Integer Polynomials

Andres Buritica Monroy

1 Basic facts

For all of these, let $p(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial with integer coefficients.

We say that $p(x)$ is *divisible* by a polynomial $q(x)$ if there is a polynomial $r(x)$ (not necessarily with integer coefficients) such that $p(x) = q(x)r(x)$. We also write $q(x) \mid p(x)$.

- (Division algorithm) For any polynomial q there are unique polynomials f and r such that $p(x) = q(x)f(x) + r$ and $\deg r < \deg q$.

  If q has integer coefficients, then f and r have rational coefficients. If q has a leading coefficient of ± 1, then f and r have integer coefficients.

- Since we proved Euclid's algorithm and Bézout's identity from the division algorithm, they still hold for polynomials.

- (Remainder theorem) If $p(a) = c$ then $x - a \mid p(x) - c$.

- (Finite differences) If c is a constant and p is a polynomial with leading coefficient ax^n, then $p(x) - p(x - c)$ is a polynomial with leading coefficient nax^{n-1}.

- (*) If a and b are integers, then $a - b \mid p(a) - p(b)$.

2 Primitive polynomials

An integer polynomial is *primitive* if its coefficients have gcd 1.

- Every nonzero rational polynomial has exactly one primitive multiple with positive leading coefficient.

- (Gauss' Lemma) The product of two primitive polynomials is primitive.

- (Gauss' Lemma, alternate form) If an integer polynomial is the product of two nonconstant rational polynomials then it is the product of two nonconstant integer polynomials.

- (Rational Root Theorem) If y and z are integers with $\gcd(y, z) = 1$ such that $p(y/z) = 0$ then $y \mid a_0$ and $z \mid a_n$.

3 Irreducibility

An integer polynomial is *irreducible* over $\mathbb{Z}$ (for the rest of this handout, I'll shorten this to irreducible) if it is not the product of two nonconstant integer polynomials.

Usually, to prove irreducibility you will assume for contradiction that the polynomial is reducible. Modular arithmetic arguments on the coefficients are often useful.

- (Unique factorisation) Every integer polynomial can be factorised into a product of a constant and primitive irreducible integer polynomials. This factorisation is unique up to the permutation and sign of these polynomials.
- (Eisenstein's Criterion) If there exists a prime q such that $q^2 \nmid a_0$, $q \mid a_i$ for each i from 0 to $n-1$, and $q \nmid a_n$, then p is irreducible.
- If an integer polynomial is irreducible mod n for some positive integer n, then it is irreducible.

4 Polynomials mod p

Let p be prime.

- Prove that unique factorisation holds for polynomials mod p. (This is not true for all integers — for instance, $(x-1)^2 \equiv (x-3)^2 \pmod 4$.)
- Prove that for every function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ there is a unique polynomial P in $\mathbb{Z}_p$ of degree less than $p-1$ such that $f(x) = P(x)$ for each $x \in \mathbb{Z}_p$.
- Let g be a generator mod p, and let $ab = p-1$. Prove that

$$\prod_{i=1}^{a}(x - g^{bi}) \equiv x^a - 1 \pmod p.$$

  What does this tell us about the roots of the cyclotomic polynomials in mod p?
- Consider all $\binom{p-1}{k}$ products of k elements of $\mathbb{Z}_p$. Prove that their sum is divisible by p.
- For any positive integer $n < p-1$, prove that

$$\sum_{i=1}^{p-1} i^n \equiv 0 \pmod p.$$

5 Problems

1. (Schur's Theorem) Prove that for every nonconstant integer polynomial, the set of primes that divide some element of its image is infinite.
2. Let p be an integer polynomial and let a be an integer such that $p(p(\cdots(p(a))\cdots)) = a$. Prove that $p(p(a)) = a$.
3. Let p be a polynomial of dgree d. Find a linear equation that the values $p(0), p(1), \ldots, p(d+1)$ always satisfy.

4. Let $P(x)$ and $Q(x)$ be polynomials whose coefficients are all equal to 1 or 7. If $P(x)$ divides $Q(x)$, prove that $1 + \deg P(x)$ divides $1 + \deg Q(x)$.

5. Let p be an irreducible integer polynomial. Prove that p does not have multiple roots.

6. Let a, b, c be integers such that $a/b + b/c + c/a$ and $a/c + c/b + b/a$ are both integers. Prove that $|a| = |b| = |c|$.

7. Prove that if p is prime, then $1 + x + x^2 + \cdots + x^{p-1}$ is irreducible.

8. Prove that if $5 \nmid a$, then $x^5 - x + a$ is irreducible.

9. Find all integer polynomials p such that

   - $p(n) > n$ for all positive integers n, and
   - for each positive integer n there is a positive integer k such that $p^{(k)}(1)$ (p repeated k times) is divisible by n.

6 Homework

1. Find all integer polynomials p such that $n \mid p(2^n)$ for all positive integers n.
2. Let p be prime. Find the least residue of the product of $(4 - x)$ mod p, where x runs over all residues mod p except the quadratic residues.
3. Find all positive integers k for which the following statement is true: if p is an integer polynomial such that $0 \leq p(i) \leq k$ for each integer $0 \leq i \leq k + 1$, then all of these $p(i)$s are equal.