Factors, Prime Factorization

Sieve, Smallest Prime Factor,

No. of factors, Sum of factors, Modulor Arithmetic

Advanced Number Theory 2

Binary Exponentiation

- ✔ Euclidean Algorithm → GCD of 2 numbers (A, B)
- ✔ GCD Properties
- ✔ Euler's Totient Function
- ✔ Euler's Theorem
- ✔ Fermat's Theorem
- ✔ Mod Inverse under Euler's & Fermat's Theorem

Bonus Concepts

GCD → Greatest common divisor

(A, B)

$\downarrow$

$\max(\mathrm{sqrt}(A, B))$ — $O(\mathrm{sqrt}(A) + \mathrm{sqrt}(B))$

A $\rightarrow$ all factors

B $\rightarrow$ all factors

$\}$ which is the biggest common factor

Euclidean Algorithm: Link

log(min(a,b))

Theorem: $\gcd(a,b) = \begin{cases} a, & \text{if } b = 0 \\ \gcd(b, a \bmod b), & \text{otherwise.} \end{cases}$

Implementation: gcd(5,10) → gcd(10,5)

Recursive

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

Iterative

```
int gcd (int a, int b) {
    while (b) {
        a %= b;
        swap(a, b);
    }
    return a;
}
```

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

$$\gcd(a, d) = \gcd(a, b + ka)$$

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

$$\boxed{a > b}$$

$$\gcd(a, b) \rightarrow \underline{\underline{x}}$$

x divides a, x divides b

if ('')

$\rightarrow$ x divides $a + b$

$\rightarrow$ x divides $a-b$

$\rightarrow$ x divides $a \times b$

if x divides $\underline{\underline{a}}$ if x divides b

$a \rightarrow x \cdot y$ $b \rightarrow x \cdot z$

$(a+b) \rightarrow x\,\underbrace{(y+z)}$

$(a-b) \rightarrow x\,\underbrace{(y-z)}$

$\gcd(a, b) \longrightarrow x$

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

$(a, b) \longrightarrow \boxed{x}$

$(a-b, b) \longrightarrow$

$(6, 16) \longrightarrow \underline{\underline{2}}$

$(6, 10) \longrightarrow 2$

$(6, 4) \longrightarrow 2$

$(2, 4) \longrightarrow 2$

$(2, 2) \longrightarrow 2$

$(0, 2) \longrightarrow 2$

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

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

GCD = Greatest common divisor

$(10, -5)$

$(-5, -5)$

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

$$\begin{array}{ccc} \downarrow & & \downarrow \quad \downarrow \\ x & & x \quad x \end{array}$$

$$\left.\begin{array}{l} b \to yx \\ a \to zx \end{array}\right\} \quad \underline{\underline{x(y-kz)}}$$

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

$$\begin{array}{ccc} \downarrow & & \downarrow \quad \downarrow \quad \downarrow \\ x & & x \quad a \quad x \end{array}$$

