



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

$$\text{gcd}(5, 15) \rightarrow 5$$

$$\text{gcd}(-5, 5) \rightarrow 5$$

$$\text{gcd}(0, 7) \rightarrow 7$$

$$\text{gcd}(-5, -10) \rightarrow 5$$

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

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

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

$$Cp \rightarrow \text{--gcd}(\text{abs}(a), \text{abs}(b))$$

→ stl

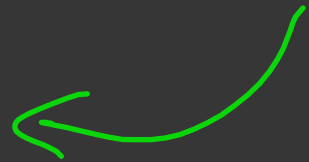
Euclid's Algo

$$\text{gcd}(a, b) = g$$

$$a = r_1 g$$

$$b = r_2 g$$

$$\begin{aligned}\underline{b-a} &= r_2 q - r_1 q \\ &= q (r_2 - r_1) = \underline{q r_3}\end{aligned}$$



$$\begin{aligned}\gcd(a, b) &= \gcd(a, b-a) \\ &= \gcd(a, b-2a) \\ &= \gcd(a, b-3a)\end{aligned}$$

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

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

$$(b - na) \geq 0$$

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

$$\begin{array}{r} b = 11 \\ \hline a = 2 \\ \hline \end{array}$$

$$(b' \gamma a)$$

$$11 - nx \geq 0$$

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

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

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

$$T_c \rightarrow \log_{\phi} \min(a, b)$$

$$\rightarrow \underline{\underline{1.14}}$$

~~Eg.~~ $\gcd(100, 24) = \gcd(24, 100)$
 $= \gcd(4, 24)$
 $= \gcd(0, 4) \leftarrow$
 $= 4$

eg:

$$\begin{aligned}\gcd(7, 11) &= \gcd(\overset{a}{4}, \overset{b}{7}) \\ &= \gcd(3, 4) \\ &= \gcd(1, 3) \\ &= \gcd(0, 1) \\ &= \textcircled{1}\end{aligned}$$

(#) LCM \rightarrow Lowest common multiple

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

$$a = d_1 g$$

$$b = d_2 g$$

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

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

$$= d_1 d_2 g$$

\Rightarrow

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

⑧ Extended Euclid's Algo.

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

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

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

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

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

↗

$$\gcd(a, b) = \overbrace{a x_1 + b y_1}^{b x_1 + b y_1}$$

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

$$x = y_1 - \left\lfloor \frac{b}{a} \right\rfloor x_1$$

$$y = x_1$$

$$b \equiv ax + by$$

$$\frac{x=0}{y=1}$$

Eg:

$$\underline{a=4}$$

$$\underline{b=-3}$$

$$4x + 3y = 1$$

$$\begin{array}{l} \underline{x=1} \\ y=-1 \end{array} \rightarrow$$

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

$$\underline{1 = 1}$$

How to check Integer solution exist?

$$ax + by = c$$

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

$$a \overset{x}{\left(\frac{gx}{c} \right)} + b \overset{y}{\left(\frac{gy}{c} \right)} = g$$

$$ax + by = g$$

$$cyg \geq 0$$

cases

$$ax + by = c$$

if $cy \cdot g \neq 0$
 $\rightarrow 0$ int sol

if $cy \cdot g = 0$
 $\rightarrow \infty$ int sol

$$ax + by = g$$

extended
Euclid

$$\frac{gx}{c} = x \rightarrow$$

$$x = \frac{cx}{g}$$

$$ax + by = c$$

$$\frac{gy}{c} = y \Rightarrow$$

$$y = \frac{cy}{g}$$

y_0

∞ solutions

$$ax_0 + by_0 = c$$

$$\underbrace{a(x_0 + b/g)}_x + \underbrace{b(y_0 - a/g)}_y = c$$

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

$\rightarrow \infty$ solutions

⑧ Binary Expo.

