R-VI. Polynomials

Po-Shen Loh
1 July 2004

1 Warm-Ups

1. Consider the cubic equation $ax^3 + bx^2 + cx + d = 0$. The roots are

$$x = -\frac{b}{3a} + \frac{1}{3} \sqrt[3]{\frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}} - \sqrt[3]{\frac{-b^3}{27a^3} + \frac{bc}{6a^2} + \frac{d}{2a}}$$

Prove that no such general formula exists for a quintic equation.

2 Theory

Thanks to Elgin Johnston (1997) for these theorems.

**Rational Root Theorem** Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ be a polynomial with integer coefficients. Then any rational solution $r/s$ (expressed in lowest terms) must have $r|a_0$ and $s|a_n$.

**Descartes’s Rule of Signs** Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ be a polynomial with real coefficients. Then the number of positive roots is equal to $N - 2k$, where $N$ is the number of sign changes in the coefficient list (ignoring zeros), and $k$ is some nonnegative integer.

**Eisenstein’s Irreducibility Criterion** Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ be a polynomial with integer coefficients and let $q$ be a prime. If $q$ is a factor of each of $a_n - 1, a_{n-2}, \ldots, a_0$, but $q$ is not a factor of $a_n$, and $q^2$ is not a factor of $a_0$, then $p(x)$ is irreducible over the rationals.

**Einstein’s Theory of Relativity** Unfortunately, this topic is beyond the scope of this program.

**Gauss’s Theorem** If $p(x)$ has integer coefficients and $p(x)$ can be factored over the rationals, then $p(x)$ can be factored over the integers.

**Lagrange Interpolation** Suppose we want a degree-$n$ polynomial that passes through a set of $n+1$ points: $\{(x_i, y_i)\}_{i=0}^n$. Then the polynomial is:

$$p(x) = \sum_{i=0}^n \frac{y_i \text{ normalization}}{(x - x_0)(x - x_1) \cdots (x - x_i)}$$

where the $i$-th “normalization” factor is the product of all the terms $(x_i - x_j)$ that have $j \neq i$. 

1
3 Problems

Thanks to Elgin Johnston (1997) for most of these problems.

1. (Crux Math., June/July 1978) Show that \( n^4 - 20n^2 + 4 \) is composite when \( n \) is any integer.

Solution: Factor as difference of two squares. Prove that neither factor can be \( \pm 1 \).

2. (St. Petersburg City Math Olympiad 1998/14) Find all polynomials \( P(x, y) \) in two variables such that for any \( x \) and \( y, P(x + y, y - x) = P(x, y) \).

Solution: Clearly constant polynomials work. Also, \( P(x, y) = P(x + y, y - x) = P(2y, -2x) = P(16x, 16y) \). Suppose we have a nontrivial polynomial. Then on the unit circle, it is bounded because we can just look at the fixed coefficients. Yet along each ray \( y = tx \), we get a polynomial whose translate has infinitely many zeros, so it must be constant. Hence \( P \) is constant along all rays, implying that \( P \) is bounded by its max on the unit circle, hence bounded everywhere. Now suppose maximum degree of \( y \) is \( N \). Study the polynomial \( P(z^{N+1}, z) \). The leading coeff of this is equal to the leading coeff of \( P(x, y) \) when sorted with respect to \( x \) as more important. Since the \( z \)-poly is also bounded everywhere, it too must be constant, implying that the leading term is a constant.

3. (Putnam, May 1977) Determine all solutions of the system

\[
\begin{align*}
x + y + z &= w \\
\frac{1}{x} + \frac{1}{y} + \frac{1}{z} &= \frac{1}{w}.
\end{align*}
\]

Solution: Given solutions \( x, y, z \), construct 3-degree polynomial \( P(t) = (t - x)(t - y)(t - z) \). Then \( P(t) = t^3 - wt^2 + At - Aw = (t^2 + A)(t - w) \). In particular, roots are \( w \) and a pair of opposites.

4. (Crux Math., April 1979) Determine the triples of integers \((x, y, z)\) satisfying the equation

\[ x^3 + y^3 + z^3 = (x + y + z)^3. \]

Solution: Move \( z^3 \) to RHS and factor as \( x^3 \pm y^3 \). We get \((x + y) = 0 \) or \((y + z)(z + x) = 0 \). So two are opposites.

5. (USSR Olympiad) Prove that the fraction \((n^3 + 2n)/(n^4 + 3n^2 + 1)\) is in lowest terms for every positive integer \( n \).

Solution: Use Euclidean algorithm for GCD. \((n^3 + 2n)n = n^4 + 2n^2, \) so difference to denominator is \( n^3 + 1 \). Yet that’s relatively prime to \( n(n^2 + 2) \).

