Pre-Session Study Guide

Number Theory ideas

We outline some number theoretic ideas that recur in the Putnam. They include modular arithmetic, polynomial congruences, representations of integers, finite field power sums, and methods of infinite descent.

I. Modular Arithmetic and Exponent Constraints

Modular arithmetic provides essential tools for constraining the possible values of integer variables, parities, and exponential expressions.

Theorem 1.1: Quadratic Residues and Powers Modulo 2^k

Let $n \in \mathbb{Z}$.

1. $n^2 \equiv 0, 1 \pmod 3$.
2. $n^2 \equiv 0, 1, 4 \pmod 8$. In particular, an odd square is always $1 \pmod 8$.
3. For any odd integer a, the multiplicative order of a modulo 2^k (for $k \geq 3$) divides 2^{k-2}.

Generic Example: Exponential Parity Barrier

Problem: Prove that $3^m - 2^n = 1$ has no positive integer solutions with $n \geq 3$ except $(m, n) = (2, 3)$ and $(1, 1)$.

Solution Strategy:

1. **Modulo 3 Analysis:** Reducing $3^m - 2^n \equiv 1 \pmod 3$ yields $-(-1)^n \equiv 1 \implies (-1)^n \equiv -1 \pmod 3$, which forces n to be **odd**.
2. **Modulo 4 Analysis:** If $n \geq 2$, reducing $3^m - 0 \equiv 1 \implies (-1)^m \equiv 1 \pmod 4$, which forces m to be **even**. Let $m = 2k$.
3. **Algebraic Factorization:** Rewrite the equation as $(3^k - 1)(3^k + 1) = 2^n$. The two factors $3^k - 1$ and $3^k + 1$ are powers of 2 differing by 2. The only powers of 2 differing by 2 are 2 and 4, yielding $3^k - 1 = 2 \implies k = 1$, so $m = 2$ and $n = 3$.

II. Chinese Remainder Theorem and Multiplicative Splitting

When analyzing modular properties modulo a composite integer $N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, global congruence conditions decompose into independent local conditions over each prime power.

Theorem 2.1: Chinese Remainder Theorem

Let $n_1, n_2, \ldots, n_k$ be pairwise coprime positive integers, and let $N = \prod_{i=1}^{k} n_i$. Then the natural ring map
$\mathrm{Z/NZ} \cong (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})$

is an isomorphism. Furthermore, the unit groups split multiplicatively:
$(\mathrm{Z/NZ})^\times \cong (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})^\times$.

Generic Example: Simultaneous Modular Reconstruction

Problem: Characterize all integers x such that $x^2 \equiv 1 \pmod{pq}$, where $p < q$ are distinct odd primes.

Solution Strategy: By the Chinese Remainder Theorem, $x^2 \equiv 1 \pmod{pq} \iff x^2 \equiv 1 \pmod{p}$ and $x^2 \equiv 1 \pmod{q}$. Since $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$ are finite fields, the quadratic $t^2 - 1 = 0$ has exactly two roots in each field:
$x \equiv \pm 1 \pmod{p}$ and $x \equiv \pm 1 \pmod{q}$.

This yields $2 \times 2 = 4$ independent system choices $(x \bmod p, x \bmod q) \in \{(1,1), (-1,-1), (1,-1), (-1,1)\}$, demonstrating that 1 has exactly **4 distinct square roots** modulo pq.

III. p-adic Valuations and Infinite Descent

The p-adic valuation $v_p(n)$ measures the exponent of the highest power of p dividing n. Combining valuation inequalities with Fermat's method of infinite descent establishes non-existence proofs for higher-degree Diophantine equations.

Theorem 3.1: Properties of p-adic Valuations

For any prime p and non-zero integers a, b:

1. $v_p(ab) = v_p(a) + v_p(b)$.
2. $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$, with strict equality if $v_p(a) \neq v_p(b)$.
3. **Legendre's Formula:** $v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n - S_p(n)}{p-1}$, where $S_p(n)$ is the sum of the base-p digits of n.

Generic Example: Proof by 2-adic Infinite Descent

Problem: Prove that $x^3 + 2y^3 = 4z^3$ has no non-zero integer solutions.

Solution Strategy:

1. Suppose a non-zero solution exists, and choose a solution (x, y, z) minimizing $|x| + |y| + |z|$.
2. Reducing modulo 2: $x^3 \equiv 0 \pmod{2} \implies 2 \mid x$. Substitute $x = 2x_1$ to get $8x_1^3 + 2y^3 = 4z^3 \implies y^3 + 2z^3 = 4x_1^3$.
3. Reducing modulo 2 again: $y^3 \equiv 0 \pmod{2} \implies 2 \mid y$. Substitute $y = 2y_1$ to get $8y_1^3 + 2z^3 = 4x_1^3 \implies z^3 + 2x_1^3 = 4y_1^3$.
4. Reducing modulo 2 a third time: $2 \mid z$. Substitute $z = 2z_1$.
5. The tuple $(x_1, y_1, z_1) = (x/2, y/2, z/2)$ forms a strictly smaller non-zero integer solution, contradicting the minimality assumption. Thus, no non-zero solution exists.

IV. Polynomial Congruences and Root Lifting

Integer-coefficient polynomials $P(x) \in \mathbb{Z}[x]$ preserve modular congruences, allowing local-to-global divisibility analysis and root lifting modulo prime powers.

