Polynomials

Alexander Remorov
alexanderrem@gmail.com

Warm-up Problem 1: Let $f(x)$ be a quadratic polynomial. Prove that there exist quadratic polynomials $g(x)$ and $h(x)$ such that $f(x)f(x+1) = g(h(x))$.
(University of Toronto Math Competition 2010)

Solution: The standard approach would be to write $f(x) = ax^2 + bx + c$ and play around with the coefficients of $f(x)f(x+1)$. It is doable, but quite messy. Let us **look at the roots**. Let $f(x) = a(x-r)(x-s)$, then:

$$f(x)f(x+1) = a^2 \cdot (x-r)(x-s+1) \cdot (x-s)(x-r+1) =$$
$$= a^2([x^2 - (r+s-1)x + rs] - r)([x^2 - (r+s-1)x + rs] - s)$$

and we are done by setting $g(x) = a^2(x-r)(x-s), h(x) = x^2 - (r+s-1)x + rs$.

Warm-up Problem 2: The polynomial $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n = 0$ with integer non-zero coefficients has n distinct integer roots. Prove that if the roots are pairwise coprime, then a_{n-1} and a_n are coprime.
(Russian Math Olympiad 2004)

Solution: Assume $\gcd(a_{n-1}, a_n) \neq 1$, then both a_{n-1} and a_n are divisible by some prime p. Let the roots of the polynomial be $r_1, r_2, \cdots, r_n$. Then $r_1r_2\cdots r_n = (-1)^n a_n$. This is divisible p, so at least one of the roots, wolog r_1, is divisible by p. We also have:

$$r_1r_2\cdots r_{n-1} + r_1r_3r_4\cdots r_{n-1} + \cdots + r_2r_3\cdots r_n = (-1)^{n-1}a_{n-1} \equiv 0 \bmod p$$

All terms containing r_1 are divisible by p, hence $r_2r_3\cdots r_n$ is divisible by p. Hence $\gcd(r_1, r_2r_3\cdots r_n)$ is divisible by p contradicting the fact that the roots are pairwise coprime. The result follows.

1 Algebra

Fundamental Theorem of Algebra: A polynomial $P(x)$ of degree n with complex coefficients has n complex roots. It can be uniquely factored as:

$$P(x) = a(x-r_1)(x-r_2)\cdots(x-r_n)$$

Vieta's Formulas: Let $P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with complex coefficients have roots $r_1, r_2, \cdots, r_n$. Then:

$$\sum_{i=1}^{n} r_i = (-1)^1\frac{a_{n-1}}{a_n}; \qquad \sum_{i<j} r_ir_j = (-1)^2\frac{a_{n-2}}{a_n}; \qquad \cdots \qquad r_1r_2\cdots r_n = (-1)^n\frac{a_0}{a_n}$$

Bezout's Theorem: A polynomial $P(x)$ is divisible by $(x - a)$ iff $P(a) = 0$.
Lagrange Interpolation: Given n points $(x_1, y_1), \cdots, (x_n, y_n)$, there is a unique polynomial $P(x)$ satisfying $P(x_i) = y_i$. Its explicit formula is:

$$P(x) = \sum_{i=1}^{n} y_i \prod_{1\le j\le n, j\ne i} \frac{x - x_j}{x_i - x_j}$$

A few general tricks related to polynomials:

- **Look at the roots**. If you want to show a polynomial is identically 0, it is sometimes useful to look at an arbitrary root r of this polynomial, and then show the polynomial must have another root, e.g. $r + 1$, thus producing a sequence of infinitely many roots.
- **Look at the coefficients**. This is particularly useful when the coefficients are integers. It is often a good idea to look at the leading coefficient and the constant term.
- Consider the degrees of polynomials. If $P(x)$ is divisible by $Q(x)$ where P, Q are polynomials, then $\deg(Q) \le \deg(P)$. A straight-forward fact, yet a useful one.
- Perform clever algebraic manipulations, such as factoring, expanding, introducing new polynomials, substituting other values for x, e.g. $x + 1$, $\frac{1}{x}$, etc.

