Number theory

Number theory is a part of math that deals with integers (whole numbers like -2, 0, 5, etc.).
It's super useful in competitive programming because many problems involve tricky integer-based tricks and optimizations.

Even simple-looking problems can be surprisingly hard! For example, take this equation:

$$x^2 + y^2 = 3$$

At first glance, it seems easy. If we allow real numbers, there are infinite solutions, like:

$$x = \sqrt{2}, y = 1$$
$$x = 1.5, y = \sqrt{0.75}$$

But if we only allow integer solutions (x and y must be whole numbers), does a solution exist?
Let's check:

If $x = 0 \rightarrow y^2 = 3 \rightarrow y$ is not an integer ($\sqrt{3} \approx 1.732$).

If $x = 1 \rightarrow y^2 = 2 \rightarrow y$ is not an integer ($\sqrt{2} \approx 1.414$).

If $x = 2 \rightarrow y^2 = -1 \rightarrow$ Not possible since squares can't be negative.

So, no integer solutions exist! This shows how number theory problems can be tricky even when they look simple.

What to expect from this series

1. Sieve, Prime Factorization and Divisors
2. Number of Divisors / Sum of Divisors / Sigma Function
3. Euler's Totient Function / Phi Function
4. Euclidean Algorithm
5. Extended Euclid
6. Bezout's Identity
7. Chinese Remainder Theorem (CRT)
8. Linear Diophantine Equation with Two Variables
9. Number of Solutions to a Basic Linear Algebraic Equation
10. Sum of Floors
11. Fibonacci Numbers

Primes and Factors

Factors (Divisors)

A number a is called a factor (or divisor) of b if a divides b exactly (with no remainder).

Notation:

If a divides b, we write $a|b$.

If a does not divide b, we write $a\nmid b$.

Example:

The factors of 24 are: 1, 2, 3, 4, 6, 8, 12, 24.

So, $4|24$ (because $24 \div 4 = 6$), but $5\nmid 24$ (since $24 \div 5 = 4.8$, not an integer).

Prime Numbers

A number $n > 1$ is a prime if its only positive divisors are 1 and itself.

Examples:

Primes: 2, 3, 5, 7, 11, 13, ...

Non-primes (composite numbers): 4 (divisible by 2), 6 (divisible by 2, 3), 9 (divisible by 3), etc.

Prime Factorization

Every integer $n > 1$ can be written uniquely as a product of primes:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$$

where:

-> $p_1, p_2, \ldots, p_k$ are distinct primes,

-> $\alpha_1, \alpha_2, \ldots, \alpha_k$ are their respective exponents (≥ 1).

Example:

The prime factorization of 84 is:

$$84 = 2^2 \times 3^1 \times 7^1$$

(We can write this as 2×2×3×7.)

Number of Factors (τ(n))

The number of positive divisors of a number n (denoted by $\tau(n)$) can be calculated using its prime factorization.

If:

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

then:

$$\tau(n) = (\alpha_1+1) \times (\alpha_2+1) \times \ldots \times (\alpha_k+1)$$

Why?

For each prime p_i, its exponent in a divisor can range from 0 to α_i, giving α_i+1 choices.

Example:

Take n=84:

$$84 = 2^2 \times 3^1 \times 7^1$$

Number of factors:

$\tau(84)=(2+1)\times(1+1)\times(1+1)=3\times2\times2=12$

The factors are:

1,2,3,4,6,7,12,14,21,28,42,84

Sum of Factors (σ(n))

The sum of all positive divisors of n (denoted $\sigma(n)$) can be computed as:

$$\sigma(n) = \prod_{i=1}^{k} (1 + p_i + p_i^2 + \ldots + p_i^{\alpha_i}) = \prod_{i=1}^{k} \left(\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right)$$

(This uses the formula for the sum of a geometric series.)

Example:

For n=84:

$$\sigma(84) = \frac{2^3-1}{2-1} \times \frac{3^2-1}{3-1} \times \frac{7^2-1}{7-1} = 7 \times 4 \times 8 = 224$$

(Check: 1+2+3+4+6+7+12+14+21+28+42+84=224)

Product of Factors (μ(n))

The product of all positive divisors of n (denoted $\mu(n)$) is:

$$\mu(n) = n^{\tau(n/2)}$$

Why?
Divisors can be paired as $(d, n/d)$, and each pair multiplies to n. Since there are $\tau(n)/2$ such pairs:

Example:

For n=84:

$\tau(84)=12 \Longrightarrow \mu(84)=846=351298031616$

(Check: 1×84=84, 2×42=84, 3×28=84, etc.)

