Integer Polynomials

Victor Rong

July 5, 2024

Definition. An integer polynomial $P(x)$ is a polynomial of the form

$$c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$$

where $c_n, c_{n-1}, \ldots, c_0 \in \mathbb{Z}$.

Integer polynomials problems span across many ideas in both algebra and number theory, the most prominent of which will be covered in this handout.

1 Warm-Up

Example 1. $P(x)$ is a polynomial such that $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. Is P an integer polynomial?

Example 2. (Schur's Theorem). For any integer polynomial $P(x)$, prove that either $P(x)$ is constant or there are infinitely many primes which divide $P(n)$ for some integer n.

Example 3. Bert is thinking of an ordered quadruple of integers (a, b, c, d). Ernie, hoping to determine these integers, hands Bert a 4-variable polynomial $P(w, x, y, z)$ with integer coefficients, and Bert returns the value of $P(a, b, c, d)$. From this value alone, Ernie can always determine Bert's original ordered quadruple. Construct, with proof, one polynomial that Ernie could have used.

2 Integer Divisibility

Lemma 2.0.1. Let P and Q be integer polynomials such that $P(n) \mid Q(n)$ for infinitely many $n \in \mathbb{N}$. Then $\frac{Q(n)}{P(n)}$ is a rational polynomial.

Note that even if the divisibility holds for all $n \in \mathbb{Z}$, we can only guarantee that $\frac{Q(n)}{P(n)}$ is rational, not integer. The same types of counterexamples as from Example 1 apply.

Lemma 2.0.2. Let P be an integer polynomial. For any $a, b \in \mathbb{Z}$, $a - b \mid P(a) - P(b)$.

Equivalently, this lemma means that $P(n) \equiv P(n \pmod d) \pmod d$. This is one of the most important tools when working with integer polynomials.

Example 4. (CMO 2016). Find all polynomials $P(x)$ with integer coefficients such that $P(P(n)+n)$ is a prime number for infinitely many integers n.

This lemma can also be very helpful for creating unexpected inequalities.

Example 5. (USAMO 1974). Let a, b, and c denote three distinct integers, and let P denote a polynomial having integer coefficients. Show that it is impossible that $P(a) = b$, $P(b) = c$, and $P(c) = a$.

2.1 Problems

1. (MOP 2005). Let $P(x)$ be an integer polynomial and n be an odd number. Suppose that $x_1, \ldots, x_n \in \mathbb{Z}$ such that $x_2 = P(x_1), x_3 = P(x_2), \ldots, x_1 = P(x_n)$. Prove that $x_1 = x_2 = \ldots = x_n$.
2. (IMO 2006). Let $P(x)$ be a polynomial of degree $n > 1$ with integer coefficients and let k be a positive integer. Consider the polynomial $Q(x) = P(P(\ldots P(P(x))\ldots))$, where P occurs k times. Prove that there are at most n integers t such that $Q(t) = t$.
3. (CMO 2010). Let $P(x)$ and $Q(x)$ be polynomials with integer coefficients. Let $a_n = n! + n$. Show that if $\frac{P(a_n)}{Q(a_n)}$ is an integer for every n, then $\frac{P(n)}{Q(n)}$ is an integer for every integer n such that $Q(n) \neq 0$.
4. (USATST 2010). Let P be a polynomial with integer coefficients such that $P(0) = 0$ and
$$\gcd(P(0), P(1), P(2), \ldots) = 1.$$
Show there are infinitely many n such that
$$\gcd(P(n) - P(0), P(n+1) - P(1), P(n+2) - P(2), \ldots) = n.$$
5. (USATST 2018). As usual, let $\mathbb{Z}[x]$ denote the set of single-variable polynomials in x with integer coefficients. Find all functions $\theta : \mathbb{Z}[x] \to \mathbb{Z}$ such that for any polynomials $p, q \in \mathbb{Z}[x]$,
   - $\theta(p + 1) = \theta(p) + 1$, and
   - if $\theta(p) \neq 0$ then $\theta(p)$ divides $\theta(p \cdot q)$.

