GCD, LCM, Linear Diophantine Equations, Fibonacci Numbers

Course on Number Theory and Maths

Raja vikramaditya Panda • Lesson 1 • Aug 22, 2021

(Euclid)

GCD / LCM / Extended Euclid

Fibonacci, Binary Expo -
(Matrix Expo)

- Striver

22/08/21

GCD

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

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

greatest common divisor

$$\gcd(0, 5) = 5$$

$\frac{-5}{5}$ $\frac{5}{5}$

$\frac{0}{5}$ $\frac{5}{5}$

Brute Force

greatest

gcd (a, b)

a = 7 , b = 11

(1, 7)

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

TC → O(min (a, b))

__gcd(abs(a), abs(b))

CPP:

$\boxed{CP \rightarrow \_\_gcd(a, b)}$

{ negative numbers }

Euclid's Algorithm

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

$b \% g$

g

$\boxed{\begin{array}{l} a \% g == 0 \\ b \% g == 0 \end{array}}$

num

$15 - 5 = 10$

$\% 5$ $\% 5$

$gcd = 2$ $(4, 6)$

$(6 - 4) = 2$

$\boxed{a \% g == 0}$

$\left(\frac{a}{g}\right) - \left(\frac{b}{g}\right)$

$\% g$

$\frac{(a-b)}{g}$

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

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

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

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

$$\vdots$$

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

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

$$\boxed{\begin{array}{l}\gcd(10, 20) \\ \downarrow \\ \gcd(20, 10)\end{array}}$$

(Swap will Happen)

$\boxed{gcd(0, num) = num}$ → Base Case

$gcd(24, 100) \rightarrow gcd(100, \overset{24}{\underline{24 \% 100}})$

$gcd(100, 24)$

↓

$gcd(24, 4)$

↓

$gcd(4, 0)$

↓ swap

$gcd(0, 4)$

$$
\begin{tikzcd}
\gcd(13, 17) \arrow[r] & \gcd(17, 13) \arrow[d] \arrow[dl] & \\
1 & \gcd(13, 4) \arrow[d] \arrow[r] & 1 \\
 & \gcd(4, 1) \arrow[d] \arrow[r] & 1 \\
 & \gcd(1, 0) \arrow[d] \arrow[r] & 1 \\
 & \gcd(0, 1) \arrow[r] & 1
\end{tikzcd}
$$

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

    return gcd(b, a % b);

}
```

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

$\phi \rightarrow 1.14$

habit $\rightarrow$ $\boxed{abs(a), abs(b)}$

LCM → a = 3, b = 4   LCM = 12

3, 6, 9, 12, 15, 18, 24

4, 8, 12, 16, 24

$\boxed{LCM = 12}$

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

$\boxed{\log_\phi mn(a,b)}$

24 = 3 × 4 × 2

24 = 4 × 3 × 2

$\rightarrow$ LDE ?

Extended Euclidean Algorithm $\times\times\times$

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

$a = 2, \quad b = 3$

$ax + by = gcd$

$2x + 3y = 1$

$\boxed{2 \times 2 + 3 \times -1 = 1}$

LDR

$$ax_0 + by_0 = g \cdot \times \frac{n}{g}$$

$$a\left(\frac{x_0 \times n}{g}\right) + \left(\frac{by_0 n}{g}\right) = n$$

$$x_1 = \frac{x_0 n}{g}$$

$$y_1 = \frac{y_0 n}{g}$$

$$ax + by = n$$

$$\Rightarrow \boxed{a\underline{x} + \underline{by} = \underline{\gcd(a,b)}}$$

$x = ?$
$y = ?$

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

→ Extended Euclidean

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

→ valid?

$b = 10$
$a = 7$

$$10 - \left\lfloor \frac{10}{7} \right\rfloor \times 7$$

$$10 - 1 \times 7 = 3$$

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

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

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

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

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

$$g = ax + by$$

$$\downarrow$$

$$g = eq_1 \quad x_1 \quad y_1$$

$$\boxed{a=0 \qquad b=1} \rightarrow \underline{gcd = b}$$

$$\underset{b}{gcd(\quad)} = \underbrace{\boxed{\cancel{a}x + \cancel{b}y}}_{0\,\boxed{x=0}\quad b\,\boxed{y=1}}$$

$gcd(a,b) = ax + by$ $\quad x \rightarrow x1 \quad y \rightarrow y1$

$gcd(b\%a, a) = eq1$

$gcd(\;) = eq2$

$gcd() = eq3$

$b = (ax + by)$ $\boxed{x=0,\ y=1}$ $\boxed{x_n = 0 \quad y_n = 1}$

only 1

LDE

$$ax + by = c$$

eq 1 $(x\ y)$

eq 1 $(x_1\ y_1)$

eq 2 $(x_2\ y_2)$

eq 3 $(x_3\ y_3)$

eq 4 $(x_4 = 0\ \ y_4 = 1)$

$x = ?\quad y = ?$
$gcd(12, 20, x, y)$

