Number Theory Problem-Solving Theorems and Strategies

Inter IIT 14.0 Maths Bootcamp – L6

IIT Kanpur SciMath Society

Basic Divisibility Properties

- $a|b$ means $\exists k \in \mathbb{Z}$ such that $b = ak$.
- If $a|b$ and $a|c$, then $a|(bx + cy)$ for all integers x, y.
- $\gcd(a, b)$ is the smallest positive integer expressible as $ax + by$ (Bézout).
- $\text{lcm}(a, b) = \dfrac{|ab|}{\gcd(a, b)}$.

Use: Simplify integer equations and modular relations.

Euclidean Algorithm and GCD

- $\gcd(a, b) = \gcd(b, a \bmod b)$.
- Termination after $O(\log \min(a, b))$ steps.
- Extended Euclidean Algorithm finds x, y such that $ax + by = \gcd(a, b)$.

Use: In modular inverses, Diophantine equations, and CRT construction.

Congruences and Modular Arithmetic

- $a \equiv b \pmod{m} \iff m|(a-b)$.
- Addition, multiplication, and exponentiation preserve congruence.
- Linear congruence $ax \equiv b \pmod{m}$ solvable iff $\gcd(a,m)|b$.
- If $\gcd(a,m) = 1$, unique solution $\pmod{m}$ given by $x \equiv a^{-1}b$.

Use: Core structure behind all modular and cryptographic reasoning.

Chicken McNugget Theorem (Frobenius Coin Problem)

Theorem: If a, b are positive coprime integers, the largest integer **not representable** as a nonnegative linear combination

$$n = ax + by, \quad x, y \in \mathbb{Z}_{\geq 0}$$

is

$$n_{\max} = ab - a - b.$$

Corollaries:

- The total number of nonrepresentable integers is $\frac{(a-1)(b-1)}{2}$.
- For non-coprime a, b, replace $\mathbb{Z}_{\geq 0}$ by multiples of $\gcd(a, b)$.

Use:

- Fast bound for "coin-sum" or "integer composition" problems.
- Helps in modular Diophantine analysis and bounding arguments.

Example: For $a = 6, b = 9$, gcd $= 3$, so largest impossible multiple is $3((2)(3) - 2 - 3) = 3$.

Fundamental Theorems

- **Euclid's Theorem:** Infinitely many primes.
- **Fundamental Theorem of Arithmetic:** Unique factorization into primes.
- **Prime Number Theorem (asymptotic):** $\pi(x) \sim \dfrac{x}{\log x}$.

Use: Foundation for multiplicative functions and modular reasoning.

Modular Inverse and Euler's Theorem

- If $\gcd(a, m) = 1$, $\exists a^{-1}$ such that $aa^{-1} \equiv 1 \pmod{m}$.
- **Euler's Totient Function:** $\varphi(m) = |\{1 \leq k \leq m : \gcd(k, m) = 1\}|$.
- **Euler's Theorem:** $a^{\varphi(m)} \equiv 1 \pmod{m}$ when $\gcd(a, m) = 1$.
- **Fermat's Little Theorem:** $a^{p-1} \equiv 1 \pmod{p}$ for prime $p \nmid a$.

Use: Fast modular exponentiation and residue class reductions.

Chinese Remainder Theorem

If $\gcd(m_1, m_2, \ldots, m_k) = 1$ pairwise, then the system

$$x \equiv a_i \pmod{m_i}, \quad 1 \leq i \leq k$$

has a unique solution $\pmod{M = m_1 m_2 \cdots m_k}$.

Use:

- Decompose computations modulo composite M.
- Construct inverses or count solutions by modulus splitting.

Problem Trick: Use CRT to combine parity, mod 3, mod 5, mod 7 constraints quickly.

Linear Diophantine Equations

Equation $ax + by = c$ has integer solution iff $\gcd(a, b)|c$.

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t, \quad d = \gcd(a, b)$$

Use: Find minimal positive solutions via modular manipulation.

Exponential and Modular Equations

- For $a^x \equiv b \pmod{m}$, use **discrete log** if small mod.
- Apply **lifting the exponent lemma (LTE)** for valuations:

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n), \text{ if } p|(x - y), p \nmid xy.$$

- Check small moduli first ($\pmod{p}$, $\pmod{p^2}$) then lift.

Use: Handling exponential congruences and p-adic reasoning.