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

$gcd(5, 9)$

$\boxed{a < b}$

b

13

2

$a < b$

$$\boxed{b - \left(\frac{b}{a}\right) \cdot a} \longrightarrow b \bmod a$$

$$\gcd(12, 30)$$

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

$$\gcd(12, 30) = \gcd(30, 12)$$

$$\gcd(30, 12) = \gcd(12, 6)$$

$$\gcd(12, 6) \rightarrow \underline{\underline{\gcd(6, 0)}}$$

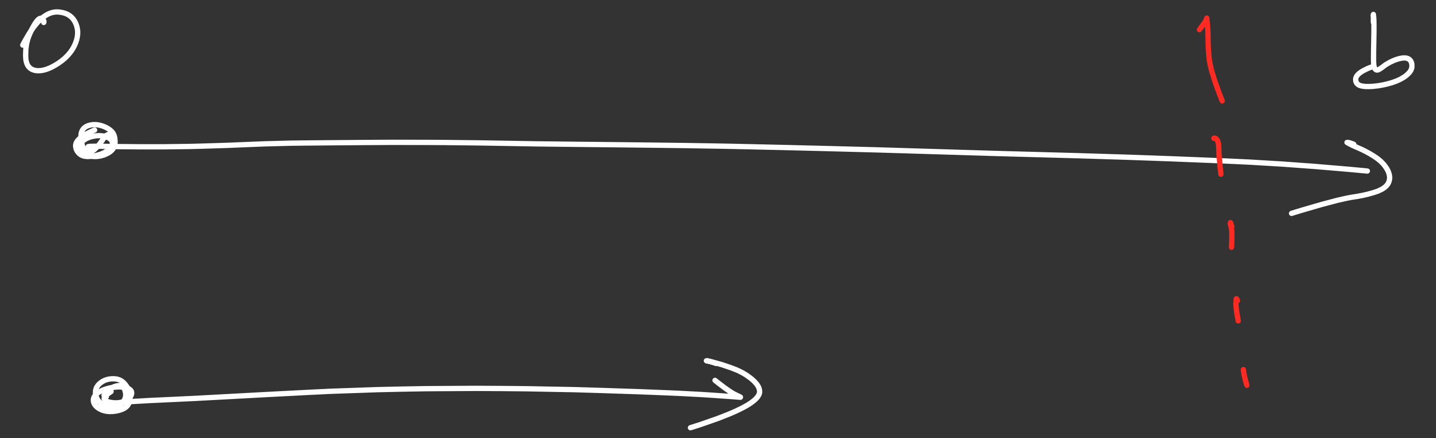
$$\boxed{\gcd(a, b)} \qquad \underline{a > b}$$

