Lecture 8 — Polynomials

Holden Lee and Josh Nichols-Barrer

1/14/11

1 Irreducible Polynomials

1. Let $n \geq 1$ and let $f(x)$ be a degree-n integer polynomial such that for $2n-1$ distinct integer values of x, the value of $f(x)$ is plus or minus a prime. Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$.
2. (IMO 1992?) Show that for each $n > 1$ the polynomial $x^n + 5x^{n-1} + 3$ is irreducible in $\mathbb{Z}[x]$.
3. Prove that the polynomial
$$f(x) = \frac{x^n + x^m - 2}{x^{\gcd(m,n)} - 1}$$
is irreducible over $\mathbb{Q}$ for all integers $n > m > 0$.
4. Let a be an integer not divisible by 5. Show that $x^5 - x - a$ is irreducible in $\mathbb{Z}[x]$.
5. Let m, n be integers with $m > 0$ and $5 \mid\mid n$ (in other words, $5|n$ and no larger power of 5 divides n). Show that $(x^4 + x^2 - 6)^m + n$ is irreducible in $\mathbb{Q}[x]$.

FROM JOSH

1. Show that the polynomial $x^{2^n} + 1$ is irreducible in $\mathbb{Z}[x]$.
2. Show that the polynomial $x^n - 1998$ is irreducible in $\mathbb{Z}[x]$.
3. Show that the polynomial $x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible in $\mathbb{Z}[x]$.
4. Let m and n be positive integers. Show that the polynomial $x^m + y^n - z^n$ is irreducible in $\mathbb{Z}[x, y, z]$.
5. Let $p \equiv 3 \bmod 4$ be a prime number and let a and b be integers such that $p|a$ and $p||b - 1$. Show that the polynomial $f(x) = x^{2p} + ax + b$ is irreducible in $\mathbb{Z}[x]$.
6. Let $a_1, a_2, \ldots, a_n$ be distinct integer numbers. Show that the polynomial
$$(x - a_1)(x - a_2) \cdots (x - a_n) - 1$$
is irreducible in $\mathbb{Z}[x]$.
7. Let $a_1, a_2, \ldots, a_n$ be distinct integer numbers. Show that the polynomial
$$(x - a_1)^2(x - a_2)^2 \cdots (x - a_n)^2 + 1$$
is irreducible in $\mathbb{Z}[x]$.

2 Blah

(C) Divisibility, GCD, and Irreducibility

Theorem 2.1 (Bézout)**:** Let K be a field and $f, g \in K[x]$. There exist polynomials $u, v \in K[x]$ so that $uf + vg = \gcd(f, g)$.

Theorem 2.2 (Chinese Remainder Theorem)**:** If polynomials $Q_1, \dots, Q_n \in K[x]$ are relatively prime, then the system $P \equiv R_i \pmod{Q_i}, 1 \le i \le n$ has a unique solution modulo $Q_1 \cdots Q_n$.

1.

3 Algebraic Numbers

Let R be an integral domain and K its fraction field, and L a field containing K. A number a in L is said to be *algebraic* over K if it satisfies a nontrivial polynomial equation with coefficients in K. The number is an *algebraic integer* if this polynomial can be chosen to be monic with coefficients in R. Unless otherwise specified, we work over $\mathbb{Z}$ and $\mathbb{Q}$.

Theorem 3.1 (Fundamental Theorem of Symmetric Polynomials)**:** Let R be a ring (say, $\mathbb{Z}$), and $f(x_1, \dots, x_n)$ a polynomial symmetric in all its variables. Then there exists a unique polynomial g such that

$$f(x_1, \dots, x_n) = g(s_1, \dots, s_n)$$

where $s_j = \sum_{1 \le i_1 < \dots < i_j \le n} x_{i_1} \cdots x_{i_j}$ are the elementary symmetric polynomials.

