Essential Modular Arithmetic & Number Theory Formulas (Updated)

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: compute $a^b \bmod m$ in $O(\log b)$ using repeated squaring

52. Fermat’s Little Theorem and Modular Inverse

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

255. Euler’s Totient Function / Phi Function

- $\phi(n) = |\{1 \le k \le n : \gcd(k,n)=1\}|$
- Prime power: $\phi(p^e) = p^e - p^{(e-1)}$
- Multiplicative form: $\phi(n) = n * \Pi_{p|n} (1 - 1/p)$
- Identity: $\Sigma_{d|n} \phi(d) = n$
- Euler’s theorem: if $\gcd(a,n)=1$, then $a^{\phi(n)} \equiv 1 \pmod n$

256. Power Tower / Generalized Euler Theorem (non■coprime case)

- Goal: compute $x^n \bmod m$ even when $\gcd(x,m) \neq 1$
- Let a be the product of common prime powers between x and m: $a = \Pi\, p_i^{k_i}$ where $p_i \mid x$ and $p_i^{k_i} \,\|\, m$
- Let k be the smallest exponent such that a divides x^k
- Then: $x^n \bmod m = (x^k \bmod m) * (x^{n-k} \bmod (m/a)) \bmod m$, with $\gcd(x, m/a) = 1$
- Reduce the remaining exponent using Euler on coprime modulus:
- $x^{n-k} \equiv x^{ (n-k) \bmod \phi(m/a) } \pmod{m/a}$
- Putting together: $x^n \bmod m = (x^k \bmod m) * (x^{ (n-k) \bmod \phi(m/a) } \bmod (m/a)) \bmod m$
- Clean periodic form (when $n \ge \log_2(m)$): $x^n \equiv x^{ \phi(m) + (n \bmod \phi(m)) } \pmod m$
- Special case (coprime): reduces to standard Euler: $x^n \equiv x^{ n \bmod \phi(m) } \pmod m$

261. Euclidean Algorithm

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

262. Extended Euclid

- Computes x,y with $ax + by = \gcd(a,b)$ (also yields modular inverse when gcd=1)

263. Bézout's Identity

- There exist integers x,y such that $ax + by = \gcd(a,b)$
- Linear Diophantine $ax + by = c$ is solvable iff $\gcd(a,b) \mid c$

265. Linear Congruence Equation

- $ax \equiv b \pmod{m}$ has solutions iff $g = \gcd(a,m)$ divides b
- If solvable, number of solutions = g; reduce to $a/g * x \equiv b/g \pmod{m/g}$

266. Chinese Remainder Theorem (CRT)

- System: $x \equiv a_i \pmod{m_i}$ with pairwise coprime m_i
- $M = \Pi\, m_i$, $M_i = M/m_i$, $y_i = \text{inverse}(M_i, m_i)$
- Solution: $x \equiv \Sigma\, a_i * M_i * y_i \pmod{M}$

269. Discrete Logarithm (Baby■Step Giant■Step)

- Solve $a^x \equiv b \pmod{m}$, with $\gcd(a,m)=1$
- Let n = ■√m■. Precompute table $T[j] = a^{j*n} \pmod{m}$ for j=0..n
- Find i in [0..n] s.t. $b * a^i$ matches some T[j]; then $x = j*n - i$

275. Linear Diophantine Equation (Two Variables)

- $ax + by = c$ has solution iff $g = \gcd(a,b) \mid c$
- If (x0,y0) is one solution, all solutions: $x = x_0 + (b/g)t$, $y = y_0 - (a/g)t$, $t \in Z$

290. Pisano Period

- Fibonacci numbers modulo m are periodic with period $\pi(m)$
- $\pi(m)$ is the smallest k such that $F_{n+k} \equiv F_n \pmod{m}$ for all n

299. Combination Technique

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

305. Lucas Theorem

- For prime p: write $n = \Sigma\, n_i p^i$, $r = \Sigma\, r_i p^i$
- $C(n,r) \equiv \Pi_i\, C(n_i, r_i) \pmod{p}$

306. nCr Modulo Any Mod

- If modulus m is composite: factorize $m = \Pi\, p_i^{e_i}$
- Compute C(n,r) modulo each $p_i^{e_i}$ (using prime■power methods), then combine via CRT
- If m is prime: use factorials + inverses modulo m

352. Matrix Exponentiation

- For linear recurrence $F_n = a1*F_{n-1} + ... + ak*F_{n-k}$
- State vector $V_n = [F_n, F_{n-1}, ..., F_{n-k+1}]^T$
- $V_n = T^{n-k} * V_k$, where T is the k×k companion matrix; compute T^p by fast exponentiation