$$\downarrow$$

1

$$\gcd(b, \underbrace{a \bmod b}_{})$$

$\underline{0 \text{ to } b-1}$



$\boxed{a \bmod b} \le c$

$$\gcd(b, \underbrace{a \bmod b}_{c}) \longrightarrow \gcd(c, b \bmod c)$$

2

One of these is bound to be smaller than $b/2$

b

c

$c < b/2$

if $c > b/2$

then

$b \bmod c$

$< b/2$

$\underline{b, c}$

$0 \le c \le b-1$

either $c < b/2$ ✓

or $b \bmod c < b/2$

$$2 \cdot \log(\min(a, b))$$

$$\downarrow$$

$$O(\log(\min(a, b)))$$

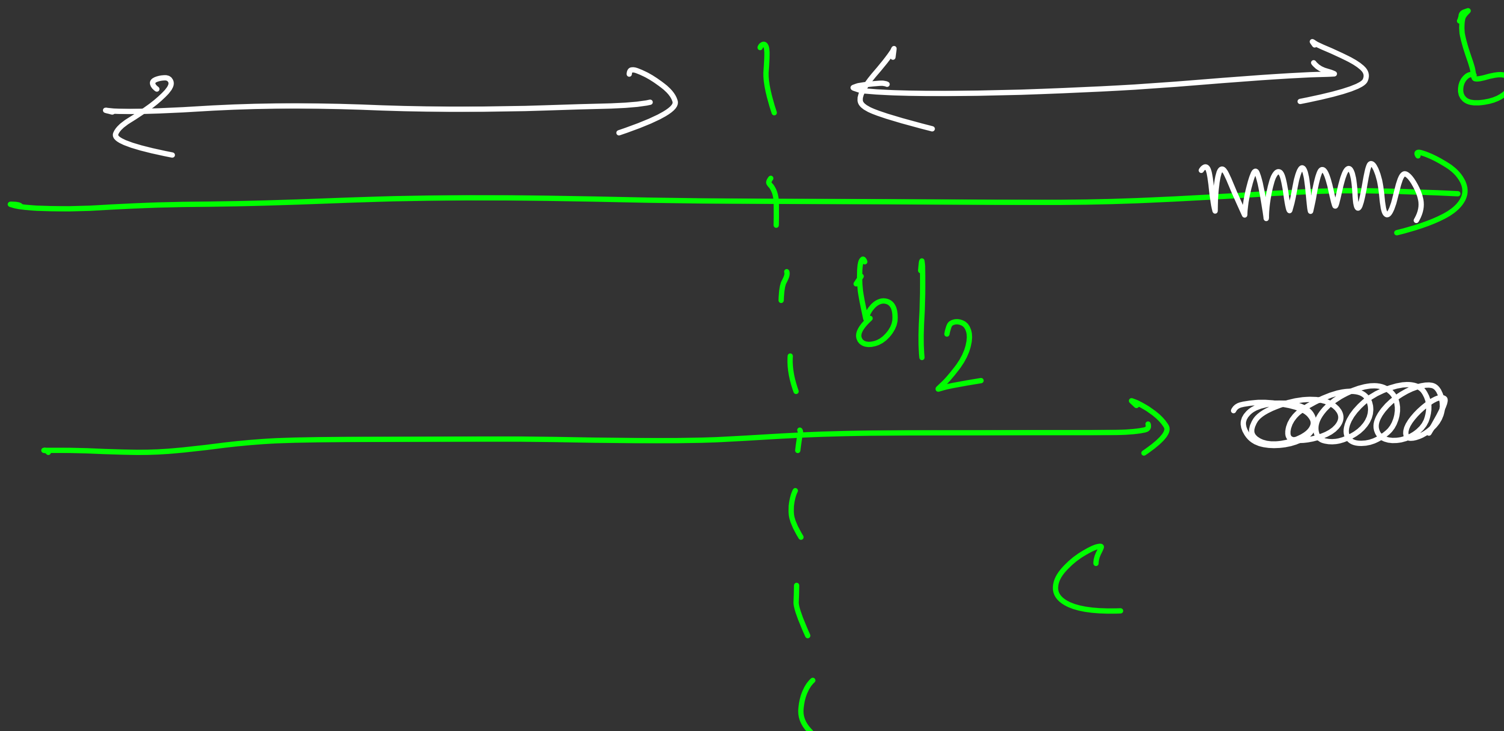
$(3, 5)$

$\downarrow \quad \downarrow$

$c \quad b$

$b \bmod c$

$>$



Important GCD results

$gcd(2,4,6,8) \rightarrow 2$

$$\frac{gcd(2,4,6,8)}{gcd(2,4)} \neq gcd(6,8)$$

- GCD(a, b) = GCD(b, a)
- GCD(a, 0) = a
- GCD(a, b, c) = GCD(GCD(a, b), c) = GCD(a, GCD(b, c)) = GCD(b, GCD(a, c))
- GCD(a, b) >= GCD(a, b, c) >= GCD(a, b, c, d)
- GCD contains the minimum powers of primes ①
- LCM contains the maximum powers of primes ②
- GCD(a, b) * LCM(a, b) = a * b ③

$gcd(a,b) \rightarrow x$

$gcd(a,b,c) \rightarrow y$

$y \leq x$

12	24	18	9	6	1

12 12 6 3 3 1

Find out no. of subarray with

GCD $\geq k$

find out biggest cf of

1 ______ a and b

2 find out biggest cf of a, b, c

$$\gcd(a, b)$$

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdots p_m^{k_m}$$

$$b = p_1^{l_1} \cdot p_2^{l_2} \cdot p_3^{l_3} \cdots p_m^{l_m}$$

$$\gcd(a, b) = p_1^{\min(l_1, k_1)} \, p_2^{\min(l_2, k_2)} \cdots p_m^{\min(l_m, k_m)}$$

$$a = 36 = 2^2 \cdot 3^2$$

$$b = 50 = 2^1 \cdot 5^2$$

$$a = 2^2 \cdot 3^2 \cdot 5^0$$

$$b = 2^1 \cdot 3^0 \cdot 5^2$$

$$\gcd = 2^1 \cdot 3^0 \cdot 5^0 = \underline{\underline{2}}$$

$$\operatorname{lcm}(18, 12) = 36$$

$$18 \rightarrow 2 \cdot 3^2$$

$$12 \rightarrow 2^2 \cdot 3^1$$

$$\operatorname{lcm} \rightarrow 2^{\max(2,1)} \cdot 3^{\max(2,1)}$$

$$\rightarrow 2^2 \cdot 3^2 = \underline{\underline{36}}$$

Euler's Totient Function: Link to study further

phi(N) = number of values X such that X <= N and gcd(X, N) = 1

phi(N) is a multiplicative function.

Properties

The following properties of Euler totient function are sufficient to calculate it for any number:

