Polynomials! (Winter Camp 2015)

James Rickards

Irreducibility Problems

A polynomial $f(x)$ with integer coefficients is called *reducible* if there exist non-constant polynomials $g(x), h(x)$ with integer coefficients such that $f(x) = g(x)h(x)$. It is *irreducible* otherwise.

Irreducibility problems are some of the most common number theoretic polynomial problems. There are only a few simple methods to deal with such problems, so in general you have to be creative. First of all:

Gauss's Lemma: Let $f(x)$ be a non-constant polynomial with integer coefficients. Then it is irreducible over the rational numbers if and only if it is irreducible over the integers.

In particular, this lemma allows us to basically ignore whether we are working with rationals or integers.

Eisenstein's Criterion: Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients, and let p be a prime number. If:
i) $p \mid a_i$ for $0 \leq i \leq n-1$
ii) $p \nmid a_n$
ii) $p^2 \nmid a_0$
Then $f(x)$ is irreducible.

Eisenstein's criterion is an excellent tool, however you often cannot directly apply it. Let a, b, c be rational numbers. Then Gauss's lemma imples that $f(x)$ is irreducible if and only if $cf(ax + b)$ is irreducible over the rationals. An integral part to some problems is figuring out good choices of a, b, c (often $a = c = 0$ and $b = \pm 1$).

Reduction modulo p: Let p be a prime, and $f(x)$ be a polynomial with integer coefficients so that p does not divide the leading coefficient. If $f(x)$ is reducible over the integers, then it is clearly reducible over the field modulo p. Therefore if you can show that $f(x)$ is irreducible modulo p, then $f(x)$ is irreducible over the integers.

Exercise: Find an integral polynomial $f(x)$ which is irreducible over the integers but reducible modulo p for every prime p.

When solving an irreducibility problem, try letting $f(x) = g(x)h(x)$ and then try to show that one of the two must be constant. In small degree cases the following is useful:

Rational Roots Test: Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients, and assume $\frac{p}{q}$ be a rational root with p, q being relatively prime. Then $p \mid a_0$ and $q \mid a_n$.

Note for degree 3 polynomials, $f(x)$ is irreducible if and only if it has no rational roots. If $f(x)$ is of degree 4, check it has no rational roots and write $f(x) = g(x)h(x)$ where g, h are quadratic; it is fairly simple to check whether this is possible or not.

Problems

1. Prove that the following polynomials are irreducible:
i) $x^5 + 2x^4 - 4x^3 + 4x^2 - 2x + 13$
ii) $x^5 - 32x^3 + 96x^2 - 64$

2. Let $n > 1$ be an integer, and let $f(x) = x^n + 5x^{n-1} + 3$. Prove that $f(x)$ is irreducible. (IMO 1993)

3. Let $f(x)$ be monic, irreducible, and $|f(0)|$ is not a perfect square. Prove that $f(x^2)$ is also irreducible. (Romania TST 2003)

4. Let p be a prime number, $n_1, \ldots, n_p$ positive integers, and let $d = \gcd(n_1, n_2, \ldots, n_p)$. Prove that the polynomial

$$\frac{x^{n_1} + x^{n_2} + \ldots + x^{n_p} - p}{x^d - 1}$$

is irreducible. (Romania TST 2010)

5. Let $a_1 \geq a_2 \geq \cdots \geq a_n > 0$ be positive integers. Show that $P(x) = x^n - a_1x^{n-1} - a_2x^{n-2} - \cdots - a_n$ is irreducible over the integers. (Yufei Zhao, Integer Polynomials Problem 17)

Root Problems

For this section, assume $f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0$ and it has roots $r_1, r_2, \cdots, r_n$.

By far the most useful result when dealing with roots is **Vieta's Formulas**. The easiest way to remember them is writing $f(x) = (x - r_1)(x - r_2)\cdots(x - r_n)$ and expanding out.

Many problems ask for properties of the roots, for example they are all real, all imaginary, all positive, etc. In this case it is useful to look at inequalities with $f(x)$, being careful that using $>$ or $<$ implies we are working with real numbers. Another useful idea is:

Descartes' Rule of Signs: Let $f(x)$ be a polynomial with real coefficients. Order the terms as usual, from highest exponent to lowest. Let d be the number of sign changes in the non-zero coefficients, then if f has r positive roots (counted with multiplicity), then $r \leq d$ and $r \equiv d \mod 2$.

