Integer Polynomials

Andres Buritica

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 $x - a \mid p(x) - c$.

- (*) 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.

- (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.

4 Problems

1. Prove that every nonconstant integer polynomial has a composite number in its image.
2. (Schur's Theorem) Prove that for every nonconstant integer polynomial, the set of primes that divide some element of its image is infinite.
3. Let p be an integer polynomial and let a be an integer such that $p(p(\cdots(p(a))\cdots)) = a$. Prove that $p(p(a)) = a$.
4. 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 $|a| = |b| = |c|$.
5. Prove that if p is prime, then $1 + x + x^2 + \cdots + x^{p-1}$ is irreducible.
6. Let f be a nonconstant integer polynomial and let n and k be positive integers. Prove that there exists a positive integer a such that each of the numbers $f(a), f(a+1), \ldots, f(a+n-1)$ has at least k distinct prime divisors.
7. Prove that if $5 \nmid a$, then $x^5 - x + a$ is irreducible.
8. 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.

5 Homework

1. Find all integer polynomials p such that $n \mid p(2^n)$ for all positive integers n.
2. Let p be an irreducible integer polynomial. Prove that p does not have multiple roots.
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.