Quadratic Congruences

- Solve $x^2 \equiv a \pmod{p}$.
- **Euler Criterion:** $a^{(p-1)/2} \equiv 1 \pmod{p} \Rightarrow$ quadratic residue.
- **Legendre Symbol:** $\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p} \in \{\pm 1, 0\}$.
- **Quadratic Reciprocity:**

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Use: Essential for modular square root and quadratic residue classification.

Key Arithmetic Functions

- $\tau(n)$ – number of divisors.
- $\sigma(n)$ – sum of divisors.
- $\mu(n)$ – Möbius function: $\mu(n) = \begin{cases} 1, & n = 1 \\ (-1)^k, & n = p_1 p_2 \cdots p_k \\ 0, & \text{otherwise} \end{cases}$
- $\varphi(n)$ – Euler totient.

All are multiplicative: $f(mn) = f(m)f(n)$ when $\gcd(m, n) = 1$.

Dirichlet Convolution and Möbius Inversion

For arithmetic functions f, g:

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

Identity: $f = g * 1 \iff g = f * \mu$ (Möbius inversion).
Use:

- Inversion of divisor sums.
- Counting coprime pairs or functions defined over divisors.

Trick: Try switching sums $\sum_{d|n}$ and using μ to isolate terms.

Wilson, Carmichael, and Orders

- **Wilson's Theorem:** $(p-1)! \equiv -1 \pmod{p}$.
- **Order of an element:** $\text{ord}_m(a)$ is least k with $a^k \equiv 1 \pmod{m}$.
- **Carmichael Function:** $\lambda(m)$ is the least L s.t. $a^L \equiv 1$ for all $\gcd(a, m) = 1$.
- $\lambda(m) | \varphi(m)$ and $a^{\lambda(m)} \equiv 1 \pmod{m}$.

Use: Find minimal exponent period or multiplicative cycle length.

Primitive Roots and Indices

- Primitive root g mod m: generates all coprime residues.
- Exists for $m = 2, 4, p^k, 2p^k$ (odd p).
- If g is primitive, then every $a \equiv g^k$ defines index $\text{ind}_g(a) = k$.
- Converts multiplicative problems $\rightarrow$ linear problems mod $\varphi(m)$.

Use: Transform powers into modular linear equations.

Divisibility and Congruence Strategies

- Always reduce to simplest modulus.
- Check small primes separately ($2, 3, 5, 7$ often sufficient).
- Replace divisibility by congruence mod divisors.
- Exploit periodicity: test residues mod small m before general.
- In optimization or construction problems, balance residues or use CRT.

Equation and Diophantine Strategies

- Start with parity and modulo analysis.
- Divide by gcd to simplify.
- For symmetric integer equations, try bounding or factoring tricks.
- Use infinite descent or modular contradiction to prove impossibility.
- In exponential cases, test small moduli to identify contradictions quickly.

Prime and Factorization Strategies

- Test small prime patterns before generalizing.
- Compare powers of primes on both sides of equations.
- Use v_p-valuation logic for exponent comparison.
- If product equals a power, each prime's exponent must be multiple of k.
- For inequalities, approximate growth using log or $\sqrt{n}$ bounds.

Advanced Modular Problem Strategies

- Convert recurrence or exponent problems using Euler/Fermat.
- Split modulus into coprime parts, solve separately via CRT.
- If modular equations are nonlinear, square both sides to linearize.
- Guess small cycles for a^k mod m to infer periodic behavior.
- For large exponents, use order or Carmichael function reduction.

Vieta Jumping Technique

Concept: A powerful method for solving symmetric Diophantine equations of the form

$$P(x, y) = 0$$

where exchanging x and y preserves structure, allowing generation of new integer solutions via Vieta's formulas.

Mechanism:

- Treat one variable (say x) as unknown and form quadratic:

$$x^2 + bx + c = 0$$

  with integer coefficients depending on y.
- Use Vieta's relations: if x_1, x_2 are roots, then

$$x_1 + x_2 = -b, \quad x_1 x_2 = c.$$

- Replace (x_1, y) by (x_2, y) to obtain a new integer solution.
- "Jump" repeatedly until reaching minimal positive solution.

General Problem-Solving Insights

- **Work modulo primes first.**
- Identify multiplicative structure: invertibility, orders, residues.
- Reduce algebraic problems to modular statements.
- For existence proofs, use Pigeonhole Principle or CRT arguments.
- Exploit symmetry, parity, and valuation reasoning — core of Olympiad NT.