Numeros primos

Un número primo es un número natural mayor que 1 que tiene únicamente dos divisores positivos distintos: él mismo y el 1.

Sea $p \in \mathbb{N}$, un número primo

$\boxed{p = p}$

$a \in \mathbb{N}$, $a \notin \mathbb{P}$

$$a = 2^{p_1} \cdot 3^{p_2} \cdot 5^{p_3} \cdot 7 \dots$$

$$a = p_1^{\#p_1} \cdot p_2^{\#p_2}$$

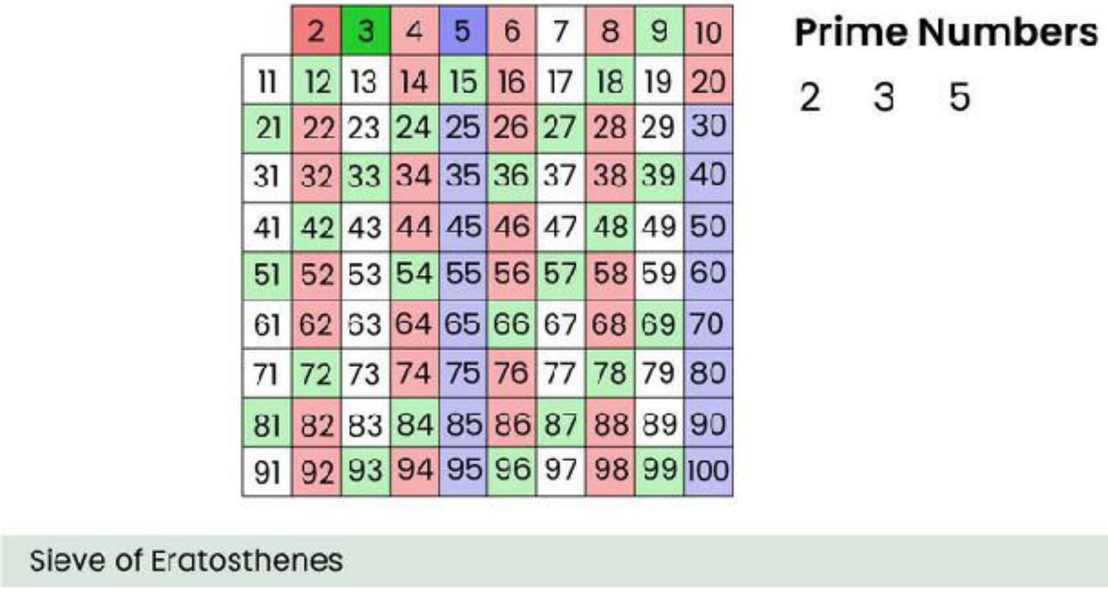
$4 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 1$

T. F. A.

$\forall a \in \mathbb{N}$ $\quad 2^{p_1} \cdot 3^{p_2} \cdot 5^{p_3} \cdots$

$\exists!$ $(p_1, p_2, p_3 \ldots)$ t. q $\quad a = 2^{p_1} \cdot 3^{p_2} \cdot 5^{p_3} \cdots$

