división como restas sucesivas

$$b - aq = 0$$

$$b - \underbrace{a - a - \dots - a}_{q \text{ veces}} = 0$$

a "b" le quito "q" veces "a" hasta llegar a 0, si no es exacto y hay un residuo

- cuando no termina en 0:

$$b - qa = \underbrace{r}_{r > 0}$$

} se le conoce como "algoritmo de la división de Euclides"

∴ b se puede escribir como:

$$b = r + qa$$, donde "q" y "r" son únicos y $0 \leq r < a$

Indefinición
$0 = \square \cdot 0 + 0$

! Cuando $r \neq 0$, decimos "a" no divide a "b" o $(a \nmid b)$

Def: Número Primo: un <u>número entero positivo</u> que tiene exactamente <u>dos</u> divisores.

- alterna: número que solo se divide por 1 o por sí mismo

ID Primos = {1, ∞}
ID Compuesto = {1, ∞}

⚠ Los divisores tienen que ser <u>distintos</u>.

- <u>uno</u> es un <u>compuesto</u>
- un número compuesto tiene <u>más</u> de <u>dos</u> divisores

- los números primos son la <u>clave</u> de la criptografía.

▲ **Teorema de Euclides:**

"Hay infinitos números primos"

▲ **Teorema fundamental de la aritmética:**

"un número entero es primo o es un producto de potencias de números primos".

• inducción fuerte

Ej:

31 es primo,

$\sqrt{31} \approx 5$ propar del 1 - 5

$2 \nmid 31$; $3 \nmid 31$; $5 \nmid 31$

$72 = 2^3 \cdot 3^2$

▲ **Def.** El máximo común divisor: dados dos enteros positivos "a" & "b", si existe un entero positivo "c" que cumple ambas:

1) $(c \mid a) \wedge (c \mid b)$ 2) Cualquier otro divisor de "a" y "b", d cumple: $(d \mid c)$ propiedad del máximo

Entonces, c es el máximo común divisor de a y b

escrito (mcd) de (a, b)

$$mcd(a,b) = C$$

Ej el ejemplo de la mis o profe:

48	2
24	2
12	2
6	2
3	3
1	

84	2
42	2
21	3
7	7
1	

$mcd(2,2,3) = 12$