Essential Modular Arithmetic & Number Theory Formulas

51. Binary Exponentiation and Basic Modular Arithmetic

• (a + b) mod m = ((a mod m) + (b mod m)) mod m
• (a - b) mod m = ((a mod m) - (b mod m) + m) mod m
• (a * b) mod m = ((a mod m) * (b mod m)) mod m
• Binary exponentiation: a^b mod m in O(log b) using squaring.

52. Fermat’s Little Theorem and Modular Inverse

• Fermat: a^(p-1) ≡ 1 (mod p), if p is prime and gcd(a,p)=1
• Euler: a^φ(m) ≡ 1 (mod m), if gcd(a,m)=1
• Inverse: a^(-1) ≡ a^(p-2) (mod p), when p is prime

255. Euler’s Totient Function / Phi Function

• φ(n) = |{1 ≤ k ≤ n : gcd(k,n)=1}|
• φ(p^e) = p^e - p^(e-1)
• φ(n) = n * Π (1 - 1/p), over distinct primes p dividing n
• Identity: Σ_{d|n} φ(d) = n
• Euler’s theorem: if gcd(a,n)=1, then a^φ(n) ≡ 1 (mod n)

256. Power Tower / Generalized Euler

• Generalized Euler: a^b mod m = a^(b mod φ(m)) mod m, when gcd(a,m)=1
• Used in power tower problems: a^(b^(c...)) mod m

261. Euclidean Algorithm

• gcd(a,b) computed via repeated remainder: gcd(a,b) = gcd(b,a mod 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 ≡ b (mod m)
• Solution exists iff gcd(a,m) divides b

266. Chinese Remainder Theorem

- $x \equiv a_i \pmod{m_i}$, with pairwise coprime m_i
- $M = \Pi\, m_i$, $M_i = M/m_i$, $y_i = M_i^{(-1)} \bmod m_i$
- $x \equiv \Sigma\, a_i * M_i * y_i \pmod{M}$

269. Discrete Logarithm (BSGS)

- Solve $a^x \equiv b \pmod{m}$
- $n = \mathrm{ceil}(\mathrm{sqrt}(m))$
- 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: $x = x_0 + (b/g)t$, $y = y_0 - (a/g)t$, $t \in Z$

290. Pisano Period

- Fibonacci modulo m is periodic
- $\pi(m)$ = smallest k such that $F_{n+k} \equiv F_n \pmod{m}$

299. Combination Technique

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

305. Lucas Theorem

- For prime p:
- $C(n,r) \equiv \Pi\, C(n_i, r_i) \pmod{p}$
- n_i, r_i 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