Polynomial Problems

(A) Values and Roots

- Get something in the form $Q(x) = 0$ and factor based on roots. Plug in a value to get the leading coefficient. Or "guess" a polynomial satisfying the equations.

- Lagrange interpolation

  Theorem 1. Given $n+1$ points $(x_0, y_0), \ldots, (x_n, y_n)$ with distinct x-coordinates, there exists exactly one polynomial f of degree at most n so that $f(x_i) = y_i$ for $i = 0, 1, \ldots, n$. This polynomial is given by the following:

  $$P(x) = \sum_{i=0}^{n} \left[y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j} \right].$$

- Over a field, a polynomial of degree at most n that is zero for $n+1$ values of x is identically 0. Two polynomials of degree at most n that are equal for $n+1$ values of x are identically equal. A polynomial of degree n can have at most n roots.

- If $(x-a)^n | f$ then $(x-a)^{n-1} | f'$.

Problems A

1. A polynomial P of degree n satisfies $P(x) = \frac{x}{x+1}$ for $x = 0, 1, \ldots, n$. Find $P(n+1)$.

2. Let $r \neq 0$ be a real number. A polynomial P of degree n satisfies $P(x) = r^x$ for $x = 0, 1, \ldots, n$. Find $P(n+1)$.

3. n points $Q_1, \ldots, Q_n$ are equally spaced on a circle of radius 1 centered at O. Point P is on ray OQ_1 so that $OP = 2$. Find the product

   $$\prod_{k=1}^{n} PQ_i$$

   in closed form, in terms of n.

4. (AwesomeMath Team Contest 2010) Let $n \geq 2$. How many polynomials $Q(x)$ of degree at most $n-1$ are there such that

   $$x(x-1)\cdots(x-n)Q(x) + x^2 + 1$$

   is the square of a polynomial?

5. (APMO 2009/2) Let a_1, a_2, a_3, a_4, a_5 be real numbers satisfying the following equations:

   $$\frac{a_1}{k^2+1} + \frac{a_2}{k^2+2} + \frac{a_3}{k^2+3} + \frac{a_4}{k^2+4} + \frac{a_5}{k^2+5} = \frac{1}{k^2}$$

   for $k = 1, 2, 3, 4, 5$. Find the value of $\frac{a_1}{37} + \frac{a_2}{38} + \frac{a_3}{39} + \frac{a_4}{40} + \frac{a_5}{41}$.

6. Let $r \geq 3$. Prove that there does not exists a real polynomial of degree at most n so that $|p(x) - r^x| < 1$ for $x = 0, 1, \ldots, n+1$.

7. (UM 2002/3) Imagine ducks as points in a plane. Three ducks are said to be in a row if a straight line passes through all three ducks. Three ducks, Huey, Dewey, and Louie, each waddle along a different straight line in the plane, each at his own constant speed. Although their paths may cross, the ducks never bump into each other. Prove that if at three separate times the ducks are in a row, then they are always in a row.

8. (IMC 2008/B4) Let $f(x), g(x)$ be nonconstant polynomials with integer coefficients such that $g(x)$ divides $f(x)$. Prove that if the polynomial $f(x) = 2008$ has at least 81 distinct integer roots, then the degree of $g(x)$ is greater than 5.

9. (USAMO 2002/3) Prove that any monic polynomial of degree n with real coefficients is the average of two monic polynomials of degree n with n real zeros.

10. (Putnam 1956) The nonconstant polynomials $f(z)$ and $g(z)$ with complex coefficients have the same set of numbers for their zeros but possibly with different multiplicities. The same is true of the polynomials $f(z) + 1$ and $g(z) + 1$. Prove that $f(z) = g(z)$. (Hint: take derivatives)

11. (Bézout bound) Let $f(x, y), g(x, y) \in \mathbb{C}[x, y]$. Prove that either f, g have a constant nonzero factor, or they have finitely many zeros (x, y) in common. (Hard: They have at most $\deg(f)\deg(g)$ common zeros.)

(B) Arithmetic Properties

Theorem 2. If P has integer coefficients, then $a - b \mid P(a) - P(b)$ for all integers a, b.

1. Let P be a nonconstant polynomial with integer coefficients. Prove that there is an integer x so that $P(x)$ is composite.

