* prime factorisation : $x = p_1^a \, p_2^b \, p_3^c \, p_4^d \, p_5^e \ldots$

$p_1, p_2, p_3 \ldots$ are prime factors.

1. $\tau(n)$ Total no. of divisors $= (a+1) * (b+1) * (c+1) * \ldots$

2. Sum of all the factors $\sigma(n)$ $= \prod_{i=1}^{k} (1 + p_i + \ldots + p_i^{a_i})$.

$$= \left(\prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1} \right).$$

3. Product of all factors $= \mu(n) \Rightarrow n^{\tau(n)/2}$

Density of Primes:

$\pi(n)$: $\approx \dfrac{n}{\ln n}$

no. of prime no $\leq n$

*.

$\pi(10^6) = \boxed{78498}$ $\quad 10^6 / \ln_{10} 6 \Rightarrow 72382$

Conjectures:

- Goldbach conjecture: Every even integer > 2 can be represented as sum of two prime number.

$n = a + b$ (a, b are prime)
$(n \geq 2)$

$$78 = 37 + 41$$

- Twin Prime conjecture: There are infinite number of pairs of the form $\{p, p+2\}$ where both p & $p+2$ are prime $(3, 5)$ $(37, 39)$ $(41, 43)$ - - -

- Legendre's conjecture: There is always one prime no. b/w n^2 & $(n+1)^2$.

Sieve of eratosthenes. Proof (Complexity)

```
for ( u=2 ; u<=n ; u++) {
    if ( sieve[x]) continue
    for ( v= 2*u; v<=n; v+=u) {
        sieve[u] = x ;
    }
}.
```

Inner loop executed n/x times,

$$\sum_{x=2}^{n} (n/x) \Rightarrow n/2 + n/3 + \dots n/n \Rightarrow O(n\log n).$$

$$\Rightarrow n\left[\, 1/2 + 1/3 + \dots 1/n \right).$$

$$\Rightarrow n(\log n)$$

$n\log\log n \sim O(n)$

$\to (n \log n)$

$n \log\log n. \sim O(n)$

Euclid's Algorithm:

$$gcd(a,b) = \max\{k > 0 : (k|a) \text{ and } (k|b)\}$$

$$gcd(a,b) = \begin{cases} a & \text{if } b = 0 \\ gcd(b, a\%b) & \text{otherwise.} \end{cases}$$

$O(\log(\min(a,b)))$

* worst T.C for consequtive Fibonacci numbers

* BINARY GCD

* If both a, b are evens

$gcd(2a, 2b) = 2\,gcd(a,b)$

* $gcd(2a, b) = gcd(a,b)$ if $b\%2 = 1$

* $gcd(a,b) = gcd(b, a-b)$ if $a\%2 = b\%2 = 1$.

fastergcd:

```
int gcd (int a, int b) {
        if (!a || !b) {
                return a | b;
        }
        unsigned shift = __builtin_ctz(a | b);
        a >>= __builtin_ctz(b);
```

```
unsigned shift = __builtin_ctz(a|b);
a >>= __builtin_ctz(a);
do {
        b >>= __builtin_ctz(b);
        if (a>b)
              swap(a,b);
        b -= a;
    } while(b);
  return a << shift;
}.
```

Euler's Totient function :

$gcd(a,b) = 1 \Rightarrow$ a & b are coprime,

E.T.F given no. of coprime numbers to N.

$$\varphi(N) = \prod_{i=1}^{K} p_i^{\alpha_i - 1} (p_i - 1)$$

ex : $N = 12$

$12 = 2^2 \times 3$ $\quad \varphi(12) = (2^1 \times 1) \times (3^0 \times 2) = 4.$

If $N \rightarrow$ prime $\varphi(N) = N-1.$

Imp prop. If 'd' are divisors of 'n' :

$$\boxed{\sum \varphi(d) = N}$$