3 Mod p

Definition. Let p be a prime. We denote the integers modulo p as $\mathbb{F}_p$. A polynomial $P(x) \in \mathbb{F}_p$ has coefficients in $\mathbb{F}_p$. Two polynomials P, Q are equal if their coefficients are equal mod p.

In fact, $\mathbb{F}_p$ is a *field*, much like $\mathbb{R}$ and $\mathbb{C}$ and so many of the same properties including unique factorization and GCD remain.

Example 6. Let p be a prime. Factor $x^p - x$ over $\mathbb{F}_p$.

Lemma 3.0.1. (Frobenius Endomorphism). For prime p and variables $x_1, \dots, x_n$, we have

$$(x_1 + x_2 + \ldots + x_n)^p \equiv x_1^p + x_2^p + \ldots + x_n^p \pmod p.$$

Note that this statement is "different" from Fermat's Little Theorem in the sense that it's working with arbitrary symbols x_i rather than elements mod p.

Theorem. (Hensel's Lemma). Let $P(x)$ be an integer polynomial and p a prime. Suppose that for some integer t, we have $P(t) \equiv 0 \pmod p$ and $P'(t) \not\equiv 0 \pmod p$. Then for any positive integer k, there exists a unique residue $t_k \pmod{p^k}$ such that $P(t_k) \equiv 0 \pmod{p^k}$ and $t \equiv t_k \pmod p$.

Example 7. (IMO 1984). Find one pair of positive integers a, b such that $ab(a+b)$ is not divisible by 7, but $(a+b)^7 - a^7 - b^7$ is divisible by 7^7.

1. (Putnam 2008). Let p be a prime number. Let $h(x)$ be a polynomial with integer coefficients such that $h(0), h(1), \dots, h(p^2-1)$ are distinct modulo p^2. Show that $h(0), h(1), \dots, h(p^3-1)$ are distinct modulo p^3.
2. (ISL 1997). Let p be a prime number and f an integer polynomial of degree d such that $f(0) = 0, f(1) = 1$ and $f(n)$ is congruent to 0 or 1 modulo p for every integer n. Prove that $d \geq p - 1$.
3. (Putnam 2002). Let p be a prime number. Prove that the determinant of the matrix

$$\begin{bmatrix} x & y & z \\ x^p & y^p & z^p \\ x^{p^2} & y^{p^2} & z^{p^2} \end{bmatrix}$$

   is congruent modulo p to a product of polynomials of the form $ax + by + cz$, where a, b, and c are integers.
4. (Romania 2007). Let

$$f = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

   be an integer polynomial of degree $n \geq 3$ such that $a_k + a_{n-k}$ is even for all $k \in \overline{1, n-1}$ and a_0 is even. Suppose that $f = gh$, where g, h are integer polynomials and $\deg g \leq \deg h$ and all the coefficients of h are odd. Prove that f has an integer root.
5. If a, b are positive integers and p a prime such that $p \mid a^2 + ab + b^2$, then prove that

$$p^3 \mid (a+b)^p - a^p - b^p.$$

6. (USATST 2016). Let p be a prime number. Let $\mathbb{F}_p$ denote the integers modulo p, and let $\mathbb{F}_p[x]$ be the set of polynomials with coefficients in $\mathbb{F}_p$. Define $\Psi : \mathbb{F}_p[x] \to \mathbb{F}_p[x]$ by

$$\Psi\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} a_i x^{p^i}.$$

   Prove that for nonzero polynomials $F, G \in \mathbb{F}_p[x]$,

$$\Psi(\gcd(F, G)) = \gcd(\Psi(F), \Psi(G)).$$

Here, a polynomial Q divides P if there exists $R \in \mathbb{F}_p[x]$ such that $P(x) - Q(x)R(x)$ is the polynomial with all coefficients 0 (with all addition and multiplication in the coefficients taken modulo p), and the gcd of two polynomials is the highest degree polynomial with leading coefficient 1 which divides both of them. A non-zero polynomial is a polynomial with not all coefficients 0. As an example of multiplication, $(x+1)(x+2)(x+3) = x^3 + x^2 + x + 1$ in $\mathbb{F}_5[x]$.