2. (USAMO 1974/1) $P(x)$ is a polynomial with integral coefficients. If a, b, c are integers so that $P(a) = b, P(b) = c, P(c) = a$, prove that $a = b = c$.

3. (IMO 2006/5) Let $P(x)$ be a polynomial of degree $n > 1$ with integer coefficients and let k be a positive integer. Consider the polynomial

$$Q(x) = \underbrace{P(P(\cdots P(P}_{k \text{ times}}(x)))).$$

   Prove that there are at most n integers such that $Q(t) = t$.

4. (Helpful for the next few problems) Let $f(x) \in R[x]$, and let $p_0, p_1, \ldots$ be a sequence of polynomials whose leading coefficients $u_0, u_1, \ldots$ are units, and $\deg(p_i) = i$. Show that f can be uniquely written in the form

$$f(x) = a_n p_n(x) + \ldots + a_1 p_1(x) + a_0 p_0(x).$$

   In particular, this is true for $p_i(x) = x^{\underline{i}} = x(x-1)\cdots(x-i+1)$.

5. (Helpful for the next few problems) Let $f(x) \in \mathbb{C}[x]$. Show that the following are equivalent:

   (a) For every $x \in \mathbb{Z}$, $f(x) \in \mathbb{Z}$.

   (b) For n consecutive integers x, where n is the degree of f, $f(x) \in \mathbb{Z}$.

   (c) There are $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ with
   $$f(x) = a_n\binom{x}{n} + a_{n-1}\binom{x}{n-1} + \cdots + a_0\binom{x}{0}.$$

   (Note $\binom{x}{n}$ is defined as $\frac{x^{\underline{n}}}{n!}$.) Prove that if $f(x)$ is a polynomial of degree n that takes on integer values for $n+1$ consecutive integer values of x, then $f(m)$ is an integer for all $m \in \mathbb{Z}$.

6. (MOSP 2001) Let f be a polynomial with rational coefficients such that $f(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. Prove that for any integers m, n, the number
   $$\operatorname{lcm}[1, 2, \ldots, \deg(f)] \cdot \frac{f(m) - f(n)}{m - n}$$
   is an integer.

7. (USAMO 1995/4) Suppose $q_0, q_1, q_2, \ldots$ is an infinite sequence of integers satisfying the following two conditions:

   (a) $m - n$ divides $q_m - q_n$ for $m > n \geq 0$,

   (b) there is a polynomial P such that $|q_n| < P(n)$ for all n.

   Prove that there is a polynomial Q such that $q_n = Q(n)$ for each n.

8. (TST 2007/6) For a polynomial $P(x)$ with integer coefficients, $r(2i-1)$ (for $i = 1, 2, 3, \ldots, 512$) is the remainder obtained when $P(2i-1)$ is divided by 1024. The sequence
   $$(r(1), r(3), \ldots, r(1023))$$
   is called the *remainder sequence* of $P(x)$. A remainder sequence is called *complete* if it is a permutation of $(1, 3, 5, \ldots, 1023)$. Prove that there are no more than 2^{35} different complete remainder sequences.

9. (TST 2008/9) Let n be a positive integer. Given an integer coefficient polynomial $f(x)$ define its *signature modulo* n to be the ordered sequence $f(1), \ldots, f(n)$ modulo n. Of the n^n such n-term sequences of integers modulo n, how many are the signature of some polynomial $f(x)$ if n is a positive integer not divisible by the cube of a prime? (Easier: if n is not divisible hy the square of a prime)

10. (variant of TST 2005/3) For a positive integer n, let S denote the set of polynomials $P(x)$ of degree n with positive integer coefficients not exceeding $n!$. A polynomial $P(x)$ in set S is called *fine* if for any positive integer k, the sequence

$P(1), P(2), P(3), \ldots$ contains infinitely many integers relatively prime to k. Prove that the proportion of fine polynomials is at most

$$\prod_{\text{prime } p \leq n} \left(1 - \frac{1}{p^p}\right).$$

(Original statement: Prove that between 71% and 75% of the polynomials in the set S are fine.)