```
int gcd(a, b, *x, *y)
{
    if (a == 0)
    {
        x = 0;
        y = 1;
        return b;
    }
    x1, y1
    ~~return~~ g = gcd(b % a, a, &x1, &y1)
        x = y1 - [b/a] * x1
        y = x1
    return g;
}
```

$eq_1(x, y)$

$eq_2(x_1, y_1)$

$eq_3(x_2 y_2)$

$eq_4(x_3 y_3)$

→ Even ↑+a (x)
→ Dec ↓+b (y)
→ Can you reach N

LDE

$$ax + by = N$$

Fibonacci (Medium Expo)

0 1 1 2 3 5 8 13 21 34 ....

$f[0] = 0$, $f[1] = 1$

```
for ( i=2 ; i<=n ; i++)
    { f[i] = f[i-1] + f[i-2];
    }
```

$\boxed{\text{Complexity} \rightarrow O(N)}$

213 → 1e9

$O(\log N) \rightarrow$ Matrix Expo

$$f(n) = f(n-1) + f(n-2)$$

Power Exponentiation / Binary Exponentiation

base = 10 , $n = 3$

ans = 10^3

ans = 1

for (i = 1 ; i <= 3 ; i++)

ans = ans × i ;

$\Rightarrow O(n)$

$\downarrow$

$O(\log_2 n)$

$(base)^{n}$ $\rightarrow$ n is even: $(base \times base)^{n/2}$ | n is odd: $(base) \times base^{n-1}$

$$\boxed{ans = 1 \times 9 \times 6561}$$

$3^{10} \rightarrow (3 \times 3)^{5} = 9^{5}$ (base = 9, n = 5)

$9^{5} \rightarrow 9^{4}$ (base = 9, n = 4)

$9^{4} \rightarrow (9 \times 9)^{2} = (81^{2})$ (base = 81, n = 2)

$81^{2} \rightarrow (81 \times 81)^{1} = (6561)^{1}$ (base = 6561, n = 1)

$6561^1 \rightarrow (6561)^0 \rightarrow 1 \quad \times$

$/2 \quad /2 \quad /2 \quad n^{-1}$

$O(\log_2 n)$

```
power(base, n)
{
  int ans = 1;
  while (n != 0)
  {
      if (n % 2 == 0)
          base = base * base;
          n = n/2;
      else
          ans = ans * base;
          n = n-1;
  }
```

STL

pow(x, y)

```
return ans;
}

int power(base, n)
{
  if (n==0) return 1;
  if (n%2==0) return power(base×base, n/2);
  else return base × power(base, n-1);