7. (Japan 2017). Let $x_1, x_2, \cdots, x_{1000}$ be integers, and $\sum_{i=1}^{1000} x_i^k$ are all multiples of 2017 for any positive integers $k \leq 672$. Prove that $x_1, x_2, \cdots, x_{1000}$ are all multiples of 2017. (Note: 2017 is prime.)

4 Irreducibility

There are two main ways to analyze if an integer polynomial is irreducible over $\mathbb{Z}[x]$: through the divisors of its coefficients or through the size of its roots. Firstly, we will show some equivalence between irreducibility over $\mathbb{Q}$ and irreducibility over $\mathbb{Z}$.

Definition. A polynomial with integer coefficients is called *primitive* if the greatest common divisor of all its coefficients is 1.

For instance, all monic polynomials are primitive.

Lemma 4.0.1. (Gauss's Lemma). If $P(x)$ and $Q(x)$ are primitive integer polynomials, their product $P(x)Q(x)$ must also be primitive.

Gauss's Lemma can also be framed as a result on irreducibility.

Lemma 4.0.2. A primitive integer polynomial $P(x)$ is irreducible over $\mathbb{Z}$ if and only if it is irreducible over $\mathbb{Q}$.

The rational root theorem is also a special case of this lemma.

Theorem. (Rational Root). Let

$$P(x) = a_d x^d + \ldots + a_0$$

for integer coefficients a_i. For any rational root $\frac{p}{q}$ in lowest terms, then $p \mid a_0$ and $q \mid a_d$.

Theorem. (Eisenstein). Let $P(x) = a_n x^n + \ldots + a_0$ be an integer polynomial. Suppose that for some prime p, we have $p \mid a_i$ for $0 \leq i \leq n-1$, but $p \nmid a_n$ and $p^2 \nmid a_0$. Then P is irreducible over $\mathbb{Z}$.

Example 8. Let p be a prime number. Prove that $P(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible over $\mathbb{Z}$.

We can also show irreducibility by bounding conditions.

Example 9. Let $P(x) = a_n x^n + \ldots + a_0$ be an integer polynomial such that $|a_0|$ is prime and

$$|a_0| > |a_1| + |a_2| + \ldots + |a_n|.$$

Prove that P is irreducible.

4.1 Problems

1. If $a_1, a_2, \ldots, a_n$ are distinct integers, prove that the polynomial $P(x) = (x-a_1)(x-a_2)\cdots(x-a_n) - 1$ is irreducible over integer polynomials.
2. Let f be an irreducible polynomial in $\mathbb{Z}[x]$. Show that f has no multiple roots.
3. (MOP 2007). Prove that for any non-constant $P \in \mathbb{Z}[x]$, there exist arbitrarily large integers r such that $P(x) - r$ is irreducible over $\mathbb{Z}$.
4. (ISL 2012). Let f and g be two nonzero polynomials with integer coefficients and $\deg f > \deg g$. Suppose that for infinitely many primes p the polynomial $pf + g$ has a rational root. Prove that f has a rational root.
5. Let p be a prime. Show that $x^{p-1} + 2x^{p-2} + \ldots + (p-1) + p$ is irreducible.
6. (IMO 2002). Find all pairs of positive integers $m, n \geq 3$ for which there exist infinitely many positive integers a such that
$$\frac{a^m + a - 1}{a^n + a^2 - 1}$$
is itself an integer.
7. (Kronecker). Let $P(x)$ be a monic integer polynomial such that all its roots lie on the unit circle of the complex plane. Prove that all the zeros of P are roots of unity. That is, for some n, k, $P(x) \mid (x^n - 1)^k$.

5 Extra Problems

A Problems

A1. (ELMO 2016). Big Bird has a polynomial P with integer coefficients such that n divides $P(2^n)$ for every positive integer n. Prove that Big Bird's polynomial must be the zero polynomial.

A2. (CMO 2024). Let N be the number of positive integers with 10 digits $\overline{d_9 d_8 \cdots d_0}$ in base 10 (where $0 \le d_i \le 9$ for all i and $d_9 > 0$) such that the polynomial

$$d_9 x^9 + d_8 x^8 + \cdots + d_1 x + d_0$$

is irreducible in $\mathbb{Q}$. Prove that N is even.