If d is odd then this implies that a positive root exists, and $d = 1$ implies that exactly one positive root exists. You can repeat the test with $f(-x)$ to give an idea of how many negative roots may exist.

Finally, plugging in values of x is helpful because of:

Intermediate Value Theorem If $g(x)$ is a continuous function that sends the reals to reals (any polynomial is continuous), then if a, b are real numbers with $g(a) < 0 < g(b)$ then there exists x between a and b such that $g(x) = 0$.

In particular, since $deg(f) = n$, if we can find real numbers $a_1 < a_2 < ... < a_{n+1}$ such that $f(a_i)$ and $f(a_{i+1})$ have opposite sign for all $1 \leq i \leq n$, then we have found n distint real roots, so all the roots are real!

Exercise: Show that for each positive integer n, all the roots of the polynomial

$$\textstyle\sum_{k=0}^{n} 2^{k(n-k)}x^k$$

are real numbers. (Putnam 2014)

Problems

1. The roots of the equation

$$x^3 - 3ax^2 + bx + 18c = 0$$

form a non-constant arithmetic progression, and the roots of

$$x^3 + bx^2 + x - c^3 = 0$$

form a non-constant geometric progression. Given that a, b, c are all real numbers, find all possible positive integral values of a and b. (India Regional MO 2014)

2. Let $x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 = 0$ be a polynomial with real coefficients such that $0 \leq a_0 \leq a_1 \leq a_2 \leq \cdots \leq a_{n-1} \leq 1$. If λ is a root with $|\lambda| \geq 1$ then $\lambda^{n+1} = 1$. (China MO 1992)

3. Let $P(x)$ be a polynomial of degree 2012 with real coefficients satisfying:

$$P(a)^3 + P(b)^3 + P(c)^3 \geq 3P(a)P(b)P(c)$$

for all reals a, b, c such that $a + b + c = 0$. Is it possible for $P(x)$ to have exactly 2012 distinct real roots? (Serbia TST 2012)

4. Let n be a positive even integer, and let $c_1, c_2, \ldots, c_{n-1}$ be real numbers satisfying

$$\textstyle\sum_{i=1}^{n-1} |c_i - 1| < 1$$

Prove that

$$2x^n - c_{n-1}x^{n-1} + c_{n-2}x^{n-2} - \cdots - c_1 x^1 + 2$$

has no real roots. (USA January TST 2014)

5. Find all real coefficient polynomials $f(x)$ which satisfy the following: i) $f(x) = a_0x^{2n} + a_2x^{2n-2} + \cdots + a_{2n-2}x^2 + a_{2n}, a_0 > 0$

ii) $\sum_{j=0}^{n} a_{2j}a_{2n-2j} \leq \left(\begin{array}{c} 2n \\ n \end{array} \right) a_0 a_{2n}$

iii) All the roots of $f(x)$ are imaginary numbers with no real part. (China TST 1997)

Other polynomial problems

1. For a polynomial $p(x)$, let $p^n(x) = p(p(\cdots p(x)\cdots))$ where p is composed n times. Prove that the polynomial

$$p^{2003}(x) - 2p^{2002}(x) + p^{2001}(x)$$

is divisible by $p(x) - x$ (Serbia/Montenegro TST 2003)

2. A nonconstant polynomial f with integer coefficients has the property such that for each prime p, there exists a prime q and integer m such that $f(p) = q^m$. Prove that $f(x) = x^n$ for some positive integer n. (Romania TST 2010)

3. We call polynomials $A(x) = a_nx^n + \ldots + a_1x + a_0$ and $B(x) = b_nx^n + \ldots + b_1x + b_0$ similar if:
i) $n = m$
ii) There is a permutation π of the set $\{0, 1, \ldots, n\}$ such that $b_i = a_{\pi(i)}$ for each $i \in \{0, 1, \ldots, n\}$
Let $P(x)$ and $Q(x)$ be similar polynomials with integer coefficients. Given $P(16) = 3^{2012}$, find the smallest possible value of $|Q(3^{2012})|$. (Serbia TST 2013)

4. Prove that for any positive integer n, there exists precicely one degree n polynomial $f(x)$ such that $f(0) = 1$, and $(x + 1)[f(x)]^2 - 1$ is an odd function. (China TST 2007 Quiz 1)