1.1 Warm-up

1. Let $P(x)$ and $Q(x)$ be polynomials with real coefficients such that $P(x) = Q(x)$ for all real values of x. Prove that $P(x) = Q(x)$ for all complex values of x.
2. (a) Determine all polynomials $P(x)$ with real coefficients such that $P(x^2) = P^2(x)$.
   (b) Determine all polynomials $P(x)$ with real coefficients such that $P(x^2) = P(x)P(x + 1)$.
   (c) Suppose $P(x)$ is a polynomial such that $P(x - 1) + P(x + 1) = 2P(x)$ for all real x. Prove that $P(x)$ has degree at most 1.
3. (USAMO 1975) A polynomial $P(x)$ of degree n satisfies $P(k) = \dfrac{k}{k+1}$ for $k = 0, 1, 2, ..., n$. Find $P(n + 1)$.

1.2 Problems

1. (Brazil 2007) Let $P(x) = x^2 + 2007x + 1$. Prove that for every positive integer n, the equation $P(P(\dots(P(x))\dots)) = 0$ has at least one real solution, where the composition is performed n times.
2. (Russia 2002) Among the polynomials $P(x), Q(x), R(x)$ with real coefficients at least one has degree two and one has degree three. If $P^2(x) + Q^2(x) = R^2(x)$ prove that one of the polynomials of degree three has three real roots.
3. Let $P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a polynomial with integer coefficients such that $|a_0|$ is prime and $|a_0| > |a_1 + a_2 + \cdots + a_n|$. Prove that $P(x)$ is *irreducible* (that is, cannot be factored into two polynomials with integer coefficients of degree at least 1).

4. (Russia 2003) The side lengths of a triangle are the roots of a cubic equation with rational coefficients. Prove that the altitudes are the roots of a degree six equation with rational coefficients.

5. (Russia 1997) Does there exist a set S of non-zero real numbers such that for any positive integer n there exists a polynomial $P(x)$ with degree at least n, all the roots and all the coefficients of which are from S?

6. (Putnam 2010) Find all polynomials $P(x), Q(x)$ with real coefficients such that $P(x)Q(x+1) - P(x+1)Q(x) = 1$.

7. (IMO SL 2005) Let a, b, c, d, e, f be positive integers. Suppose that $S = a+b+c+d+e+f$ divides both $abc + def$ and $ab + bc + ca - de - ef - fd$. Prove that S is composite.

8. (USAMO 2002) Prove that any monic polynomial (a polynomial with leading coefficient 1) of degree n with real coefficients can be written as the average of two monic polynomials of degree n with n real roots.

9. (Iran TST 2010) Find all two-variable polynomials $P(x, y)$ such that for any real numbers a, b, c:
$$P(ab, c^2+1) + P(bc, a^2+1) + P(ca, b^2+1) = 0$$

10. (China TST 2007) Prove that for any positive integer n, there exists exactly one polynomial $P(x)$ of degree n with real coefficients, such that $P(0) = 1$ and $(x+1)(P(x))^2 - 1$ is an odd function. (A function $f(x)$ is odd if $f(x) = -f(-x)$ for all x).

2 Number Theory

By $\mathbb{Z}[x]$ we denote all the polynomials of one variable with integer coefficients. Arguably the most useful property when it comes to polynomials and integers is:

$$\boxed{\text{If } P(x) \in \mathbb{Z}[x], \text{ and } a, b \text{ are integers, then } (a-b) | (P(a) - P(b))}$$

Recall that polynomial in $\mathbb{Z}[x]$ is irreducible over the integers if it cannot be factored into two polynomials with integer coefficients.

Eisenstein's Criterion: *Let $P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in \mathbb{Z}[x]$ be a polynomial and p be a prime dividing $a_0, a_1, ..., a_{n-1}$, such that $p \nmid a_n$ and $p^2 \nmid a_0$. Then $P(x)$ is irreducible.*

Proof: Assume $P(x) = Q(x)R(x)$, where $Q(x) = b_k x^k + b_{k-1}x^{k-1} + ... + b_1 x + b_0, R(x) = c_l x^l + c_{l-1}x^{l-1} + ... + c_1 x + c_0$. Then $b_0 c_0$ is divisible by p but not p^2. Wolog $p|b_0, p \nmid c_0$. Since $p|a_1 = b_1 c_0 + b_0 c_1$ it follows that $p|b_1$. Since $p|a_2 = b_2 c_0 + b_1 c_1 + b_0 c_2$ it follows that $p|b_2$. By induction it follows that $p|b_k$ which implies that $p|a_n$, a contradiction.