Proof. Induct on the degree of f and the number of variables. □

Theorem 3.2: The *minimal (irreducible) polynomial* p of $a \in L$ is the monic polynomial of minimal degree in $K[x]$ that has a as a root. Any polynomial in $K[x]$ that has a as a root is a multiple of p.

Proof. The polynomials in $K[x]$ that have a as a root form an ideal. $K[x]$ is a principal ideal domain, so is generated by one element. □

The degree of the minimal polynomial of a over K is also called as the degree of a over K. This is the dimension of $K(a)$ as a vector space over K; i.e. it takes d elements $1, a, \dots, a^{d-1}$ to generate $K(a)$ over K. The zeros of the minimal polynomial of a are called the *conjugates* of a.

Theorem 3.3: The numbers in L that are algebraic over K form a field. The algebraic integers over R form a ring.

Proof. We need to show that if a, b are algebraic numbers and $k \in K$ then so are ka, $a + b$, ab, and $1/a$.

Proof 1 Let p, q be the minimal polynomials of a, b, let $a_1, \dots, a_k$ be the conjugates of a and $b_1, \dots, b_l$ be the conjugates of b. Then the coefficients of

$$\prod_i (x - ka_i), \prod_{i,j} (x - (a_i + b_j)), \prod_{i,j} (x - (a_i b_j)), \prod_i (x - (1/a_i))$$

are symmetric in the a_i and symmetric in the b_j so by the Fundamental Theorem can be written in terms of the elementary symmetric polynomials in the a_i and in the b_j. But

by Vieta's Theorem these are expressible in terms of the coefficients of p, q, which are in K. Hence these polynomials have coefficients in K and have $ka, a+b, ab, 1/a$ as roots, as desired. If a, b are algebraic integers so are $ra, r \in R$, $a+b$, ab by noting that the coefficients of the first three polynomials are in R and the polynomials are monic.
Proof 2 Consider the field generated by a, b over K. It is spanned by $a^i b^j$ for $0 \le i < k$ and $0 \le j < l$, and hence is finite-dimensional as a vector space. Hence for any c in this field, $1, c, c^2, \ldots$ must satisfy a linear dependency relation, i.e. c is algebraic. (The proof for algebraic integers is similar but more involved.) $\square$

Note that the first proof gives us the additional fact that the conjugates of $a+b$ are among the $a_i + b_j$ and the conjugates of ab are among the $a_i b_j$.
Theorem 3.4 (Rational Roots Theorem)**:** The possible rational roots of $a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ are $\frac{p}{q}$ where $p|a_0$ and $q|a_n$. Thus all algebraic integers that are rational are also in $\mathbb{Z}$ (which we will call rational integers).

3.1 Problems

1. Suppose that $f \in \mathbb{Z}[x]$ is irreducible and has a root of absolute value at least $\frac{3}{2}$. Prove that if α is a root of f then $f(\alpha^3 + 1) \neq 0$.

2. Let $a_1, \ldots, a_n$ be algebraic integers with degrees $d_1, \ldots, d_n$. Let $a_1', \ldots, a_n'$ be the conjugates of $a_1, \ldots, a_n$ with greatest absolute value. Let $c_1, \ldots, c_n$ be integers. Prove that if the LHS of the following expression is not zero, then

$$|c_1 a_1 + \ldots + c_n a_n| \geq \left(\frac{1}{|c_1 a_1'| + \cdots + |c_n a_n'|} \right)^{d_1 d_2 \cdots d_n - 1}.$$

For example,

$$|c_1 + c_2\sqrt{2} + c_3\sqrt{3}| \geq \left(\frac{1}{|c_1| + |2c_2| + |2c_3|} \right)^3.$$

3. Let p be a prime and consider k pth roots of unity whose sum is not 0. Prove that the absolute value of their sum is at least $\frac{1}{k^{p-2}}$.