A3. (USAMTS 2018). A nonnegative integer is called *uphill* if its decimal digits are non-decreasing from left to right (0 is considered to be uphill). A polynomial $P(n)$ has rational coefficients and $P(n)$ is an integer for every uphill number n. Is it necessarily true that $P(n)$ is an integer for all integers n?

A4. (ISL 2019). We say that a set S of integers is rootiful if, for any positive integer n and any $a_0, a_1, \cdots, a_n \in S$, all integer roots of the polynomial $a_0 + a_1 x + \cdots + a_n x^n$ are also in S. Find all rootiful sets of integers that contain all numbers of the form $2^a - 2^b$ for positive integers a and b.

A5. (ISL 2012). Consider a polynomial $P(x) = \prod_{j=1}^{9}(x + d_j)$, where $d_1, d_2, \ldots d_9$ are nine distinct integers. Prove that there exists an integer N, such that for all integers $x \ge N$ the number $P(x)$ is divisible by a prime number greater than 20.

B Problems

B1. (ISL 2013). Prove that there exist infinitely many positive integers n such that the largest prime divisor of $n^4 + n^2 + 1$ is equal to the largest prime divisor of $(n+1)^4 + (n+1)^2 + 1$.

B2. (ARMO 2022). We call a polynomial $P(x)$ good if the numbers $P(k)$ and $P'(k)$ are integers for all integers k. Let $P(x)$ be a good polynomial of degree d, and let N_d be the product of all composite numbers not exceeding d. Prove that the leading coefficient of the polynomial $N_d \cdot P(x)$ is integer.

B3. (ARMO 2019). Let $P(x)$ be a non-constant polynomial with integer coefficients and let n be a positive integer. The sequence $a_0, a_1, \ldots$ is defined as follows: $a_0 = n$ and $a_k = P(a_{k-1})$ for all positive integers k. Assume that for every positive integer b the sequence contains a bth power of an integer greater than 1. Show that $P(x)$ is linear.

B4. (ISL 2009). Let $P(x)$ be a non-constant polynomial with integer coefficients. Prove that there is no function T from the set of integers into the set of integers such that the number of integers x with $T^n(x) = x$ is equal to $P(n)$ for every $n \ge 1$, where T^n denotes the n-fold application of T.

B5. (APMO 2018). Find all polynomials $P(x)$ with integer coefficients such that for all real numbers s and t, if $P(s)$ and $P(t)$ are both integers, then $P(st)$ is also an integer.

C Problems

C1. (IMO 2023). For each integer $k \geq 2$, determine all infinite sequences of positive integers a_1, a_2, ... for which there exists a polynomial P of the form

$$P(x) = x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0,$$

where c_0, c_1, ..., c_{k-1} are non-negative integers, such that

$$P(a_n) = a_{n+1}a_{n+2}\cdots a_{n+k}$$

for every integer $n \geq 1$.

C2. (IMO 2017). An ordered pair (x, y) of integers is a primitive point if the greatest common divisor of x and y is 1. Given a finite set S of primitive points, prove that there exist a positive integer n and integers $a_0, a_1, \ldots, a_n$ such that, for each (x, y) in S, we have:

$$a_0x^n + a_1x^{n-1}y + a_2x^{n-2}y^2 + \cdots + a_{n-1}xy^{n-1} + a_ny^n = 1.$$

C3. (ISL 2011). Let $P(x)$ and $Q(x)$ be two polynomials with integer coefficients, such that no nonconstant polynomial with rational coefficients divides both $P(x)$ and $Q(x)$. Suppose that for every positive integer n the integers $P(n)$ and $Q(n)$ are positive, and $2^{Q(n)} - 1$ divides $3^{P(n)} - 1$. Prove that $Q(x)$ is a constant polynomial.

C4. (China 2014). Show that there are no 2-tuples (x, y) of positive integers satisfying the equation $(x + 1)(x + 2)\cdots(x + 2014) = (y + 1)(y + 2)\cdots(y + 4028)$.

C5. (USATSTST 2016). Decide whether or not there exists a nonconstant polynomial $Q(x)$ with integer coefficients with the following property: for every positive integer $n > 2$, the numbers

$$Q(0),\ Q(1), Q(2),\ \ldots,\ Q(n-1)$$

produce at most $0.499n$ distinct residues when taken modulo n.