Lemma [Schur] *Let $P(x) \in \mathbb{Z}[x]$ be a non-constant polynomial. Then there are infinitely many primes dividing at least one of the non-zero terms in the sequence $P(1), P(2), P(3), ...$*

Proof: Assume first that $P(0) = 1$. There exists an integer M such that $P(n) \neq 1$ for all $n > M$ (or else $P(x) - 1$ has infinitely many roots and therefore is constant). We also have $P(n!) \equiv 1 (\mod n!)$, and by taking arbitrarily large integers n we can generate arbitrarily large primes dividing $P(n!)$.

If $P(0) = 0$, the result is obvious. Otherwise consider $Q(x) = \dfrac{P(xP(0))}{P(0)}$ and apply the same line of reasoning to $Q(x)$; the result follows.

For polynomials in $\mathbb{Z}[x]$ it is often useful to work modulo a positive integer k. If $P(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ and k is a positive integer we call $\overline{P(x)} = \sum_{i=0}^{n} \overline{a_i} x^i$ the reduction of $P(x)$ (mod k), where $\overline{a_i} = a_i$ (mod k). Some useful facts about reduced polynomials:

1. Let $P(x), Q(x), R(x), S(x) \in \mathbb{Z}[x]$, such that $P(x) = (Q(x) + R(x))S(x)$. Then $\overline{P(x)} = (\overline{Q(x)} + \overline{R(x)})(\overline{S(x)})$.
2. Let p be a prime and $P(x) \in \mathbb{Z}[x]$. Then the factorization of $\overline{P(x)}$ is unique modulo p (more formally, in $\mathbb{F}_p[x]$ up to permutation.) Note that this result does not hold when p is not a prime. For example, $x = (2x+3)(3x+2)$ mod 6 if $x, 2x+3, 3x+2$ are prime.
   Also remember that all roots of $P(x)$ modulo p are in the set $\{0, 1, \ldots, p-1\}$.

2.1 Warm-Up

1. (a) Let p be a prime number. Prove that $P(x) = x^{p-1} + x^{p-2} + ... + x + 1$ is irreducible.
   (b) Prove Eisenstein's Criterion by considering a reduction modulo p.

2. (Iran 2007) Does there exist a sequence of integers $a_0, a_1, a_2, ...$ such that $\gcd(a_i, a_j) = 1$ for $i \neq j$, and for every positive integer n, the polynomial $\displaystyle\sum_{i=0}^{n} a_i x^i$ is irreducible?

3. (a) (Bezout) Let $P(x), Q(x)$ be polynomials with integer coefficients such that $P(x), Q(x)$ do not have any roots in common. Prove that there exist polynomials $A(x), B(x)$ and an integer N such that $A(x)P(x) + B(x)Q(x) = N$.
   (b) Let $P(x), Q(x)$ be monic non-constant irreducible polynomials with integer coefficients. For all sufficiently large n, $P(n)$ and $Q(n)$ have the same prime divisors. Prove that $P(x) \equiv Q(x)$.

2.2 Problems

1. (a) (USAMO 1974)Let a, b, c be three distinct integers. Prove that there does not exist a polynomial $P(x)$ with integer coefficients such that $P(a) = b, P(b) = c, P(c) = a$.
   (b) (IMO 2006) Let $P(x)$ be a polynomial of degree $n > 1$ with integer coefficients and let k be a positive integer. Let $Q(x) = P(P(\ldots P(P(x))\ldots))$, where the polynomial P is composed k times. Prove that there are at most n integers t such that $Q(t) = t$.

2. (Romania TST 2007) Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial of degree $n \geq 3$ with integer coefficients such that $P(m)$ is even for all even integers m. Furthermore, a_0 is even, and $a_k + a_{n-k}$ is even for $k = 1, 2, ..., n-1$. Suppose $P(x) = Q(x)R(x)$ where $Q(x), R(x)$ are polynomials with integer coefficients, $\deg Q \leq \deg R$, and all coefficients of $R(x)$ are odd. Prove that $P(x)$ has an integer root.

