Number Theory

Bharat Singla

Expert on CodeForces

5 ⭐ on CodeChef

Today’s plan:

- Sieve of Eratosthenes & Prime Factorization using Sieve
- GCD & LCM
- Modular Arithmetic
- Binary / Fast Exponentiation
- Modular Inverse using Fermat’s Little Theorem
- nCr

Sieve of Eratosthenes!

	2	3	4	5	6	7	8	9	10	Prime numbers
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	50	
51	52	53	54	55	56	57	58	59	60	
61	62	63	64	65	66	67	68	69	70	
71	72	73	74	75	76	77	78	79	80	
81	82	83	84	85	86	87	88	89	90	
91	92	93	94	95	96	97	98	99	100	
101	102	103	104	105	106	107	108	109	110	
111	112	113	114	115	116	117	118	119	120	

$TC = O(n \log n)$

Euclid's GCD

$$gcd(a,b) = \max_{k} (k \mid a \ \& \ k \mid b)$$

$$gcd(12,16) = 4$$

$$gcd(a,b) \quad [a > b]$$
$$= gcd(b, a-b)$$

$gcd(16,12) \rightarrow 4$
$= gcd(12,4)$
$= gcd(8,4)$
$= gcd(4,4)$
$= gcd(4,0)$ → Base case

Euclid's GCD

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

$$lcm(a, b) = \frac{a * b}{gcd(a, b)}$$

Modular Arithmetic

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

$$(a-b) \% m = (a \% m - b \% m + m) \% m$$

$$(a * b) \% m = (a \% m * b \% m) \% m$$

Fast Exponentiation

a^b $\quad 3^6 = (3^3 \cdot 3^3) = (3^3)^2$

$3^3 = (3^1)^2 \cdot 3$

$expo(a,b) = expo(a, b/2)^2$

if b is odd: $* b$

Modular Inverse

$(a / b) \% m = (a \% m / b \% m) \% m$ ✗

$a * inv(b) \leftarrow a/b$

mul inverse : $x = \frac{1}{x}$ $\left[x \cdot \frac{1}{x} = 1\right]$

mod mul inverse : $(x \cdot i) \equiv 1 \pmod m$

Fermat's Little Theorem = $x^{m-1} \equiv 1 \pmod m$

$\Rightarrow x^{m-2} \equiv \frac{1}{x} \equiv inv(x)$