- If p is a prime number, then $\gcd(p, q) = 1$ for all $1 \le q < p$. Therefore we have:

$$\phi(p) = p - 1.$$

- If p is a prime number and $k \ge 1$, then there are exactly p^k/p numbers between 1 and p^k that are divisible by p. Which gives us:

$$\phi(p^k) = p^k - p^{k-1}.$$

- If a and b are relatively prime, then:

$$\phi(ab) = \phi(a) \cdot \phi(b).$$

Euler's Totient Function

N

how many numbers from 1 to N are such that

$\gcd(x, N) = 1$

$$\phi(n) = \sum_{x=1}^{n} (1) \quad \text{such that} \quad \gcd(x, n) = 1$$

$\boxed{6} \to 1, 2, 3, 4, 5, 6$

✓ ✓

$\boxed{7} \to 1, 2, 3, 4, 5, 6, 7$

✓ ✓ ✓ ✓ ✓ ✓

$\boxed{8} \to 1, 2, 3, 4, 5, 6, 7, 8$

✓ ✓ ✓ ✓

$$\phi(p) = p-1$$

p is not divisible by any no other than 1 and p

$$\phi(2) = 1$$

$$\phi(3) = 2 \qquad \phi(5) = 4 \qquad \phi(7) = 6$$

$$\phi(11) = 10$$

$\phi(p^k)$

p is prime

k is normal positive integer

$\phi(2^4)$

✓	✗	✓	✗	✓	✗	✓	✗
1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
✓	✗	✓	✗	✓	✗	✓	✗

$$(p^k, \; p \cdot x) \geq p$$

$$(p^k, \; \underline{y}) \longrightarrow 1$$

$$a = p_1^{k_1},\ p_2^{k_2} \ \text{-----}\ p_m^{k_m}$$

$$b = p_1^{l_1},\ p_2^{l_2} \ \text{-----}\ p_m^{l_m}$$

$$\gcd \rightarrow p_1^{\min(l_1,\ k_1)} \ \text{-----}\ p_m^{\min(l_m,\ k_m)}$$

$$\begin{cases} p^k \rightarrow p^k \quad p_1^0 \quad p_2^0 \ \text{----}\ p_m^0 \\ x \rightarrow p^y \quad p_1^{a_1} \quad p_2^{a_2} \ \text{----}\ p_m^{a_m} \end{cases}$$

$$\gcd \rightarrow y = 0$$

$3^3 \rightarrow$ 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

$27 - 9$

$=$

$$\phi(p) = p-1$$

$$\phi(p^k) = \boxed{p^k - \frac{p^k}{p}}$$

$$= p^k\left(1-\frac{1}{p}\right)$$

$$= p^k - p^{k-1}$$

$\phi(n) \longrightarrow$ multiplicative function

$$f(a \times b) = f(a) \cdot f(b)$$

provided $\gcd(a, b) > 1$

No. of divisors of N

$$N = p_1^{k_1} \, p_2^{k_2} \cdots p_m^{k_m}$$

$$\underline{(k_1+1)}\,\underline{(k_2+1)} \cdots \underline{(k_m+1)}$$

$$N = 2^2 \cdot 3^4$$

$$(2+1) \cdot (4+1)$$

$$f(N) = f(2^2 \cdot 3^4)$$

$$\Downarrow$$

$$\underline{f(2^2)} \cdot f(3^4)$$

$$(2+1) \cdot (4+1)$$

$N \longrightarrow \left(p_1^{k_1}\right) \cdot \left(p_2^{k_2}\right)$

Sum of divisors of N

$N = p_1^{k_1} \; p_2^{k_2} \; \cdots \; p_m^{k_m}$

$(p_1^0 + p_1^1 \cdots p_1^{k_1})(p_2^0 + p_2^1 \cdots) \cdots (p_m^0 \cdots p_m^{k_m})$

$\dfrac{(p_1^{k_1+1} - 1)}{(p_1 - 1)} \cdot \left(\dfrac{p_2^{k_2+1} - 1}{p_2 - 1}\right) \cdots$

No. of divisors of $A \times B$

A $\quad$ B $\quad$ $\gcd(A, B) \Rightarrow 1$

$\downarrow$ $\quad$ $\downarrow$

x $\quad$ y $\quad$ $x \cdot y$

Multiplicative function:

$$f(A \cdot B) = f(A) \cdot f(B)$$

such that $\gcd(A, B) = 1$

Completely multiplicative function

$$f(A \cdot B) = f(A) \cdot f(B)$$

$$\phi(N) = \phi(p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m})$$

$$\phi(p_1^{k_1}) \cdot \phi(p_2^{k_2}) \cdots \phi(p_m^{k_m})$$

$$\left(p_1^{k_1} - \frac{p_1^{k_1}}{p_1}\right) \cdot \left(p_2^{k_2} - \frac{p_2^{k_2}}{p_2}\right) \cdots \left(p_m^{k_m} - \frac{p_m^{k_m}}{p_m}\right)$$

$$p_1^{k_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{k_2}\left(1 - \frac{1}{p_2}\right) \cdots p_m^{k_m}\left(1 - \frac{1}{p_m}\right)$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\cdots\left(1-\frac{1}{p_m}\right)$$