3. (USA TST 2010) Let $P(x)$ be a polynomial with integer coefficients such that $P(0) = 0$ and $\gcd(P(0), P(1), P(2), \ldots) = 1$. Prove that there are infinitely many positive integers n such that $\gcd(P(n) - P(0), P(n+1) - P(1), P(n+2) - P(2), \ldots) = n$.

4. (Iran TST 2004) Let $P(x)$ be a polynomial with integer coefficients such that $P(n) > n$ for every positive integer n. Define the sequence x_k by $x_1 = 1, x_{i+1} = P(x_i)$ for $i \geq 1$. For every positive integer m, there exists a term in this sequence divisible by m. Prove that $P(x) = x + 1$.

5. (China TST 2006) Prove that for any $n \geq 2$, there exists a polynomial $P(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ such that:

   (a) $a_0, a_1, ..., a_{n-1}$ all are non-zero.
   (b) $P(x)$ is irreducible.
   (c) For any integer x, $|P(x)|$ is not prime.

6. (Russia 2006) A polynomial $(x+1)^n - 1$ is divisible by a polynomial $P(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0$ of even degree k, such that all of its coefficients are odd integers. Prove that n is divisible by $k + 1$.

7. (USAMO 2006) For an integer m, let $p(m)$ be the greatest prime divisor of m. By convention, we set $p(\pm 1) = 1$ and $p(0) = \infty$. Find all polynomials f with integer coefficients such that the sequence $\{p\left(f\left(n^2\right)\right) - 2n\}_{n\geq 0}$ is bounded above. (In particular, $f\left(n^2\right) \neq 0$ for $n \geq 0$.)

8. Find all non-constant polynomials $P(x)$ with integer coefficients, such that for any relatively prime integers a, b, the sequence $\{f(an+b)\}_{n\geq 1}$ contains an infinite number of terms and any two of which are relatively prime.

9. (IMO SL 2009) Let $P(x)$ be a non-constant polynomial with integer coefficients. Prove that there is no function T from the set of integers into the set of integers such that the number of integers x with $T^n(x) = x$ is equal to $P(n)$ for every positive integer n, where T^n denotes the n-fold application of T.

10. (USA TST 2008) Let n be a positive integer. Given polynomial $P(x)$ with integer coefficients, define its signature modulo n to be the (ordered) sequence $P(1), \ldots, P(n)$ modulo n. Of the n^n such n-term sequences of integers modulo n, how many are the signature of some polynomial $P(x)$ if:

    (a) n is a positive integer not divisible by the square of a prime.
    (b) n is a positive integer not divisible by the cube of a prime.

3 Hints to Selected Problems

3.1 Algebra

2. Difference of squares.
3. Prove that for any complex root r of $P(x)$, we have $|r| > 1$.
4. Use Heron's formula to prove the square of the area is a rational number.
5. Look at the smallest and the largest numbers in S by absolute value. Use Vieta's thoerem.
7. The solution involves polynomials.
8. A polynomial has n real roots iff it changes sign $n+1$ times. Define one of the polynomials as $kQ(x)$ where $Q(x)$ has n roots and k is a constant.
9. Prove that $P(x, y)$ is divisible by $x^2(y-1)$.
10. Let $P(x) = Q(x) + R(x)$ where Q is an even function and R is an odd function.

3.2 Number Theory

2. Reduce modulo 2. Prove that $\deg R(x) = 1$.
3. Let $P(x) = x^k Q(x)$ with $Q(x) \neq 0$. Consider prime $n = p^k$ where p is prime.
4. Prove that $x_{k+1} - x_k | x_{k+2} - x_{k+1}$.
5. Reduce modulo 2.
6. Use Eisenstein's Criterion.
7. Look at the irreducibe factors of f. Prove they are of form $4x - k^2$.
8. What can you say about $\gcd(n, f(n))$?
9. For $k \in \mathbb{N}$, look at a_k, the number of integers x, such that k is the smallest integer for which $T^k(x) = x$.
10. First solve the problem if n is a prime.