Theorem 4.1: Polynomial Congruences and Hensel's Lemma

Let $P(x) \in \mathbb{Z}[x]$.

1. **Preservation of Congruence:** If $a \equiv b \pmod{m}$, then $P(a) \equiv P(b) \pmod{m}$. In particular, $(a-b) \mid (P(a) - P(b))$.
2. **Hensel's Lemma:** Let p be a prime. If $r \in \mathbb{Z}$ satisfies $P(r) \equiv 0 \pmod{p^k}$ and $P'(r) \not\equiv 0 \pmod{p}$, then there exists a unique root $r' \pmod{p^{k+1}}$ such that $r' \equiv r \pmod{p^k}$ and $P(r') \equiv 0 \pmod{p^{k+1}}$.

Generic Example: Polynomial Divisibility Constraints

Problem: Let $P(x) \in \mathbb{Z}[x]$ be a polynomial with positive integer coefficients. Show that if $P(n)$ divides $P(P(n)+c)$ for all $n \geq 1$, then $P(c) = 0$.

Solution Strategy: Since $P(n) + c \equiv c \pmod{P(n)}$, applying Theorem 4.1(1) yields: $\mathrm{P(P(n) + c)} \equiv P(c) \pmod{P(n)}$.

Thus, $P(n) \mid P(P(n)+c) \iff P(n) \mid P(c)$. For a nonconstant polynomial with positive coefficients, $|P(n)| > |P(c)|$ for all sufficiently large n. The only way a larger integer $P(n)$ can divide a fixed constant $P(c)$ for all large n is if $P(c) = 0$.

V. Power Sums over Finite Fields and Primitive Roots

Sums of powers of all non-zero elements in a finite field $\mathbb{F}_p$ exhibit a sharp structural dichotomy governed by primitive roots.

Theorem 5.1: Power Sums over $\mathbb{F}_p$

Let p be a prime, $j \geq 0$ an integer, and $S_j = \sum_{x=1}^{p-1} x^j \pmod{p}$. Then:

$$\mathrm{S}_j \equiv \begin{cases} -1 \pmod{p} & \text{if } (p-1) \mid j \text{ and } j > 0, \\ 0 \pmod{p} & \text{if } (p-1) \nmid j \text{ or } j = 0 \text{ (with } 0^0 = 1). \end{cases}$$

Generic Example: Power Sum Vanishing

Problem: Let $p > 3$ be a prime. Prove that $\sum_{x=1}^{p-1} x^k \equiv 0 \pmod{p}$ for all $k \in \{1, 2, \ldots, p-2\}$.

Solution Strategy: Since $1 \leq k \leq p-2$, k is not a multiple of $p-1$. By Theorem 5.1, $S_k \equiv 0 \pmod{p}$ immediately.

VI. Linear Recurrences and Divisibility Sequences

Integer sequences $(u_n)_{n \geq 0}$ satisfying homogeneous linear recurrence relations possess intrinsic periodicity and algebraic divisibility properties.

Theorem 6.1: Modular Periodicity and Divisibility Sequences

Let $(u_n)_{n\geq 0}$ be a linear recurrence sequence with integer coefficients.

1. **Pisano Periodicity:** For any integer $m \geq 2$, the sequence $(u_n \bmod m)_{n\geq 0}$ is purely periodic if the trailing coefficient of the characteristic polynomial is coprime to m.
2. **Divisibility Sequence Property:** If $u_0 = 0$ and $u_n = Au_{n-1} + Bu_{n-2}$ with $\gcd(A, B) = 1$, then $u_m \mid u_n$ whenever $m \mid n$.

Generic Example: Divisibility in Second-Order Recurrences

Problem: Let $u_0 = 0, u_1 = 1$, and $u_{n+1} = 4u_n - u_{n-1}$ for $n \geq 1$. Show that $k \mid n \implies u_k \mid u_n$.
Solution Strategy: Using the characteristic equation $r^2 - 4r + 1 = 0$, roots are $\alpha, \beta = 2 \pm \sqrt{3}$. Binet's formula yields $u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$. If $n = k \cdot m$, then:
$\mathrm{u}_{km} = \frac{(\alpha^k)^m - (\beta^k)^m}{\alpha - \beta} = \left(\frac{\alpha^k - \beta^k}{\alpha - \beta}\right) \cdot \left(\sum_{j=0}^{m-1} \alpha^{k(m-1-j)} \beta^{kj}\right) = u_k \cdot v_m,$

where v_m is an integer expression. Thus $u_k \mid u_n$.

VII. Recommended References for Further Study

[1] **T. Andreescu and D. Gelca**, *Putnam and Beyond*, 2nd ed., Springer, 2017.

[2] **I. Niven, H. S. Zuckerman, and H. L. Montgomery**, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley & Sons, 1991.

[3] **G. H. Hardy and E. M. Wright**, *An Introduction to the Theory of Numbers*, 6th ed., Oxford University Press, 2008.

[4] **K. S. Kedlaya, B. Poonen, and R. Vakil**, *The William Lowell Putnam Mathematical Competition 1985–2000: Problems, Solutions, and Commentary*, MAA, 2002.

[5] **K. S. Kedlaya, D. Kane, J. Kane, and E. O'Dorney**, *The William Lowell Putnam Mathematical Competition 2001–2016: Problems, Solutions, and Commentary*, MAA, 2020.

[6] **K. S. Kedlaya**, *The Putnam Archive*, available online at https://kskedlaya.org/putnam-archive/.