Euler's Totient Function:

$n = p_1^{a_1} \, p_2^{a_2} \cdots p_k^{a_k}$

Idea:

$$\boxed{\phi(n) = \phi(p_1{}^{a_1}) \cdot \phi(p_2{}^{a_2}) \cdots \phi(p_k{}^{a_k})}$$

$$= \left(p_1{}^{a_1} - p_1{}^{a_1-1}\right) \cdot \left(p_2{}^{a_2} - p_2{}^{a_2-1}\right) \cdots \left(p_k{}^{a_k} - p_k{}^{a_k-1}\right)$$

$$= p_1^{a_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdot p_2^{a_2} \cdot \left(1 - \frac{1}{p_2}\right) \cdots p_k^{a_k} \cdot \left(1 - \frac{1}{p_k}\right)$$

$$= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

result = n → result = result − result/p

Euler’s Totient Function:

Implementation:

```
int phi(int n) {
    int result = n;
    for (int i = 2; i * i <= n; i++) {
        if (n % i == 0) {
            while (n % i == 0)
                n /= i;
            result -= result / i;
        }
    }
    if (n > 1)
        result -= result / n;
    return result;
}
```

Sqrt(N)

$$\underbrace{n\left(1-\frac{1}{p_1}\right)}_{m}\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_m}\right)$$

result = n

$$\text{result} = \frac{\text{result} - \text{result}}{p} = n$$

$$= n - \frac{n}{p}$$

result = result − result/p_k =

$\underline{\underline{N}} \longrightarrow p_1^{k_1} \; p_2^{k_2} \; ---- \; 8_m^{k_n}$

$\boxed{f(N)} \longrightarrow (\quad)\,(\quad)\,(\quad) \; ---- \; (\quad)$

Euler's Totient Function: 1 to 10^6

Bonus problem:

- Find phi(x) for all numbers from 1 to N. Link

Nice property:

- Divisor sum property. Link

$$\sum_{d \mid n} \phi(d) = N$$

$N = 6$

$(1, 2, 3, 6)$

$\downarrow\ \downarrow\ \downarrow\ \downarrow$

$(1\ 1\ 2\ 2) \longrightarrow 6$

N is divisible P_1 & P_2 P_3

$$N = N - \frac{N}{P_1} \text{ ——— }$$

$$N = N - \frac{N}{P_2} \text{ ——— }$$

$$N = N - \frac{N}{P_3} \text{ ——— }$$

$$N = 2 \cdot 3 \cdot 6 = 36$$

$$N = 36 - \frac{36}{2} = 18$$

$$N = 18 - \frac{18}{3} = 12$$

$$N = 12 - \frac{12}{6} = \boxed{10}$$

$$phi(i) = i$$

```
for (int i = 2 ; i <= n ; i++){
    if ( prime(i))
        phi(i) = i-1

        for(int j = 2i ; j <= n ; j += i)

            phi(j) = phi(j) - phi(j)
                                  i
}
```

Euler's Theorem and Fermat's Theorem: Link

Euler's Theorem $\boxed{a^{\phi(m)} \equiv 1 \pmod{m}}$ if a and m are relatively prime.