6. (Po, 2004) Prove that \( x^4 - x^3 - 3x^2 + 5x + 1 \) is irreducible.

Solution: Eisenstein with substitution \( x \mapsto x + 1 \).

7. (Canadian Olympiad, 1970) Let \( P(x) \) be a polynomial with integral coefficients. Suppose there exist four distinct integers \( a, b, c, d \) with \( P(a) = P(b) = P(c) = P(d) = 5 \). Prove that there is no integer \( k \) with \( P(k) = 8 \).

Solution: Drop it down to 4 zeros, and check whether one value can be 3. Factor as \( P(x) = (x - a)(x - b)(x - c)(x - d)R(x) \); then substitute \( k \). 3 is prime, but we’ll get at most two \( \pm 1 \) terms from the \((x - a)\) product.

8. (Monthly, October 1962) Prove that every polynomial over the complex numbers has a nonzero polynomial multiple whose exponents are all divisible by \( 10^9 \).

Solution: Factor polynomial as \( a(x - r_1)(x - r_2) \cdots (x - r_n) \). Then the desired polynomial is \( a(x^{10} - r_1^{10}) \cdots (x^{10} - r_n^{10}) \), where \( P = 10^9 \). Each factor divides the corresponding factor.
9. (Elgin, MOP 1997) For which $n$ is the polynomial $1 + x^2 + x^4 + \cdots + x^{2n-2}$ divisible by the polynomial $1 + x + x^2 + \cdots + x^{n-1}$?

**Solution:** Observe:

\[
(x^2 - 1)(1 + x^2 + x^4 + \cdots + x^{2n-2}) = x^{2n} - 1
\]
\[
(x - 1)(1 + x + x^2 + \cdots + x^{n-1}) = x^n - 1
\]
\[
(x + 1)(1 + x^2 + x^4 + \cdots + x^{2n-2}) = (x^n + 1)(1 + x + x^2 + \cdots + x^{n-1}).
\]

So if the quotient is $Q(x)$, then $Q(x)(x + 1) = x^n + 1$. This happens iff $-1$ is a root of $x^n + 1$, which is iff $n$ is odd.

10. (Czech-Slovak Match, 1998/1) A polynomial $P(x)$ of degree $n \geq 5$ with integer coefficients and $n$ distinct integer roots is given. Find all integer roots of $P(P(x))$ given that $0$ is a root of $P(x)$.

**Solution:** Answer: just the roots of $P(x)$. Proof: write $P(x) = x(x-r_1)(x-r_2)\cdots(x-r_N)$. Suppose we have another integer root $r$; then $r(r-r_1)\cdots(r-r_N) = r_k$ for some $k$. Since degree is at least 5, this means that we have $2r(r-r_k)$ dividing $r_k$. Simple analysis shows that $r$ is between 0 and $r_k$; more analysis shows that we just need to defuse the case of $2ab \mid a+b$. Assume $a \leq b$. Now if $a = 1$, only solution is $b = 1$, but then we already used ±1 in the factors, so we actually have to have $12r(r-r_k)$ dividing $r_k$, no good. If $a > 1$, then $2ab > 2b \geq a+b$, contradiction.

11. (Hungarian Olympiad, 1899) Let $r$ and $s$ be the roots of

\[ x^2 - (a+d)x + (ad-bc) = 0. \]

Prove that $r^3$ and $s^3$ are the roots of

\[ y^2 - (a^3+d^3+3abc+3bcd)y + (ad-bc)^3 = 0. \]

Hint: use Linear Algebra.

**Solution:** $r$ and $s$ are the eigenvalues of the matrix

\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix}
\]

The $y$ equation is the characteristic polynomial of the cube of that matrix.

12. (Hungarian Olympiad, 1981) Show that there is only one natural number $n$ such that $2^8 + 3^{11} + 2^n$ is a perfect square.

**Solution:** $2^8 + 3^{11} = 48^2$. So, need to have $2^n$ as difference of squares $N^2 - 48^2$. Hence $(N + 48)$, $(N - 48)$ are both powers of 2. Their difference is 96. Difference between two powers of 2 is of the form $2^M(2^N - 1)$. Uniquely set to $2^7 - 2^5$.

13. (MOP 97/9/3) Let $S = \{s_1, s_2, \ldots, s_n\}$ be a set of $n$ distinct complex numbers, for some $n \geq 9$, exactly $n - 3$ of which are real. Prove that there are at most two quadratic polynomials $f(z)$ with complex coefficients such that $f(S) = S$ (that is, $f$ permutes the elements of $S$).

14. (MOP 97/9/1) Let $P(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ be a nonzero polynomial with integer coefficients such that $P(r) = P(s) = 0$ for some integers $r$ and $s$, with $0 < r < s$. Prove that $a_k \leq -s$ for some $k$. 

3