Perfect Numbers

A number n is called perfect if it equals the sum of its proper divisors (excluding itself):

$$n = \sigma(n) - n$$

Example:

28 is a perfect number because:

1+2+4+7+14 = 28

6 is also perfect:

1+2+3 = 6

Open Problem:

Are there any odd perfect numbers? No one knows yet!

Number of primes

Infinite Number of Primes

Theorem: There are infinitely many prime numbers.

Proof (by contradiction):

Suppose there were only a finite number of primes. Let them be:

$P=\{p_1,p_2,\ldots,p_n\}$

(Example: $p_1=2, p_2=3, p_3=5, \ldots$).

Now, construct a new number:

$N=p_1 \times p_2 \times \ldots \times p_n+1$

(Example: If P={2,3,5}, then N = 2×3×5+1 = 31).

Key Observation:

-> N is not divisible by any prime in P (since it leaves a remainder of 1 when divided by any p_i).

-> But N must have a prime factor (either itself or a new prime not in P).

Contradiction: P was supposed to contain all primes, but we found another prime (either N or its factor).

Conclusion: There must be infinitely many primes.

Density of primes

The density of primes describes how frequently primes appear among numbers.

Definition: $\pi(n)$ = number of primes $\leq n$.

Example: $\pi(10)=4$ (primes: 2, 3, 5, 7).

$\pi(20)=8\pi(20)=8$ (primes: 2, 3, 5, 7, 11, 13, 17, 19).

Prime Number Theorem (Approximation):

For large n,

$$\pi(n) \approx \frac{n}{\ln n}$$

This means primes become less frequent as numbers grow, but they still appear fairly often.

Example:

$$\text{For } n = 10^6 : \pi(10^6) = 78{,}498 \quad \text{(actual count)} \frac{10^6}{\ln(10^6)} \approx 72{,}382 \quad \text{(approximation)}$$

The approximation is about 8% off, but gets better for larger n.

Conjectures

Despite centuries of research, some problems about primes remain unsolved.
These conjectures are widely believed to be true, but no proofs exist yet.

1. Goldbach's Conjecture

Statement:
Every even integer n>2 can be written as the sum of two primes.

Examples:

4 = 2+2

10 = 3+7 = 5+5

100 = 3+97 = 11+89

Status:
✔ Verified for all n≤4×10^18 (computationally).
❌ No general proof exists.

Fun Fact:
A similar conjecture (weak Goldbach) states that every odd n>5 is the sum of three primes—this was proven in 2013!

2. Twin Prime Conjecture

Statement:
There are infinitely many twin primes—pairs of primes differing by 2.

Examples:

(3,5)

(11,13)

(1, 000, 037, 1, 000, 039)

Status:
✔ Infinite pairs with gaps ≤ 246 exist (Zhang, 2013).
❌ No proof for gaps = 2 yet.

Programming Angle:
Finding twin primes efficiently requires optimized sieving algorithms.

3. Legendre's Conjecture

Statement:
There's always at least one prime between n^2 and (n+1)^2 for any integer n≥1.

Examples:

n=1: Between 1 and 4 → primes 2,3.

n=2: Between 4 and 9 → primes 5,7.

n=10: Between 100 and 121 → primes 101,103,...,113.

Status:
✔ Verified up to n=10^18.
❌ No general proof.

Implications:
If true, primes are dense enough to avoid large gaps between squares.

Basic Prime Algorithms

1. Primality Check (Trial Division)

Idea:

A number n is prime if it has no divisors other than 1 and itself. To test this efficiently:

Only check divisors up to √n (since if n=a×b, one of them must be ≤ √n).

Algorithm:

```
bool is_prime(int n) {
    if (n < 2) return false;           // 0 and 1 are not primes
    for (int x = 2; x * x <= n; x++) {
        if (n % x == 0) return false;  // Found a divisor → not prime
    }
    return true;                       // No divisors → prime
}
```

Time Complexity: O(√n)

2. Prime Factorization (Trial Division)

Idea:

Break down n into its prime factors by repeatedly dividing by the smallest possible primes.

Algorithm:

```
vector<int> prime_factors(int n) {
    vector<int> factors;
    for (int x = 2; x * x <= n; x++) {
        while (n % x == 0) {          // Divide n by x as long as possible
            factors.push_back(x);
            n /= x;
        }
    }
    if (n > 1) factors.push_back(n);  // Last remaining prime factor
    return factors;
}
```

Time Complexity: O(√n)

i	n	ret
2	252	$\{\}$
2	126	$\{2\}$
2	63	$\{2,2\}$
3	21	$\{2,2,3\}$
3	7	$\{2,2,3,3\}$