Criba de Eratostenes

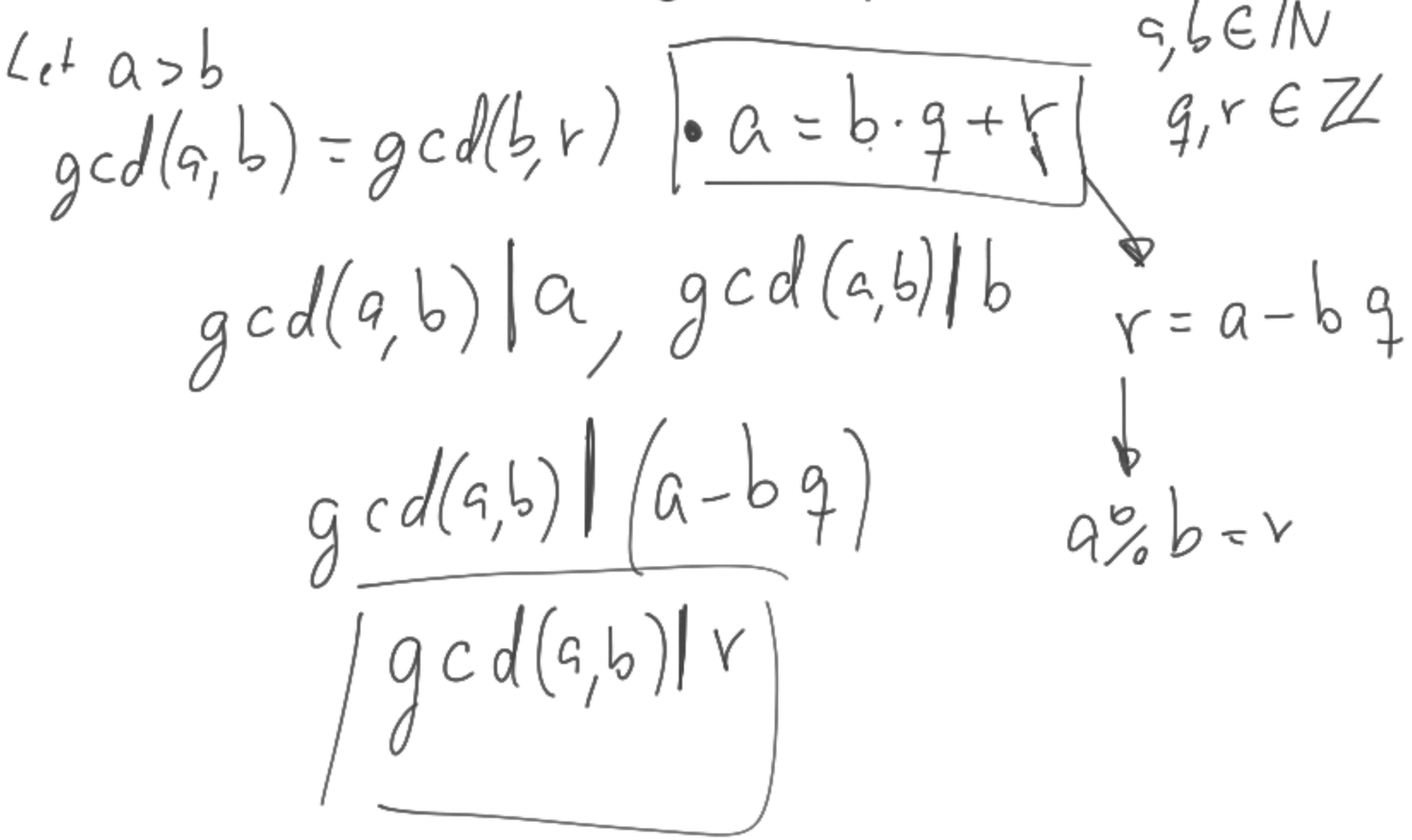


Factorizacion en factores primos

```cpp
vector<int> factor(int n) {
    vector<int> ret;
    for (int i = 2; i * i <= n; i++) {
        while (n % i == 0) {
            ret.push_back(i);
            n /= i;
        }
    }
    if (n > 1) { ret.push_back(n); }
    return ret;
}
```

GCD o MCD

El MCD de dos números es el mayor divisor posible de dos números, es decir, el número más grande que divide ambos números.




```java
int gcd(int a, int b) {
    if (b == 0)
        return a;
    return gcd(b, a % b);
}
```

LCM o MCM

$$LCM(a,b) = \frac{a \cdot b}{gcd(a,b)}$$

$a \cdot b / gcd(a,b)$ ✗

$(a / gcd(a,b)) \cdot b$ ✓

$gcd(a,b) = d$

$a = d \cdot a_0 \qquad b = d \cdot b_0$

$a_0, b_0 \in \mathbb{N}$ | a_0, b_0 son coprimos

$d \cdot a_0 \cdot b_0$ → multiplo de a y b

m es multiplo de $a, b \Rightarrow$ a divide a m, b divide a m

$m = k \cdot a \ (k \in \mathbb{N}) = k \cdot d \cdot a_0$ ← divisible por $d b_0$

$k a_0$ divisible por b_0

K divisible por b_0

Aritmetica modular

$$(a + b) \bmod m = (a \bmod m + b \bmod m) \bmod m$$

$$(a - b) \bmod m = (a \bmod m - b \bmod m) \bmod m$$

$$(a \cdot b) \pmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$$

$$a^b \bmod m = (a \bmod m)^b \bmod m$$

Aritmetica modular

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$

If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$	Symmetric Property
If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$	Transitive Property
If $a \equiv b \pmod{m}$ then $ac = bc \pmod{mc}$ for $c > 0$	Scalar Multiple
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c = (b + d) \pmod{m}$	Addition Property
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac = bd \pmod{m}$	Multiplication Property
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a - c = (b - d) \pmod{m}$	Substraction Property

Exponenciacion modular

```
6  ll exp(ll x, ll n, ll m) {
7      assert(n >= 0);
8      x %= m;  // note: m * m must be less than 2^63 to avoid ll overflow
9      ll res = 1;
10     while (n > 0) {
11         if (n % 2 == 1) { res = res * x % m; }
12         x = x * x % m;
13         n /= 2;
14     }
15     return res;
16 }
```

Inverso modular

$$ax \equiv 1 \pmod{m}$$

F.L.T.

$$a^{p-1} \equiv 1 \pmod{p}$$ → si p es primo

$$a^{p-2} \cdot a \equiv 1 \pmod{p}$$

a^{p-2} es inverso multiplicativo de a $\forall a$

$a^{p-2} \% p$

Bezout's Identity

$$a \cdot x + b \cdot y = \gcd(a, b)$$

$\forall a, b \in \mathbb{N} \quad \exists x, y \in \mathbb{Z} \text{ s.t. } ax + by = \gcd(a, b)$

Conjecture de Goldbach

$\forall a \in \mathbb{N} \quad a > 2$

$\exists p_1, p_2 \in \mathbb{P}$

$$a = p_1 + p_2$$