Number Theory Advanced - 1

Dev Karan Singh (devkaran1231)
Expert at codeforces (1817)
5 star at codechef (2040)

Number Theory Advanced - 1

- GCD & LCM
- Euclid’s Algorithm
- Extended Euclid’s Algorithm
- Linear Diophantine Equation
- Binary Exponentiation
- Modular Arithmetic
- Modular Multiplicative Inverse (Fermat Little Theorem)

GCD / LCM

↳ greatest common Divisor

$\gcd(5, 15) \rightarrow 5$

$\gcd(-5, 5) \rightarrow 5$

$\gcd(0, 7) \rightarrow 7$

$\gcd(-5, -10) \rightarrow 5$

$$\gcd(a,b) = \gcd(\operatorname{abs}(a), \operatorname{abs}(b))$$

$$\max(\gcd(a,b)) = ?$$

$$\max(\gcd(a,b)) = \min(a,b)$$

```
for(int i = min(a,b), i >= 1 , i--){
    if( a%i == 0 & b%i == 0)
        return i;
    }
}
```

$Tc \rightarrow O(\min(a,b))$

$$\boxed{\text{Cp} \rightarrow \_\_gcd(abs(a), abs(b))}$$ → stl

Euclid's Algo

$$gcd(a, b) = g$$

$$a = \lambda_1 g$$

$$b = \lambda_2 g$$

$$b-a = d_2 g - d_1 g$$

$$= g(d_2 - d_1) = g d_3$$

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

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

$$= \gcd(a, b-3a)$$

$$b - \left\lfloor \frac{b}{a} \right\rfloor \times a = b \% a$$

$$= \gcd(a, b - na)$$

$$(b \% a)$$

$$b - na \geq 0$$

$$n \leq \left\lfloor \frac{b}{a} \right\rfloor$$

$b = 11$

$a = 2$

$$11 - n \times 2 \geq 0$$

$$\Rightarrow \boxed{n \leq 5}$$

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

$$\boxed{\gcd(a, b) = \gcd(b \% a, a)}$$

$$\boxed{gcd(0, b) = b}$$

Code →

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

$$\boxed{TC \rightarrow \log_{\phi} \min(a, b) \qquad \phi \rightarrow \underline{1.14}}$$

Eg:

$$gcd(100, 24) = gcd(24, 100)$$

$$= gcd(4, 24)$$

$$= gcd(0, 4) \leftarrow$$

$$= 4$$

Eg:

$$\gcd(\overset{a}{7}, \overset{b}{11}) = \gcd(\overset{a}{4}, \overset{b}{7})$$
$$= \gcd(3, 4)$$
$$= \gcd(1, 3)$$
$$= \gcd(0, 1)$$
$$= 1$$

LCM → Lowest common multiple

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

$$a = d_1 g$$

$$b = d_2 g$$

$$\boxed{\mathrm{LCM}(a,b) = \frac{a \times b}{\gcd(a,b)}}$$

$$\mathrm{LCM}(a,b) = \frac{d_1 \cancel{g} \times d_2 g}{\cancel{g}}$$

$$= d_1 d_2 g$$

$$\Rightarrow \boxed{LCM(a,b) = \frac{a \times b}{gcd(a,b)}}$$

Extended Euclid's Algo:

$$ax + by = \gcd(a, b)$$

$$\gcd(b \% a, a) = (b \% a)x_1 + ay_1$$

$$\boxed{b \% a = b - \left\lfloor \frac{b}{a} \right\rfloor \times a}$$

$$\gcd(b\%a, a) = \left(b - \left\lfloor \frac{b}{a} \right\rfloor \times a\right) x_1 + a y_1$$

$$\gcd(b\%a, a) = a\left(y_1 - \left\lfloor \frac{b}{a} \right\rfloor x_1\right) + b x_1$$

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

$$\gcd(a, b) = a\left(y_1 - \left\lfloor \frac{b}{a} \right\rfloor x_1\right) + b x_1$$

$$\boxed{\begin{aligned} x &= y_1 - \left\lfloor \frac{b}{a} \right\rfloor x_1 \\ y &= x_1 \end{aligned}}$$

$$\boxed{b = ax + by}$$

$$\boxed{\begin{array}{c} x = 0 \\ \hline y = 1 \end{array}}$$

Eg:

$a = 4$ $\quad$ $b = 3$

$$4x + 3y = 1$$

$x = 1$

$y = -1$

$$4 + (-3) = 1$$

$$1 = 1$$

LDE

$$\boxed{ax + by = c}$$

$a, b, c \rightarrow$ Int

$x, y \rightarrow$ Integral value?

Eg.

