Pre-Session Study Guide

Number Theory problems

I picked five Putnam problems using number theory, we will see them at our next session. I asked Gemini to produce a study guide to help prepare for the problems. Below is the result.

I. Modular Arithmetic and Exponent Constraints

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

Key Concept 1: Modular Reduction of Exponential Equations

When analyzing Diophantine equations involving exponential expressions of the form $a^m \pm b^n = C$:

- **Small Prime Moduli:** Reducing modulo small integers (e.g., $3, 4, 8$) often establishes parity constraints on exponents or restricts base residues.
- **Quadratic Residues:** Reducing modulo 4 or 8 restricts possible values for squares ($x^2 \equiv 0, 1, 4 \pmod 8$), which immediately limits parity options for exponents.
- **Cyclic Powers:** The sequence of powers $a^n \pmod m$ is purely periodic. Identifying the period (order of $a \pmod m$) restricts n to specific congruence classes.

Strategy Checklist: Exponential Analysis

1. Test the equation modulo 3 to eliminate base possibilities or establish the parity of exponents.
2. Test modulo 4 or 8 to deduce the parity of base variables and odd/even exponent constraints.
3. Look for prime factorizations of constant terms C to discover algebraic divisibility relations.

II. Polynomial Congruences and Integral Divisibility

Polynomials with integer coefficients preserve modular congruences, leading to powerful constraints on divisibility.

Key Concept 2: The Fundamental Polynomial Congruence

Let $P(x) \in \mathbb{Z}[x]$ be a polynomial with integer coefficients.

- **Divisibility Property:** For any integers a and b, $(a - b) \mid (P(a) - P(b))$.
- **Modular Shift:** For any integer k, $P(x + k \cdot M) \equiv P(x) \pmod{M}$.
- **Self-Composition Modulo $P(n)$:** Substituting $x = P(n) + c$ into $P(x)$ yields: $P(P(n) + c) \equiv P(c) \pmod{P(n)}$.

  In particular, taking $c = 1$ gives $P(P(n)+1) \equiv P(1) \pmod{P(n)}$, meaning $P(n) \mid P(P(n)+1)$ if and only if $P(n) \mid P(1)$.
- **Growth Bounds:** For nonconstant polynomials with positive coefficients and $n > 1$, $0 < |P(1)| < |P(n)|$, which prevents $P(n)$ from dividing $P(1)$.

III. Sums of Consecutive Integers and Parity Factorizations

Representing integers as sums of consecutive terms involves analyzing factorizations into pairs of opposite parity.

Key Concept 3: Representation as Consecutive Integer Sums

Let N be a positive integer.

- **Sum Formula:** A sum of k consecutive positive integers starting at $a \geq 1$ is given by: $N = \sum_{i=0}^{k-1}(a + i) = \frac{k(2a+k-1)}{2} \implies 2N = k(2a + k - 1)$.
- **Opposite Parity Factorization:** The factors k and $M = 2a + k - 1$ satisfy $M > k \geq 1$ and have opposite parity (one is odd, the other is even).
- **Bijection with Odd Divisors:** Each odd divisor $d > 1$ of N (or $2N$) uniquely determines a valid length $k > 1$ for a sum of consecutive integers:
  - If $d < \sqrt{2N}$, set $k = d$ and $2a + k - 1 = 2N/d$.
  - If $d > \sqrt{2N}$, set $k = 2N/d$ and $2a + k - 1 = d$.
- **Uniqueness Condition:** An integer N has a *unique* representation as a sum of $k > 1$ consecutive positive integers if and only if N has exactly one odd prime factor (i.e., $2N = p \cdot 2^m$ for some prime p and integer $m \geq 1$).

IV. Power Sums over Finite Fields and CRT Decomposition

Evaluating sums of powers over coprime residue classes requires understanding finite field multiplicative group structures and Chinese Remainder Theorem (CRT) decomposition.

Key Concept 4: Power Sums in Finite Fields

Let p be a prime number, and let $S_j = \sum_{x \in \mathbb{F}_p^*} x^j \pmod{p}$.

- **Case 1:** $(p-1) \mid j$**:** By Fermat's Little Theorem, $x^{p-1} \equiv 1 \pmod{p}$ for all $x \not\equiv 0 \pmod{p}$. Thus, each term $x^j \equiv 1 \pmod{p}$, giving:
$\mathrm{S}_j \equiv \sum_{x=1}^{p-1} 1 = p - 1 \equiv -1 \pmod{p}$.

- **Case 2:** $(p-1) \nmid j$**:** Let g be a primitive root modulo p. Multiplication by g permutes the nonzero residue classes $\mathbb{F}_p^*$. Therefore:
$\mathrm{S}_j = \sum_{x \in \mathbb{F}_p^*} x^j \equiv \sum_{x \in \mathbb{F}_p^*} (gx)^j = g^j S_j \pmod{p} \implies (g^j - 1) S_j \equiv 0 \pmod{p}$.

  Since $(p-1) \nmid j$, $g^j \not\equiv 1 \pmod{p}$, forcing $S_j \equiv 0 \pmod{p}$.

Key Concept 5: Extension to Composite Moduli via CRT

Let $M = p_1 p_2 \cdots p_r$ be a square-free integer, and let $A = \{n \in \{1, \ldots, M\} : \gcd(n, M) = 1\}$.

- By the Chinese Remainder Theorem, the sum $S(j) = \sum_{n \in A} n^j \pmod{M}$ splits into independent power sums modulo each prime factor p_i.
- Modulo p_i, the set A covers each nonzero residue class in $\mathbb{F}_{p_i}^*$ an equal number of times (specifically, $\frac{\phi(M)}{p_i - 1}$ times).
- Consequently, $M \mid S(j)$ if and only if $(p_i - 1) \nmid j$ for every prime factor $p_i \mid M$.

V. Diophantine Equations, Valuations, and Infinite Descent

Proving that certain Diophantine power equations have no non-trivial integer solutions relies on p-adic valuations and Fermat's principle of infinite descent.

Key Concept 6: p-adic Valuations and Infinite Descent

Let $v_p(n)$ denote the p-adic valuation of n (the exponent of the highest power of p dividing n).

- **Valuation Properties:**
$\mathrm{v}_p(ab) = v_p(a) + v_p(b), \quad v_p(a+b) \geq \min(v_p(a), v_p(b))$.

  If $v_p(a) \neq v_p(b)$, equality holds: $v_p(a+b) = \min(v_p(a), v_p(b))$.

- **Application to Diophantine Power Equations:** For equations of the form $c_1a^n + c_2b^n = c_3c^n$ with $n \geq 3$:

  1. Analyzing v_2 or v_p of individual terms often forces a, b, c to share a common factor p.
  2. Assuming $\gcd(a, b, c) = 1$ leads to an immediate contradiction.
  3. Alternatively, dividing through by p^n produces a strictly smaller integer solution, initiating an infinite descent that demonstrates no minimal positive solution exists.

VI. References for Further Study

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

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

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

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

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

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