Congruency

Fermat's Theorem $a^{m-1} \equiv 1 \pmod{m}$ if m is prime

$(a^{\phi(m)}) \% m = 1$

Practice Problem: Link

(a, m) and

$\gcd(a, m) = 1$

then

$$a^{\phi(m)} \equiv 1 \bmod m$$

$$\left(a^{\phi(m)}\right) \% m = 1$$

$a = 2, \quad m = 5$

$\phi(m) = 4$

$2^4 = 16 \% 5 = 1$

$a = 11, \quad m = 6$

$\phi(6) = \phi(2) \cdot \phi(3)$

$= 1 \cdot 2$

$$\Rightarrow 2$$

$$a^{\phi(6)} = a^2 = 11^2 = \underline{\underline{121}}$$

$$(121)\ \%\ 6 = 1$$

if a and m are relatively prime

$\gcd(a, m) = 1$

$$\left(a^{\phi(m)}\right) \% m = 1$$

$$\left(a^{m-1}\right) \% m = 1 \quad \text{if } m \text{ is prime}$$

$$a^{b^c} \longrightarrow \left(a^{(b^c)}\right) \% \, m$$

$a \rightarrow 10^9$

$b \rightarrow 10^9$ $\qquad$ $m \rightarrow 10^9 + 7$

$c \rightarrow 10^9$

$\gcd(a, m) = 1$

$\gcd(c, m) = 1$

$\gcd(b, m) = 1$

$$a^{m-1} \equiv 1 \mod m$$

$$a^{k\cdot(m-1)} = \left(a^{m-1} \cdot a^{m-1} \cdots a^{m-1}\right)$$

$$= (1 \cdot 1 \cdot 1 \cdots))$$

$$\equiv 1 \mod m$$

$$a^{(b^c)} \quad , \quad a^{k(m-1)} = 1$$

$$\boxed{b^c = x\cdot(m-1) + y}$$

$$a^{x\cdot(m-1)+y} \longrightarrow \boxed{a^{x\cdot(m-1)}} \cdot \underline{a^{y}}$$

$$a^{\boxed{(b^c)}} \longrightarrow \text{too large}$$

$$\downarrow$$

$$a^{\boxed{k\cdot(m-1)}} = 1$$

$$a^{b^c} \% m = \left[a^{\boxed{(b^c \bmod (m-1))}}\right] \% m$$

a^{b^c}

$\gcd(a, m) = 1$, m is prime

$$a^{m-1} \equiv 1 \mod m$$

$$a^{m-1} \cdot a^{m-1} \equiv 1 \mod m$$

$$\boxed{a^{k \cdot (m-1)}} \equiv 1 \mod m$$

$x \; , \; \underline{\underline{y}}$

$$\boxed{x \,\%\, y}$$

$$a^{(b^c)} \% m$$

$\log n$

$$\left[a^{\boxed{(b^c \% (m-1))}} \right] \% m$$

$\log n$ $(\log n + \log n)$

$a^{b^c} \% 14$

$\gcd(14, a) = 1$

$a^{\phi(14)} \equiv 1 \mod 14$

Mod Inverse using Euler's Theorem and Fermat's Theorem:

$$a^{\phi(m)} \equiv 1 \mod m \longrightarrow a^{\phi(m)-1} \equiv a^{-1} \mod m$$

$$a^{m-1} \equiv 1 \mod m \longrightarrow a^{m-2} \equiv a^{-1} \mod m$$

$$(A \mid B) \% m$$

$$= \left[(A \% m) \cdot (B^{-1} \% m) \right] \% m$$

$$\frac{A}{B} = A \times C$$

$$\boxed{C = \frac{1}{B}}$$

$$(C \cdot B) = 1$$

$B \rightarrow$ multiplicative inverse

C

$$C \cdot B = 1$$

$$C = 1/B$$

Multiplicative modulo inverse

$$(A \cdot B) \% m = 1$$

$$B^{m-1} = 1 \mod m$$

$$B^{m-2} \cdot B^{1} = B^{m-1} = 1 \mod m$$

$$\boxed{B^{m-2}} \cdot B^{1} = 1 \mod m$$

multiplicative modulo inverse of

X w.r.t to mod M

$$\boxed{X^{M-2}} \cdot X \equiv 1 \mod M$$

$$\left(\frac{A}{B}\right) \% M = \left((A \% m) \cdot (B^{-1} \% m) \right) \% m$$

$$= \left((A \% m) \cdot (B^{m-2}) \% m \right) \% m$$

A A B B B

$$\left(\frac{5!}{2!\,3!}\right) \% \, m$$

$$\left(\frac{a}{b \cdot c}\right) \% \, m = \left(a \cdot b^{m-2} \cdot c^{m-2}\right) \% \, m$$

multiplicative modulo inverse of a wrt m

$\gcd(a, m) = 1$ and

m is not prime

$$a^{\phi(m)} \equiv 1 \mod m$$

$$\boxed{a^{\phi(m)-1}} \cdot \boxed{a} \equiv 1 \mod m$$

Not so important stuff (Learn on your own)

- Extended Euclidean Algo Link → 1/100
- Linear Diophantine Equations Link → 1/500
- Mod Inverse in O(logM) for general M Link → 1/500
- Chinese Remainder Theorem Link → 1/1000
- Checking for Prime in O(logP) - Miller Rabin Test Link → 1/5000