11. Integer polynomials

Po-Shen Loh
CMU Putnam Seminar, Fall 2013

1 Famous results

Divisibility. If $a$ and $b$ are integers, and $p(x)$ is a polynomial with integer coefficients, then $p(a) - p(b)$ is always divisible by $a - b$.

Chinese remainder theorem. Let $m_1, m_2, \ldots, m_k$ be positive integers which are pairwise relatively prime, and let $a_1, \ldots, a_k$ be arbitrary integers. Then, the following system has integer solutions for $x$:

\begin{align*}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\vdots \\
x &\equiv a_k \pmod{m_k},
\end{align*}

and all solutions $x$ have the same residue modulo the product $m_1m_2\cdots m_k$.

Gauss’s lemma. Non-constant integer polynomials which are irreducible over $\mathbb{Z}$ are also irreducible over $\mathbb{Q}$.

Eisenstein’s criterion. Suppose that $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$, and there is a prime number $p$ such that (i) $p$ divides each of $a_0, a_1, \ldots, a_{n-1}$, (ii) $p$ does not divide $a_n$, and (iii) $p^2$ does not divide $a_0$. Then, $f(x)$ is irreducible over $\mathbb{Q}$.

2 Problems

1. Albert Einstein and Homer Simpson are playing a game in which they are creating a polynomial

$$p(x) = x^{2012} + a_{2011}x^{2011} + \cdots + a_1x + a_0.$$ 

They take turns choosing one of the coefficients $a_0, \ldots, a_{2011}$, assigning a real value to it (even though the topic of this week is integer polynomials). Once a value is assigned to a coefficient, it cannot be overwritten in a future turn, and the game ends when all coefficients have been assigned. Albert moves first. Homer’s goal is to make $p(x)$ divisible by a fixed polynomial $m(x)$, and Albert’s goal is to prevent this.

(a) Which of the players has a winning strategy if $m(x) = x - 2012$?

(b) What if $m(x) = x^2 + 1$?

2. Let $p$, $q$, and $s$ be nonconstant integer polynomials such that $p(x) = q(x)s(x)$. Suppose that the polynomial $p(x) - 2008$ has at least 81 distinct integer roots. Prove that the degree of $q$ must be greater than 5.
3. Let \( p \) be a quadratic polynomial with integer coefficients. Suppose that \( p(z) \) is divisible by 5 for every integer \( z \). Prove that all coefficients of \( p \) are divisible by 5.

4. Let \( x, y, z \) be integers such that \( x^4 + y^4 + z^4 \) is divisible by 29. Prove that \( x^4 + y^4 + z^4 \) is actually divisible by \( 29^4 \).

5. Let \( p \) be a polynomial with integer coefficients, and let \( a_1, \ldots, a_k \) be distinct integers. Prove that there always exists an \( a \in \mathbb{Z} \) such that \( p(a) | p(a_i) \) for all \( i \).

6. Let \( f(x) \) be a rational function, i.e., there are polynomials \( p \) and \( q \) such that \( f(x) = p(x)/q(x) \) for all \( x \). Prove that if \( f(n) \) is an integer for infinitely many integers \( n \), then \( f \) is actually a polynomial.

7. Let \( a, b \) be integers. Show that the set \( \{ ax^2 + by^2 : x, y \in \mathbb{Z} \} \) misses infinitely many integers.

8. Let \( a, b \) be integers. Show that the set \( \{ ax^5 + by^5 : x, y \in \mathbb{Z} \} \) misses infinitely many integers.

9. Let \( a, b, n \) be integers (\( n \) positive) for which the set \( \{ ax^n + by^n : x, y \in \mathbb{Z} \} \) includes all but finitely many integers. Prove that \( n = 1 \).

10. Let \( p \) be a polynomial with real coefficients and degree \( n \). Suppose that \( \frac{p(b) - p(a)}{b - a} \) is an integer for all \( 0 \leq a < b \leq n \). Prove that \( \frac{p(b) - p(a)}{b - a} \) is an integer for all pairs of distinct integers \( a < b \).

3 Homework

Please write up solutions to two of the problems, to turn in at next week’s meeting. One of them may be a problem that we discussed in class.