Number Theory

The part of mathematics devoted to the study of the set of integers and their properties is known as number theory.

- ★ Prerequisite
- ★ Divisibility
- ★ Modular Arithmetic
- ★ Primes

Prerequisite

Ceil and Floor

★ Ceil is a mathematical function the rounds the number up.

- $\lceil 2 \rceil = 2$
- $\lceil 2.01 \rceil = 3$
- $\lceil 3.9 \rceil = 4$
- $\lceil 5.1 \rceil = 6$

Ceil and Floor

★ Floor is a mathematical function the rounds the number down.

- $\lfloor 2 \rfloor = 2$
- $\lfloor 2.01 \rfloor = 2$
- $\lfloor 3.9 \rfloor = 3$
- $\lfloor 5.1 \rfloor = 5$

NOTE: C++ Truncate decimal part when working with integers .e.g(int, long long)

Types of Integers

- Even Number An integer that is a multiple of 2.
  - 2, 4, 6, 8, ...
- Odd Numbers Any none even number.
  - 1, 3, 5, 7, ...
- Prime Numbers A positive integer with exactly two positive divisor: itself and 1.
  - 2, 3, 5, 7, 11, ...
- Composite Numbers Any none prime number.
  - 4, 6, 8, 9, 10, ...

Sequences and Summations

Sequences

A sequence is a discrete structure used to represent an ordered list. For example, 1, 2, 3, 5, 8 is a sequence with five terms and 1, 3, 9, 27, 81 , … , 3n , … is an infinite sequence.

Sequences and Summations

Arithmetic progression

$a, a + d, a + 2d, \dots , a + nd, \dots$

a is an initial term

d is a common difference

$term_n = a + d(n-1)$

Even numbers is an arithmetic sequence ($a = 2$, $d = 2$)

2, 4, 6, 8, …..

Odd numbers is a arithmetic sequence ($a = 1$, $d = 2$)

1, 3, 5, 7, …..

Sequences and Summations

Arithmetic progression

Summation of first n terms with a(initial term) and d (common difference)

$S_n = (n/2) \cdot (2 \cdot a + d \cdot (n-1))$

Summation of first n terms with a(initial term) and L(nth term)

$S_n = (n/2) \cdot (a + L)$

Sequences and Summations

PROBLEM

Count the number of substrings for a string of length n

aabcd (n = 5)

5 + 4 + 3 + 2 + 1

1 + 2 + 3 + 4 + 5 (a = 1, d = 1)

Sn = (5/2) * (1 + 1 + 1(4)) = 5 / 2 * 6 = 15

Divisibility

Divisibility

Definition

If a and b are integers with a ≠ 0, we say that a divides b if there is an integer c such that b = ac (or equivalently, if b/a is an integer).

When a divides b we say that a is a factor or divisor of b, and that b is a multiple of a.

- $a \mid b$ denotes that a divides b.
- $a \nmid b$ denotes a does not divide b

EXAMPLES

- 3 … 7
- 3 … 6
- 7 … 7
- 7 … 14
- 2 … 9
- 5 … 25

EXAMPLES

- $3 \nmid 7$
- $3 \mid 6$
- $7 \mid 7$
- $7 \mid 14$
- $2 \nmid 9$
- $5 \mid 25$

THEOREM

Let a, b, and c be integers, where $a \neq 0$. Then

- if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$
- if $a \mid b$, then $a \mid bc$ for all integers c
- if $a \mid b$ and $b \mid c$, then $a \mid c$

if $a \mid b$, then $a \mid bn$ for all integers n and $a \mid c$, then $a \mid cm$ for all integers m

then $a \mid (bn + cm)$

Modular Arithmetic

If the first day of a given year is saturday what is the name of day 27 of this year?

Hmmmmm 🤔?

1. Saturday
2. Sunday
3. Monday
4. Tuesday
5. Wednesday
6. Thursday
7. Friday

- **27 - 7 = 20**
- **20 - 7 = 13**
- **13 - 7 = 6**
- **6** (Thursday)

Here 6 is called Remainder.

We can do it faster with mod operator (%)

27 % 7 = 6

27 = 3 * 7 + 6(remainder)

Let’s generalize this equation

THEOREM

Let a be an integer and d a positive integer.

Then there are unique integers q and r, with $0 \le r < d$, such that

$$a = qd + r$$

$$q = \lfloor a/d \rfloor \quad \text{(quotient)}$$

$$r = a \bmod d = a - qd \quad \text{(remainder)}$$

Let m be a positive integer and let a and b be integers. Then

- $(a + b) \bmod m = (a \bmod m + b \bmod m) \bmod m$
- $(a - b) \bmod m = (a \bmod m - b \bmod m) \bmod m$
- $(a \times b) \bmod m = (a \bmod m \times b \bmod m) \bmod m$
- $(a \wedge b) \bmod m = (a \bmod m) \wedge b \bmod m$
- $(a / b) \bmod m \neq (a \bmod m / b \bmod m) \bmod m$ (WRONG ⛔!)

NOTE : We use Modular Inverse, extended euclidean algorithm in solving this equation (a/b) mod m.