(C) Divisibility, GCD, and Irreducibility

Theorem 3 (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 4 (Chinese Remainder Theorem). If polynomials $Q_1, \ldots, Q_n \in K[x]$ are relatively prime, then the system $P \equiv R_i \pmod{Q_i}, 1 \leq i \leq n$ has a unique solution modulo $Q_1 \cdots Q_n$.

1. Let f, g be relatively prime polynomials with integer coefficients. Prove that there exist nonzero polynomials u, v with integer coefficients such that $uf + vg = k$ where k is a nonzero integer. Suppose that $u_1 f + v_1 g = k_0$ and u_1, v_1 are integer polynomials with $u_1 = \sum_{i=0}^{m} a_i, v = \sum_{i=0}^{n} b_i x^i$, $\deg(u_1) < \deg(g)$, $\gcd(a_0, \ldots, a_m, b_0, \ldots, b_n) = 1$. Then $k_0 \mid k$.

2. Let f, g be polynomials with integer coefficients and with no common factor. Prove that $\gcd(f(n), g(n)), n \in \mathbb{Z}$ can only attain a finite number of values.

3. Let $f : \mathbb{Q} \to \mathbb{Q}$ satisfy $f(f(f(x))) + 2f(f(x)) + f(x) = 4x.$ and $f(f(\cdots f(x))) = x$ where f is taken 2009 times. Prove that $f(x) = x$.

4. (USAMO 1997/3) Prove that for any integer n, there exists a unique polynomial Q with coefficients in $\{0, 1, \ldots, 9\}$ such that $Q(-2) = Q(-5) = n$.

5. Suppose that f and g are integer polynomials such that $f(n)/g(n)$ is an integer for infinitely many $n \in \mathbb{Z}$. Show that as polynomials, $g(x)$ divides $f(x)$.

6. (IMO 2002/3) Find all pairs of integers $m > 2, n > 2$ such that there are infinitely many positive integers a for which $a^n + a^2 - 1$ divides $a^m + a - 1$.

7. (ISL 1996/A6) Let n be an even positive integer. Prove that there exists a positive integer k so that
$$k = f(x) \cdot (x+1)^n + g(x) \cdot (x^n + 1)$$
for some polynomials $f(x), g(x)$ having integer coefficients. If k_0 denotes the least such k, show that $k_0 = 2^q$ where q is the odd integer determined by $n = q \cdot 2^r, r \in \mathbb{N}$.

(D) 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 5 (Fundamental Theorem of Symmetric Polynomials). Let R be a ring (say, $\mathbb{Z}$), and $f(x_1, \ldots, x_n)$ a polynomial symmetric in all its variables. Then there exists a unique polynomial g such that

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

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

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

Theorem 6. 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 $1, a, \ldots, a^{d-1}$ to generate $K(a)$ over K. The zeros of the minimal polynomial of a are called the *conjugates* of a.

Theorem 7. 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 $a_1, \ldots, a_k$ be the conjugates of a and $b_1, \ldots, b_l$ 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.) □

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 8 (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).

Problems D

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 $\frac{1}{k^{p-2}}$.

(E) Cyclotomic and Chebyshev Polynomials

The nth cyclotomic polynomial is defined by
$$\Phi_n(x) = \prod_{0 \leq j < n, \gcd(j,n)=1} (x - e^{\frac{2\pi i j}{n}})$$

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 9. 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. (Komal) Prove that there exists a positive integer n so that any prime divisor of $2^n - 1$ is smaller that $2^{\frac{n}{1993}} - 1$.
3. 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
4. (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.
5. (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 $\theta = \pi/6$.
6. (Chebyshev) Let $p(x)$ be a real polynomial of degree $n \geq 1$ with leading coefficient 1. Then
$$\max_{-1\leq x\leq 1} |p(x)| \geq \frac{1}{2^{n-1}}.$$
7. 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 10. Let $r_1, \ldots, r_n$ be the roots of $\sum_{i=0}^{n} a_i x^i$, and let
$$s_j = \sum_{1\leq i_1 < \ldots < i_j \leq n} r_{i_1} \cdots r_{i_j}.$$
  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 $p \geq 5$.

2. Prove that for prime $p \geq 5$,

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

3. (APMO 2006/3) Prove that for prime $p \geq 5$, $\binom{p^2}{p} \equiv p \pmod{p^5}$.

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.