C6. (USATSTST 2019). Suppose P is a polynomial with integer coefficients such that for every positive integer n, the sum of the decimal digits of $|P(n)|$ is not a Fibonacci number. Must P be constant? (A Fibonacci number is an element of the sequence $F_0, F_1, \ldots$ defined recursively by $F_0 = 0, F_1 = 1$, and $F_{k+2} = F_{k+1} + F_k$ for $k \geq 0$.)

6 Exercise Solutions

6.1 Warm-up Solutions

Example 1. $P(x)$ is a polynomial such that $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. Is P an integer polynomial?

Proof. False. Consider $P(n) = \frac{n(n-1)}{2}$ for example. In fact, $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$ if and only if $P(x)$ can be written as

$$P(x) = \sum_{j=0}^{d} c_j \binom{x}{j}$$

for $c_j \in \mathbb{Z}$. □

Example 2. (Schur's Theorem). For any integer polynomial $P(x)$, prove that either $P(x)$ is constant or there are infinitely many primes which divide $P(n)$ for some integer n.

Proof. Assume for the sake of contradiction that P is non-constant and only finitely many primes divide $P(n)$. Let Q be the product of all these primes. Furthermore, consider the constant term a_0 of P. It must be non-zero, otherwise we can clearly generate new prime divisors. Then for any integer k, we have

$$P(a_0Qk) = \sum_{j=0}^{d} a_j(a_0Qk)^d = a_0(Q \cdot (\cdots) + 1).$$

Clearly Q cannot divide the right term and so it must either be 1 or introduce a new prime divisor. We can vary k so that it is not 1, and so we are done. □

Example 3. Bert is thinking of an ordered quadruple of integers (a, b, c, d). Ernie, hoping to determine these integers, hands Bert a 4-variable polynomial $P(w, x, y, z)$ with integer coefficients, and Bert returns the value of $P(a, b, c, d)$. From this value alone, Ernie can always determine Bert's original ordered quadruple. Construct, with proof, one polynomial that Ernie could have used.

Proof. One possible constructions is to first generate a large M such as

$$M(w, x, y, z) = 1000(w^2 + x^2 + y^2 + z^2 + 1) >> w, x, y, z.$$

Then we construct P so that the values of a, b, c, d are written almost as digits base M. In particular, we can choose

$$P(w, x, y, z) = M(w, x, y, z)^4 + wM(w, x, y, z)^3 + xM(w, x, y, z)^2 + yM(w, x, y, z) + z.$$

Then to decode $P(a, b, c, d)$, we can find $M(a, b, c, d)$ and then read off the digits. Note that there are some finer details here, as the numbers may be negative. □

6.2 Integer Divisibility Solutions

Example 4. (CMO 2016). Find all polynomials $P(x)$ with integer coefficients such that $P(P(n)+n)$ is a prime number for infinitely many integers n.

Proof. From our lemma, note that

$$P(n) \mid P(P(n)+n) - P(n).$$

In particular, we can write $P(P(n)+n) = P(n)Q(n)$ for some $Q \in \mathbb{Z}[x]$. If $d = \deg(P)$, then Q must have degree $d^2 - d$. For $P(P(n)+n)$ to be a prime number for infinitely many integers n, we must have $P(n)$ or $Q(n)$ be ± 1 for infinitely many integers n. So either P or Q must be a constant polynomial $\implies d \leq 1$. For $d = 0$, clearly $P(x) \equiv p$ for a prime p is the only solution. For $d = 1$, consider $P(n) = an + b$. Then

$$P(P(n)+n) = a(a+1)n + ab + b = (a+1)(an+b).$$

So $a + 1 = \pm 1$. A quick check finds that $P(n) = -2n + c$ for c odd is the only set of linear solutions. □

Example 5. (USAMO 1974). Let a, b, and c denote three distinct integers, and let P denote a polynomial having integer coefficients. Show that it is impossible that $P(a) = b$, $P(b) = c$, and $P(c) = a$.

