Essential Modular Arithmetic & Number Theory Formulas

51. Binary Exponentiation and Basic Modular Arithmetic

- $(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
- $(a - b) \bmod m = ((a \bmod m) - (b \bmod m) + m) \bmod m$
- $(a * b) \bmod m = ((a \bmod m) * (b \bmod m)) \bmod m$
- Binary exponentiation: $a^b \bmod m$ in $O(\log b)$ using squaring.

52. Fermat’s Little Theorem and Modular Inverse

- Fermat: $a^{(p-1)} \equiv 1 \pmod{p}$, if p is prime and $\gcd(a,p)=1$
- Euler: $a^{\phi(m)} \equiv 1 \pmod{m}$, if $\gcd(a,m)=1$
- Inverse: $a^{(-1)} \equiv a^{(p-2)} \pmod{p}$, when p is prime

255. Number of Divisors / Sum of Divisors

- If $n = p_1^{e_1} * p_2^{e_2} * ... * p_k^{e_k}$
- $d(n) = (e_1+1)(e_2+1)...(e_k+1)$
- $\sigma(n) = \Pi \left((p_i^{(e_i+1)} - 1) / (p_i - 1) \right)$

256. Power Tower / Generalized Euler

- Generalized Euler: $a^b \bmod m = a^{(b \bmod \phi(m))} \bmod m$, when $\gcd(a,m)=1$
- Used in power tower problems: $a^{(b^{(c...)})} \bmod m$

261. Euclidean Algorithm

- $\gcd(a,b)$ computed via repeated remainder: $\gcd(a,b) = \gcd(b,a \bmod b)$

262. Extended Euclid

- Finds x,y such that $ax + by = \gcd(a,b)$

263. Bézout’s Identity

- $ax + by = \gcd(a,b)$
- $ax + by = c$ solvable iff $\gcd(a,b)$ divides c

265. Linear Congruence Equation

- $ax \equiv b \pmod{m}$
- Solution exists iff $\gcd(a,m)$ divides b

266. Chinese Remainder Theorem

- $x \equiv ai \pmod{mi}$, with pairwise coprime mi
- $M = \Pi$ mi, Mi = M/mi, yi = Mi^(-1) mod mi
- $x \equiv \Sigma$ ai * Mi * yi (mod M)

269. Discrete Logarithm (BSGS)

- Solve a^x ≡ b (mod m)
- n = ceil(sqrt(m))
- Precompute a^(jn)
- Match b * a^i with table

275. Linear Diophantine Equation with Two Variables

- ax + by = c has solution iff gcd(a,b) divides c
- General solution: x = x0 + (b/g)t, y = y0 - (a/g)t, t∈Z

290. Pisano Period

- Fibonacci modulo m is periodic
- π(m) = smallest k such that F_{n+k} ≡ F_n (mod m)

299. Combination Technique

- C(n,r) = n! / (r!(n-r)!)
- C(n,r) = C(n-1,r-1) + C(n-1,r)
- Vandermonde: Σ C(r,k)C(s,n-k) = C(r+s,n)

305. Lucas Theorem

- For prime p:
- C(n,r) ≡ Π C(ni, ri) (mod p)
- ni,ri are base-p digits of n,r

306. nCr Modulo Any Mod

- If m is prime: factorial precomputation
- If m composite: factorize m and use CRT

352. Matrix Exponentiation

- [F_n, F_{n-1}]^T = [[a, b],[1, 0]]^(n-1) * [F_1, F_0]^T
- General method for solving linear recurrences