base^x

BF \rightarrow $\text{ans} = 1$

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

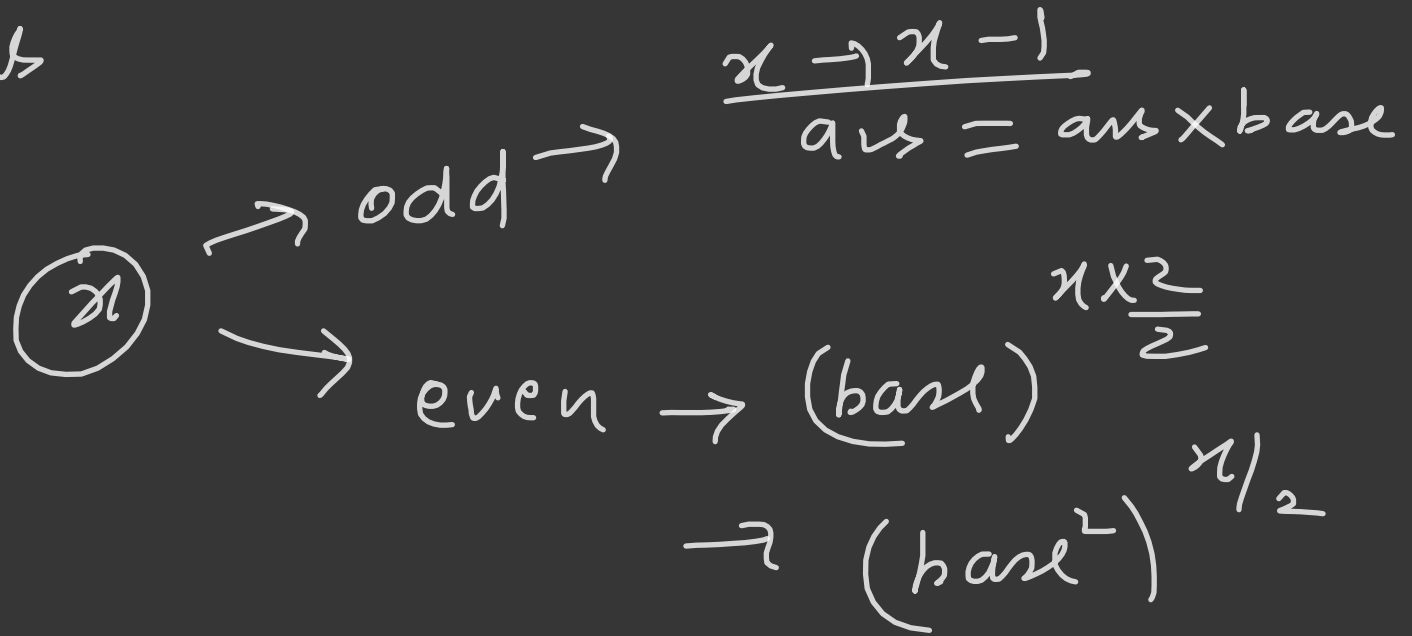
$\text{ans} = \text{ans} \times \text{base};$

↵

return ans;

TC $\rightarrow O(x)$

ans



```
while (x > 0) {
```

```
    if (x % 2 == 0) {
```

```
        base = base * base ;
```

```
        x = x / 2 ;
```

```
    } else {
```

```
        x = x - 1 ;
```

```
        ans = ans * base ;
```

```
}  
}  
return ans,
```

128

dry
run

base = 16

$x = 0$

$ans = 8 \times 16$

→ 128

$$Tc \rightarrow \log_2(x)$$

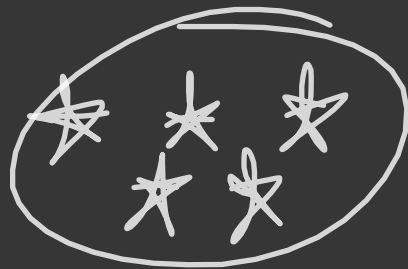
Ⓢ

Modular arithmetic

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 \rightarrow 0 to 9

$$\boxed{\text{fact}(n)} \rightarrow 1 \times 2 \times 3 \times 4 \rightarrow$$

$$(1 \times 2) \rightarrow 2 \times 3 \rightarrow (6 \times 4) \checkmark$$

$$24 \times 10 \rightarrow 4 \quad \swarrow \quad 10$$

fact(100) → 0 to —

output
—
—
—

connect
output
—
—

[0 to mod - 1]

$$a + b$$

$$a - b$$

$$a \times b$$

$$a \div b$$

$$(a \div m + b \div m) \div m$$

$$a + b + c$$

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

$$10^9 + 7$$

$$\% \text{mod}$$



$$0 \text{ to } 10^9 + 6$$

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 inverse of number

$$\text{number } x \text{ (} x \text{)} = 1$$

$$\text{number} = 5 \quad x = 1/5$$

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

a
↓
number

$x \rightarrow$ mult. inverse

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

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

$$\boxed{a\underline{x} - \text{mod } x\underline{y} = 1} \rightarrow \text{LDF}$$

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

prime

Fermat
little
theorem

→ $a^p - a$ is an integer multi.

of p ($p \rightarrow$ prime and $a \rightarrow$ any number)

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

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

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

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

$$\frac{(a \% \text{mod})}{\approx (a^{-1}) \% \text{mod}}$$

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