Proof. Assume for the sake of contradiction that it is possible. We have

$$a - b \mid P(a) - P(b),\ b - c \mid P(b) - P(c),\ c - a \mid P(c) - P(a)$$

$$\implies a - b \mid b - c \mid c - a \mid a - b.$$

$$\implies |a - b| \leq |b - c| \leq |c - a| \leq |a - b|.$$

This chain of inequalities means that their differences must all be equal in absolute value. If $a-b = -(b-c)$ or a similar cyclic equation, then $a = c$ contradicting a, b, c distinct. Otherwise, we must have $a-b = b-c = c-a = t$ for some integer t. But then note that $3t = (a-b)+(b-c)+(c-a) = 0$ and thus $a = b = c$, contradiction. So the assumption was false. □

6.3 Mod p Solutions

Example 6. Let p be a prime. Factor $x^p - x$ over $\mathbb{F}_p$.

Proof. By Fermat's Little Theorem, we know that a is a solution to $x^p - x \equiv 0 \pmod{p}$ for any $a \in \mathbb{F}_p$. So $x - a$ factors into $x^p - x$. In particular, we have p factors and we know the degree of $x^p - x$ is p. Thus, we see that

$$x^p - x \equiv x(x-1)\cdots(x-p+1) \pmod{p}.$$

Note that the leading coefficient needed to be determined. □

Example 7. (IMO 1984). Find one pair of positive integers a, b such that $ab(a+b)$ is not divisible by 7, but $(a+b)^7 - a^7 - b^7$ is divisible by 7^7.

Proof. We can write

$$(a+b)^7 - a^7 - b^7 = 7ab(a+b)(a^2+ab+b^2)^3.$$

So it suffices to find a, b such that $7^3 \mid a^2+ab+b^2$. Consider the polynomial $P(x) = x^2+x+1$. We note that $P(2) \equiv 0 \pmod 7$ and $P'(2) \not\equiv 0 \pmod 7$. So we can use this to find a $P(t) \equiv 0 \pmod{7^2}$. In particular, we can write $t = 7s+2$. Then we want

$$7^2 \mid (7s+2)^2 + (7s+2) + 1 \implies 7^2 \mid 35s + 7.$$

So $s = 4, t = 30$ works. We repeat this again with

$$7^3 \mid (49s+30)^2 + (49s+30) + 1 \implies 7^3 \mid (2 \cdot 30 + 1) \cdot 49 \cdot s + 30^2 + 30 + 1.$$

Trying this out, we see that $s \equiv -1 \pmod 7$ works, giving $s = 6, t = 324$. So $(a, b) = (324, 1)$ is a valid solution. □

6.4 Irreducibility Solutions

Example 8. For p prime, show that $P(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible over $\mathbb{Z}$.

Proof. We will show that $P(x+1)$ is irreducible, which clearly implies the result. Indeed,

$$P(x+1) = \frac{(x+1)^p - 1}{(x+1) - x} = x^{p-1} + px^{p-2} + \ldots + p.$$

Note in particular that p divides all the intermediate binomial coefficients. It is also apparent that p does not divide the leading coefficient and p^2 does not divide the constant term. So by Eisenstein's, we are done. □

Example 9. Let $P(x) = a_n x^n + \ldots + a_0$ be an integer polynomial such that $|a_0|$ is prime and

$$|a_0| > |a_1| + |a_2| + \ldots + |a_n|.$$

Prove that P is irreducible.

Proof. Assume for the sake of contradiction that P can be written as $P(x) = A(x)B(x)$ for $A, B \in \mathbb{Z}[x]$. Then the constant terms of A, B must be $\{\pm 1, \pm a_0\}$ as $|a_0|$ is prime. Say A has constant term 1 and integer leading coefficient T. Then the product of A's roots is $\frac{1}{T}$, and so A must have some complex root r such that $|r| \le 1$. As P must also have this root, we have

$$P(r) = \sum_{j=0}^{n} a_j r^j = 0 \implies -a_0 = \sum_{j=1}^{n} a_j r^j.$$

However,

$$|a_0| = \left| \sum_{j=1}^{n} a_j r^j \right| \le \sum_{j=1}^{n} |a_j||r^j| \le \sum_{j=1}^{n} |a_j| < |a_0|,$$

contradiction. □