4 Cyclotomic and Chebyshev Polynomials

The nth cyclotomic polynomial is defined by

$$\Phi_n(x) = \prod_{0 \le j < n, \gcd(j,n)=1} (x - e^{\frac{2\pi i j}{n}})$$

Equivalently, it can be defined by the recurrence $\Phi_0(x) = 1$ and

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{m|n, m<n} \Phi_m(x)}.$$

Hence, it has integer coefficients.
Theorem 4.1: The cyclotomic polynomials are irreducible over $\mathbb{Q}[x]$.

Proof. We need the following lemma:

Suppose ω is a primitive nth root of unity, and that its minimal polynomial is $g(x)$. Let p be a prime not dividing n. Then ω^p is a root of $g(x) = 0$.

Since $\Phi_n(\omega) = 0$, we can write $\Phi_n = fg$. If $g(\omega^p) \neq 0$ then $f(\omega^p) = 0$. Since ω is a zero of $f(x^p)$, $f(x^p)$ factors as

$$f(x^p) = g(x)h(x)$$

for some polynomial $h \in \mathbb{Z}[x]$.

Now, in $\mathbb{Z}/p\mathbb{Z}[x]$ note $(a_1 + \ldots + a_k)^p = a_1^p + \ldots + a_k^p$ ($\Phi : a \to a^p$ is a homomorphism in $\mathbb{Z}/p\mathbb{Z}[x]$ since $(P+Q)^p = P^p + Q^p$ by the binomial theorem.). Hence

$$g(x)h(x) \equiv f(x^p) \equiv f(x)^p \pmod{p}.$$

Hence $f(x)$ and $g(x)$ share a factor modulo p. However, the derivative of $x^n - 1$ modulo p is $nx^{n-1} \neq 0$, showing that $x^n - 1$ has no repeated irreducible factor modulo p; hence Φ_n has no repeated factor modulo p. Since $\Phi_n = fg$, this produces a contradiction.

Therefore $g(\omega^p) = 0$, as needed.

Any primitive nth root is in the form ω^k for k relatively prime to n. Writing the prime factorization of k as $p_1 \cdots p_m$, we get by the lemma that $\omega^{p_1}, \omega^{p_1 p_2}, \ldots, \omega^{p_1 \cdots p_m}$ are all roots of g. Hence g contains all primitive nth roots of unity as roots, and $\Phi_n = g$ is irreducible. □

Application: Special case of Dirichlet's Theorem: Given n there are infinitely many primes $p \equiv 1 \pmod{n}$.

The Chebyshev polynomials are defined by the recurrence $T_0(x) = 1, T_1(x) = x, T_{i+1}(x) = 2xT_i(x) - T_{i-1}(x)$ for $i \geq 1$. They satisfy

$$T_n(\cos\theta) = \cos n\theta$$

since $\cos((n+1)\theta) = 2\cos\theta\cos n\theta - \cos(n-1)\theta$. Furthermore,

$$T_n\left(\frac{1}{2}\left(x + \frac{1}{x}\right)\right) = \frac{1}{2}\left(x^n + \frac{1}{x^n}\right).$$

The roots of $T_n(x)$ are $\cos\left(\frac{\pi}{n} + \frac{2\pi k}{n}\right), 0 \leq k < n$.

Problems E

1. Let p be a prime. Prove that any equiangular p-gon with rational side lengths is regular.

2. Suppose P is polynomial of degree at most 7 so that

$$P\left(\frac{\sqrt{2}+\sqrt{6}}{4}\right) = -\frac{\sqrt{6}-\sqrt{2}}{4}$$
$$P\left(\frac{\sqrt{3}}{2}\right) = -\frac{\sqrt{3}}{2}$$
$$P\left(\frac{1}{2}\right) = \frac{1}{2}$$
$$P\left(\frac{\sqrt{6}-\sqrt{2}}{4}\right) = -\frac{\sqrt{2}+\sqrt{6}}{4}$$
$$P\left(-\frac{\sqrt{2}+\sqrt{6}}{4}\right) = \frac{\sqrt{6}-\sqrt{2}}{4}$$
$$P\left(-\frac{\sqrt{3}}{2}\right) = \frac{\sqrt{3}}{2}$$
$$P\left(-\frac{1}{2}\right) = -\frac{1}{2}$$
$$P\left(-\frac{\sqrt{6}-\sqrt{2}}{4}\right) = \frac{\sqrt{2}+\sqrt{6}}{4}$$

   Find $P(5/4)$.