$4x + 6y = 28$

$$\boxed{\begin{aligned} x &= 1 \\ y &= 4 \end{aligned}}$$

How to check Integer solution exist?

$$ax + by = c$$

$$ax + by = c \times \frac{g}{g}$$

$$a\overbrace{\left(\frac{gx}{c}\right)}^{X} + b\overbrace{\left(\frac{gy}{c}\right)}^{Y} = g$$

$$\boxed{ax + by = g}$$

$c \% g = 0$

<u>cases</u>

$ax + by = c$

if $c \% g != 0$
$\rightarrow$ 0 int sol

if $c \% g = 0$
$\rightarrow$ ∞ int sol^n

$$\boxed{aX + bY = g}$$

Extended Euclid

$$ax + by = c$$

$$\frac{gx}{c} = X \rightarrow \boxed{x = \frac{cX}{g}}$$

x_0

$$\frac{gy}{c} = Y \Rightarrow \boxed{y = \frac{cY}{g}}$$

y_0

$\underline{\infty \text{ solution}}$

$$a x_0 + b y_0 = c$$

$$a\underbrace{\left(x_0 + b/g\right)}_{x} + b\underbrace{\left(y_0 - a/g\right)}_{y} = c$$

$$\boxed{\begin{aligned} x &= x_0 + (b/g)K \\ y &= y_0 - (a/g)K \end{aligned}}$$

$\rightarrow$ $\underline{\infty \text{ solutions}}$

Binary Expo.

$\boxed{base^x}$

BF → $\boxed{ans = 1}$

```
for(int i = 0; i < x; i++)

      ans = ans * base;
}
return ans;
```

TC → O(x)

ans

$$x \to x-1$$

$$ans = ans \times base$$

$x \to$ odd $\to$

$x \to$ even $\to (base)^{\frac{x \times 2}{2}}$

$\to (base^2)^{x/2}$

```
while (x > 0) {
    if (x % 2 == 0) {
        base = base x base;
        x = x/2;
    } else {
        x = x - 1;
        ans = ans x base;
```

}

}

return ans;

128

dry run

base = 16

x = 0

ans = 8x16

128

$$\boxed{TC \rightarrow \log_2(x)}$$

Modular arithmatic

factorial

↳ $1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9$

$\times 10$

$\times 11$

10^{18}

limit → 0 to 9

$\boxed{fact(4)}$ → $1 \times 2 \times 3 \times 4$ →

1×2 → 2×3 → $(6 \times 4) \% 10$

$24 \% 10 \rightarrow 4$

0 to ____

fact(100) →

output

correct output

[0 to mod − 1]

$a+b$	$a-b$	$a \times b$	$a \div b$
$(a \% \text{ mod} + b \% \text{ mod}) \% \text{ mod}$			
$a+b+c$			

$$((a \% m + b \% m) \% m + c \% m) \% m$$

$1e^9 + 7$

$\boxed{\%mod}$

$\boxed{0 \text{ to } 1e^9 + 6}$

large enough

prime

multiplication

$a \times b \rightarrow (a \% \text{mod} \times b \% \text{mod}) \% \text{mod}$

$a \times b \times c \rightarrow ((a \% \text{mod} \times b \% \text{mod}) \% \text{mod} \times c \% \text{mod}) \% \text{mod}$

division

multiplicative inver of number

$$\text{number} \times x = 1$$

number $= 5$ $\quad x = 1/5$

number $= 1$ $\quad x = 1$

a $\quad$ $x \to$ mult. inverse

$\downarrow$

number

$$(ax) \% \text{mod} = 1$$

$$ax = \text{mod}\, xy + 1$$

$$\boxed{a\underline{x} - \text{mod}\, x\underline{y} = 1} \to \text{LDE}$$

$$\boxed{\gcd(a, mod) = 1}$$

$$\boxed{\text{prime}}$$

Fermat little theorem

$a^p - a$ is an integer multi. of p ($p \to$ prime and $a \to$ any number)

$(a^p - a) \% p = 0$

$(a^p) \% \text{mod} = (a) \% \text{mod}$

$$(a^{-1}) \% p \approx (a^{p-2}) \% p$$

$$(a \times b^{-1}) \% \, mod$$

$$(a^{mod-2}) \% \, mod \approx (a^{-1}) \% \, mod$$

$$(a \% \, mod \times (b^{mod-2}) \% \, mod) \% \, mod$$

$$\left(\frac{a}{b \times c}\right) \% \, mod$$

$$\rightarrow \left(a \times b^{-1} \times c^{-1}\right) \% \, mod$$

$$\left(\left(a \% \, mod \times \left(b^{mod-2}\right) \% \, mod\right) \% \, mod \times \left(c^{mod-2}\right) \% \, mod\right)$$

$\% \, mod$

$$\frac{a \times b}{c \times d} \rightarrow \left[a \times b \times c^{mod-2} \times d^{mod-2} \right]$$

[4 mods for the number] and [3 more mod after each multi]