REMARK: we say that a divides b if there is an integer c such that b = ac

b = ac + 0

q (quotient) = a

r (remainder) = 0

Then we exclude the following, if a divides b then b mod a = 0

- If a | b, then b % a = 0.
- If b % a = 0, then a | b.

Primes

Definition

An integer p greater than 1 is called prime if the only positive factors of p are 1 and p.

A positive integer that is greater than 1 and is not prime is called composite.

Primes : 2, 3, 5, 7, 11, 13, 17, 19, 23, ………..

Composite : 4, 6, 8, 9, 10, 12, 14, 15, 16, ………

If $a \mid b$ and $a \neq 1$ and $a \neq b$ then b is a composite number(not prime).

THEOREM

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes, where the prime factors are written in order of nondecreasing size.

$9 = 3 \cdot 3 = 3^2$

$15 = 3 \cdot 5$

$24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$

$641 = 641$

$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$

$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

PROBLEM

Given an integer n find its divisors.

Someone say : let's iterate from 1 to n and check if the current number divides n or not.

Time Complexity : O(n)

Can we do better 🤔 !? Hmmmmmmm ….

Yes 🤗, let's analyze

If we have integer a , b and b divides a Then $a = bc$

$a / b = c$ and $a / c = b$

Let’s say that one of these two divisors (b,c) is less than or equal $\sqrt{a}$

Then, it’s sufficient to iterate from 1 up to $\sqrt{a}$

But why one of them is less than $\sqrt{a}$

Let’s say b and c and greater then $\sqrt{a}$

$bc > \sqrt{a}\,\sqrt{a}$

$bc > a$, which is a contradiction.

Time Complexity : $O(\sqrt{a})$

PROBLEM

Check if n is prime number of not

PROBLEM

Get the prime factorization for number n

PROBLEM

Given a and b get their greatest common divisor (gcd) (analyzed later)

PROBLEM

Given a and b get their least common multiple (lcm) (analyzed later)

Greatest Common Divisors

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b.

The greatest common divisor of a and b is denoted by gcd(a, b).

gcd (24, 36) = ?

The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12. Hence, gcd(24, 36) = 12.

Definition : The integers a and b are relatively prime (co primes) if their greatest common divisor is 1.

Are 17 and 22 relatively primes (co primes) ?

gcd(17,22) = 1, then the answer is YES.

Definition : The integers a_1 , a_2 , … , a_n are pairwise relatively prime

if $\gcd(a_i , a_j) = 1$ whenever $1 \leq i < j \leq n$.

10, 17, 21 are pairwise relatively prime.

USING prime factorization to get gcd(a,b)

$a = p_1^{a1}\ p_2^{a2} \dots p_n^{an}$

$b = p_1^{b1}\ p_2^{b2} \dots p_n^{bn}$

$gcd(a,b) = p_1^{min(a1,b1)}\ p_2^{min(a2,b2)} \dots p_n^{min(a3,b3)}$

$120 = 2^3 \cdot 3 \cdot 5$

$500 = 2^2 \cdot 5^3$

$gcd(120,500) = 2^{min(3,2)} \cdot 3^{min(1,0)} \cdot 5^{min(1,3)} = 20$

least common multiple

The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b.

The least common multiple of a and b is denoted by lcm(a, b).

$a = p_1^{a1}\, p_2^{a2} \cdots p_n^{an}$

$b = p_1^{b1}\, p_2^{b2} \cdots p_n^{bn}$

$\mathrm{lcm}(a,b) = p_1^{\max(a1,b1)}\, p_2^{\max(a2,b2)} \cdots p_n^{\max(a3,b3)}$

$120 = 2^3 \cdot 3 \cdot 5$

$500 = 2^2 \cdot 5^3$

$\mathrm{lcm}(120,500) = 2^{\max(3,2)} \cdot 3^{\max(1,0)} \cdot 5^{\max(1,3)} = 3000$

THEOREM

Let a and b be positive integers. Then $ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$.

$a = 120$

$b = 500$

$\gcd(a,b) = 20$

$\operatorname{lcm}(a,b) = 3000$

$120 \cdot 500 = 60000$

$20 \cdot 3000 = 60000$

PROBLEM

Given a and b get their greatest common divisor ($a < b$)

Someone say : let’s Get all divisors of a and get the greatest one the divides b.

Someone say : let’s Get Their prime factorization of a and get the greatest one the divides b.

Time Complexity : $O(\sqrt{a})$

Can we do better 🤔 !? Hmmmmmmm ….

Yes 🤗, let’s analyze

The Euclidean Algorithm

gcd(a,b) = c, then c | a and c | b

a = qb + r , a - qb = r, r = a % b.

gcd(a,b) = gcd(b,r) = gcd(b, a % b)

c | a , c | b

c | na + mb

c | a - qb

c | r

gcd(a,b) = gcd(b,r)

Time Complexity : O(log(min(a,b))

PROBLEM

Given an integer n find all primes <= n

Someone say let's iterate from 1 to n and check if the current number is prime or not.
Time Complexity : $O(n\sqrt{n})$

Can we do better 🤔 !? Hmmmmmmm ….

Yes 🤗, let's analyze

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

The Sieve of Eratosthenes

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49

Time Complexity : O(nlog(n))

THANKS

🥰