3. (IMO) The sequence of polynomials $f_n(x)$ is defined as follows:

$$f_0(x) = x \text{ and } f_n(x) = f_{n-1}(x)^2 - 2.$$

   Show that for all positive integers n, the equation $f_n(x) = x$ has all real distinct roots.

4. (Komal) Prove that there exists a positive integer n so that any prime divisor of $2^n - 1$ is smaller that $2^{\frac{n}{1993}} - 1$.

5. Find all rational $p \in [0, 1]$ such that $\cos p\pi$ is...
   (a) rational
   (b) the root of a quadratic polynomial with rational coefficients

6. (China) Prove that there are no solutions to $2\cos p\pi = \sqrt{n+1} - \sqrt{n}$ for rational p rational and positive integer n.

7. (TST 2007/3) Let θ be an angle in the interval $(0, \pi/2)$. Given that $\cos\theta$ is irrational and that $\cos k\theta$ and $\cos[(k+1)\theta]$ are both rational for some positive integer k, show that $\theta = \pi/6$.

8. (Chebyshev) Let $p(x)$ be a real polynomial of degree $n \geq 1$ with leading coefficient 1. Then

$$\max_{-1\leq x\leq 1} |p(x)| \geq \frac{1}{2^{n-1}}.$$

9. Prove that $\cos\frac{\pi}{4n}\cdot\cos\frac{3\pi}{4n}\cdots\cos\frac{(2n-1)\pi}{4n}=\frac{1}{2^{n-\frac{1}{2}}}$.

(F) Polynomials in Number Theory

- (Lagrange) A polynomial of degree n over a field can have at most n zeros.
- To evaluate a sum or product it may be helpful to find a polynomial with those terms as zeros and use Vieta's relations.

  Theorem 4.2: Let $r_1,\ldots,r_n$ be the roots of $\sum_{i=0}^n a_i x^i$, and let

  $$s_j=\sum_{1\le i_1<\ldots<i_j\le n} r_{i_1}\cdots r_{i_j}.$$

  Then $s_j=(-1)^j\frac{a_{n-j}}{a_n}$.

1. (Wolstenholme) Prove that $\binom{pa}{pb}\equiv\binom{a}{b}\pmod{p^3}$ for prime $p\ge 5$.
2. Prove that for prime $p\ge 5$,

   $$p^2|(p-1)!\left(1+\frac{1}{2}+\cdots+\frac{1}{p-1}\right).$$

3. (APMO 2006/3) Prove that for prime $p\ge 5$, $\binom{p^2}{p}\equiv p\pmod{p^5}$.
4. (ISL 2005/N3) Let a,b,c,d,e,f be positive integers. Suppose that the sum $S=a+b+c+d+e+f$ divides both $abc+def$ and $ab+bc+ca-de-ef-fd$. Prove that S is composite.
5. (China TST 2009/3) Prove that for any odd prime p, the number of positive integers n satisfying $p\mid n!+1$ is less than or equal to $cp^{\frac{2}{3}}$, where c is a constant independent of p.
6. (TST 2002/2) Let p be a prime number greater than 5. For any positive integer x, define

   $$f_p(x)=\sum_{k=1}^{p-1}\frac{1}{(px+k)^2}.$$

   Prove that for all positive integers x and y the numerator of $f_p(x)-f_p(y)$, when written in lowest terms, is divisible by p^3.