}
```

Codeforces

Concepts

↳ Emp

3 problem

Slow

Specialist

1400 | 1500

→ CR

→ CP

3 problem

Super fast

1700–1800

$$f(n) = f(n-1) + f(n-2)$$

$$f(n) = \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} f(n-1) \\ f(n-2) \end{bmatrix}$$

$$\begin{bmatrix} f(n) \\ f(n-1) \end{bmatrix} = \underset{(2\times 2)}{\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}} \underset{[2\times 1]}{\begin{bmatrix} f(n-1) \\ f(n-2) \end{bmatrix}}$$

$n=2$

$$\begin{matrix} f(2) \\ f(1) \end{matrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} f(1) \\ f(0) \end{bmatrix} \text{ — } 1$$

$$n=3 \quad \begin{bmatrix} f(3) \\ f(2) \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} f(2) \\ f(1) \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^2 \begin{bmatrix} f(1) \\ f(0) \end{bmatrix} \text{ --- } 3$$

$n = 4$

$$\begin{matrix} f(4) \\ f(3) \end{matrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} f(3) \\ f(2) \end{bmatrix}$$

$$\begin{bmatrix} f(4) \\ f(3) \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^3 \begin{pmatrix} f(1) \\ f(0) \end{pmatrix} \text{ --- } 4$$

$$\begin{bmatrix} f(n) \\ f(n-1) \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{n-1}} \begin{bmatrix} f(1) \\ f(0) \end{bmatrix}$$

$$\begin{bmatrix} f(n) \\ f(n-1) \end{bmatrix} = \begin{bmatrix} x & y \\ w & z \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} f(n) \\ f(n-1) \end{bmatrix} = \begin{bmatrix} x \\ w \end{bmatrix}$$

$$\boxed{f(n) = x}$$

$$\boxed{f(n) = \text{ans}[0][0]}$$

$$f(n) = \text{power}\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, n-1\right)[0][0]$$

$(\text{base} \times \text{base})$

$n = n/2$

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

$n = n-1$

ans = 1

n % 2 == 0
base = base × base

n = n/2

n % 2 == 0
ans = ans × base

n = n − 1

Binary Expo

$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \rightarrow$ ans [2][2] = [{1,0},{0,1}]

$\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix} \leftarrow$ base [2][2] = {{1,1},{1,0}}

```
while(n>0)
{
   if(n%2==0)
   {
     multiply(base, base)
       n=n/2;

   }
   else multiply(ans, base);
       n=n-1;
}
```

```
return ans[0][0];

}

multiply(int mat1[2][2], int mat2[2][2])
{
  res[2][2];

res[0][0] =
res[0][1] =

res[1][0] =

res[1][1] =

mat[0][0] = res[0][0], mat[0][1] = res[0][0]
      mat[1][0] = res[1][0],   mat[1][1] = res[0][0].
   mat[1][0]
```

Remove

}

$$mat1 \begin{bmatrix} 00 & 01 \\ 10 & 11 \end{bmatrix} \qquad mat2 \begin{bmatrix} 00 & 01 \\ 10 & 11 \end{bmatrix}$$

$$\underline{res[0][0]} = mat1[0][0] \times mat2[0][0]$$
$$+ \ mat[0][1] \times mat2[1][0] \ ;$$

(Q) Sum of first N fibonacci Number ...

$\boxed{3:39}$

```
for(i=0; i<=n; i++)
{
    Sum = Sum + f[n];
}
```

$O(n)$

$f(n)$ 0 1 1 2 3 5 8 13 21

$s(f(n)) \to$ 0 1 2 4 7 12 20

$$\boxed{s(f(n)) = f(n+2) - 1}$$

$\boxed{O(\log_2 n)}$

Matrix Expo

AMA

(2 questions of Medium) ←

Patterns for 3 months

→ Sat / Sun → on some same day

2 hours Class

4,

Testing → Codeleave

Stress Testing

TC

Mon - Friday

Do 2-3 Problems

Daily (Mon-Fri)

10-12

~~Codeforces~~ "(Binary Search" Pr)

~~Codechef~~

~~Hash~~

Completely

BS → SDE

3 days → CF / CC / HE

Practice

Every Contest at CF → Grind

After Contest → Use whatsapp Group to discuss

3 problems

(Speed, Accuracy, Facing Unknown

→ Help you in Clear CR

6|7

Ctd / Jaue

Referral