Putnam Seminar: Week 4
Polynomials & Number Theory
Tuesday, November 29, 2022

Important Notes:

• The Putnam exam is happening on Saturday December 3, 2022 in DL 220. You can sign up and get more information at this link: https://www.maa.org/math-competitions/putnam-competition

Reference: Questions supplied by Prof. Pat Devlin (Some problems taken from Putnam and Beyond by Gelca and Andreescu, also Mathematical Puzzles: A Connoisseur’s Collection by Peter Winkler.)

Polynomials

• Polynomials: polynomials look like \( p(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \) (if \( a_n \neq 0 \), then \( p(x) \) is said to have degree \( n \)).

• Single variable: If \( \deg(p(x)) \leq n \) and \( p(x) \) has at least \( n + 1 \) distinct roots, then \( p(x) = 0 \) [i.e., \( a_i = 0 \) for all \( i \)]. (This works over any field.)

• Useful thing about modular arithmetic: Given integers \( a \) and \( b \) and a polynomial \( f(x) \) with integer coefficients, \( a - b \) must divide \( f(a) - f(b) \).

• Rational roots test: Say \( P(x) = \sum_{i=0}^{n} a_i x^i \) has integer coefficients, \( a_n \neq 0 \), and \( r \) and \( s \) are integers. If \( P(r/s) = 0 \), then \( r \) divides \( a_0 \) and \( s \) divides \( a_n \).

• Two variables: Suppose \( P(x, y) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,j} x^i y^j \). And suppose there are sets \( A, B \) where \( |A| = |B| = n + 1 \) and that \( P(a, b) = 0 \) for all \( (a, b) \in A \times B \). Then \( P(x, y) = 0 \) [i.e., all \( a_{i,j} = 0 \)]

• Multiplicity: If \( r \) is a root with multiplicity \( m \), then \( p^{(j)}(r) = 0 \) for \( 1 \leq j \leq m - 1 \) and \( p^{(m)}(r) \neq 0 \). (where \( p^{(j)}(x) \) is the \( j \)th derivative)

• Viète’s relations: Suppose \( a_n \neq 0 \) and \( P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \) factors as \( P(x) = a_n (x - r_1)(x - r_2) \cdots (x - r_n) \). Then we have

\[
\begin{align*}
-a_{n-1}/a_n &= r_1 + r_2 + \cdots + r_n \\
-a_{n-2}/a_n &= r_1 r_2 + r_1 r_3 + \cdots + r_{n-1} r_n \\
&\vdots \\
(-1)^k a_{n-k}/a_n &= \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} r_{i_1} r_{i_2} \cdots r_{i_k} \\
&\vdots \\
(-1)^n a_0/a_n &= r_1 r_2 r_3 \cdots r_{n-1} r_n.
\end{align*}
\]
Number Theory

- **Modular arithmetic:** When trying to prove things about divisibility, primes, or non-existence of solutions, reach for modular arithmetic. It’s great.

- **Quadratic residues:** Every odd square is one more than a multiple of 8. (Other useful moduli to think on are 3, 5, et cetera?) Similarly, $x^3$ is $0, \pm 1 \mod 7$.

- **Fundamental theorem of arithmetic:** Prime factorization is unique.

- **gcd:** Fact $\gcd(a, b) = \gcd(a - kb, b)$. Another fact: $\gcd(x^a - 1, x^b - 1) = x^{\gcd(a, b)} - 1$.

- **Euler’s theorem:** If $\gcd(a, n) = 1$, then $a^{\varphi(n)} = 1 \mod n$, where $\varphi(n) = \# \{x \leq n : \gcd(x, n) = 1\}$.

- **Factoring trick** $xy + ax + by = (x + b)(y + a) - ab$

1. Find all polynomials $P(x)$ with real coefficients for which there is a positive integer $n$ such that for all $x$, we have $P\left(x + \frac{1}{n}\right) + P\left(x - \frac{1}{n}\right) = 2P(x)$.

2. Find all polynomials with integer coefficients satisfying $P(P'(x)) = P'(P(x))$ for all $x \in \mathbb{R}$.

3. (Putnam 1971) Find all polynomials $p(z)$ where $p(0) = 0$ and $p(z^2 + 1) = p(z)^2 + 1$.

4. (USAMO 1974) Let $a, b, c$ be distinct integers. Show there is no polynomial $P(x)$ with integer coefficients such that $P(a) = b$, $P(b) = c$, and $P(c) = a$.

5. (Putnam 2003) Do there exist polynomials $a(x), b(x), c(y), d(y)$ such that

$$1 + xy + x^2y^2 = a(x)c(y) + b(x)d(y)$$

hold identically?

6. (Putnam 2004) Suppose $p(x) = \sum_{i=0}^{n} c_i x^i$ is a polynomial with integer coefficients, and suppose that $r$ is a rational number such that $p(r) = 0$. Show that the following $n$ numbers are all integers

$$c_n r, c_n r^2 + c_{n-1} r, c_n r^3 + c_{n-1} r^2 + c_{n-2} r, \ldots, c_n r^n + c_{n-1} r^{n-1} + \cdots + c_1 r.$$

7. (Putnam 2003) Let

$$f(z) = a z^4 + b z^3 + c z^2 + d z + e = a(z - r_1)(z - r_2)(z - r_3)(z - r_4),$$

where $a, b, c, d, e$ are integers and $a \neq 0$. Show that if $r_1 + r_2$ is rational and $r_1 + r_2 \neq r_3 + r_4$ then $r_1 r_2$ is a rational number.

8. (Putnam 2016) Find the smallest positive integer $j$ such that for every polynomial $p(x)$ with integer coefficients and for every integer $k$, the integer

$$p^{(j)}(k) = \left. \frac{d^j}{dx^j} p(x) \right|_{x=k}$$

(the $j^{th}$ derivative of $p(x)$ evaluated at $k$) is divisible by 2016.
9. (USAMO 1975) Let $P(x)$ be a polynomial of degree $n$ and suppose $P(k) = k/(k + 1)$ for all integers $0 \leq k \leq n$. Find $P(n + 1)$.

10. Prove that there are infinitely many primes of the form $4n + 3$.

11. Prove that there are infinitely many primes of the form $4n + 1$.

12. Find all primes $p$ such that $p^2 + 2$ is also prime.

13. (Putnam 1988) Prove that every composite number (greater than 1) is expressible as $xy + xz + yz + 1$ with $x, y,$ and $z$ positive integers.

14. (Putnam 1989) How many primes among the positive integers, written as usual in base 10, are such that their digits are alternating 1’s and 0’s beginning and ending with 1?

15. (Putnam 2010) Prove that for each positive integer $n$, the number

$$10^{10^n} + 10^{10^n} + 10^n - 1$$

is not prime.