Lecture 13 — Polynomials and Number Theory

Holden Lee

3/4/2011

In many ways, polynomials are similar to integers. Like integers, polynomials admit division with remainder, existence of greatest common divisors, and unique factorization. In Section 1 we will state the main theorems concretely. In Section 2 we do some problem solving involving polynomials with integer or rational coefficients, and in Section 3 we give some surprising applications to number theory. For the more advanced reader, in the last section we restate the results of Section 1 more abstractly and prove them. We will see that the core reason behind unique factorization for integers and for polynomials are the same.

Note this is a continuation of Lecture 8; in particular, we assume knowledge of the basic definitions, etc. given there.

1 Main Theorems

In this section K will stand for $\mathbb{C}$ (the complex numbers), $\mathbb{R}$ (the real numbers), $\mathbb{Q}$ (the rational numbers), or $\mathbb{Z}/p\mathbb{Z}$ (the integers modulo p), while R will stand for any one of the before sets or $\mathbb{Z}$ (the integers). Note that the sets we label with K all have multiplicative inverses, i.e. are *fields*.

Our first result is that when we divide polynomials, we can be assured to get a remainder with degree smaller than our divisor.

Theorem 1.1 (Division with remainder)**:** If $f, g \in K[x]$, then there exist polynomials $q, r \in K[x]$ such that $\deg r < \deg g$ and

$$f = qg + r.$$

If $f, g \in \mathbb{Z}[x]$ and g is monic, then there exist $q, r \in \mathbb{Z}[x]$ such that $\deg r < \deg g$ and

$$f = gq + r.$$

Proof. This is the division algorithm familiar from high school algebra class. Namely, if f has leading term ax^n and g has leading term bx^m with $n \geq m$, then $f - \frac{a}{b}x^{n-m}$ has degree less than f. Thus we can keep subtracting multiples of g from f until the result has degree less than $\deg g$.

If g is monic, then $b = 1$ so at each stage we subtracted an integer polynomial multiple of g, and both the quotient q and the remainder r will have integer coefficients. □

Theorem 1.2 (Bézout)**:** Given $f, g \in R[x]$, there exists a polynomial h, called the **greatest common divisor** and denoted $\gcd(f, g)$, such that the following hold:

1. h divides both f and g.
2. If p divides both f and g then p divides h.

Let $f, g \in K[x]$. There exist polynomials $u, v \in K[x]$ so that $uf + vg = \gcd(f, g)$.

(Note that h is only determined up to a unit. We'll "sweep this under the rug" and allow any choice of h up to that constant.)

To calculate the gcd, we often use the Euclidean algorithm. Given polynomials f and g, for any polynomial q we have

$$\gcd(f, g) = \gcd(g, f - qg).$$

Supposing $\deg f \geq \deg g$, take q so that $f - qg = r$ has degree less than g, as in the division algorithm; this reduces the degree of f. Repeating this process decreases the degrees of the polynomials; we eventually get to $\gcd(h, 0)$ in which case the answer is seen to be h.

Theorem 1.3 (Unique factorization)**:** Every polynomial in $R[x]$ factors uniquely in $R[x]$, up to constants. In fact, every polynomial in $R[x_1, \ldots, x_n]$ factors uniquely in $R[x_1, \ldots, x_n]$, up to constants.

We give two more useful results.

Theorem 1.4 (Chinese Remainder Theorem)**:** If polynomials $Q_1, \ldots, Q_n \in K[x]$ are pairwise relatively prime, then the system $P \equiv R_i \pmod{Q_i}, 1 \leq i \leq n$ has a unique solution modulo $Q_1 \cdots Q_n$.

Theorem 1.5 (Rational Roots Theorem)**:** Suppose $f(x) = a_n x^n + \cdots + a_0$ is a polynomial with integer coefficients and with $a_n \neq 0$. Then all rational roots of f are in the form

$$\frac{\text{factor of } a_0}{\text{factor of } a_n}.$$

In particular, if $a_n = \pm 1$, then all rational roots of f are integers.

Here's a cute application of Bézout's Theorem:

Example 1.6: 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.

Solution. By Bézout's Theorem, we have $u(x)f(x) + v(x)g(x) = 1$ for some $u, v \in \mathbb{Q}[x]$ and nonzero. Clearing denominators of u and v, we get $u'(x)f(x) + v'(x)g(x) = k$ for some $u', v' \in \mathbb{Z}[x]$ and nonzero $k \in \mathbb{Z}$. Hence $\gcd(f(n), g(n)) \mid k$.

1.1 Problems

1. [1] Show by example we cannot always carry out division with remainder in $\mathbb{Z}[x]$ and that Bézout's Theorem does not hold for $\mathbb{Z}[x]$.
2. [1] Compute the greatest common divisors in $\mathbb{Z}[x]$:
   (a) $\gcd(x^6 - x^5 - x^2 + 1, x^3 - 2x^2 + 2x - 1)$.
   (b) $\gcd(x^{12} - 1, x^8 + 1)$.
3. Find the greatest common divisor in $\mathbb{Z}[x]$:

(a) [2] $\gcd(x^n - 1, x^m - 1)$.

(b) [2.5] $\gcd(x^n + 1, x^m + 1)$.

Are your answers the same if we work in $(\mathbb{Z}/p\mathbb{Z})[x]$?

4. [1.5] Let $n > 0$ be an integer. Find the remainder upon division of $x^n + x^{n-1} + \cdots + 1$ by:

   (a) $x^2 + 1$.

   (b) $x^2 + x + 1$.

   (c) $x^2 - x + 1$.

5. [2.5] 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 $u_1 = \sum_{i=0}^{m} a_i x^i$, $v = \sum_{i=0}^{n} b_i x^i$, $\deg(u_1) < \deg(g)$, $\gcd(a_0, \ldots, a_m, b_0, \ldots, b_n) = 1$. Prove that $k_0 \mid k$.

6. [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 $f(x) = x$.

7. [3] (BAMO 2004) Find all polynomials f with integer coefficients taking irrationals to irrationals.

8. [5] (USAMO 1997/3) Prove that for any integer n, there exists a unique polynomial Q with coefficients in $\{0, 1, \ldots, 9\}$ such that $Q(-2) = Q(-5) = n$.

9. [2] For how many integers n is $\frac{n^3+1000}{n-10}$ an integer?

10. [2] 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 $f(x)$.

11. [5] (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 $a^m + a - 1$.

2 Arithmetic Properties

In this section we concentrate on polynomials with integer coefficients. The following is a simple but very useful idea.

Theorem 2.1: If P has integer coefficients, then $a - b \mid P(a) - P(b)$ for all integers a, b.

Proof. Let $m = a - b$. Then $a \equiv b \pmod{m}$. Let $P = c_n x^n + \cdots + c_1 x + c_0$. Then

$$c_n a^n + \cdots + c_1 a + c_0 \equiv c_n b^n + \cdots + c_1 b + c_0 \pmod{m}$$

giving $P(a) \equiv P(b) \pmod{m}$, as needed.

□

Here is a typical application. Note the use of the extremal principle.

Example 2.2 (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 $a = b = c$.

Proof. If not, then no two are equal. Without loss of generality, assume that c is between a and b. Then

$$|P(a) - P(b)| = |c - b| < |b - a|.$$

However, $b - a \mid P(b) - P(a)$, a contradiction. □

Example 2.3: Let P be a nonconstant polynomial with integer coefficients. Prove that there is an integer x so that $P(x)$ is composite.

Proof. Take n so that $P(n)$ is nonzero. Suppose it is prime. For all $k \in \mathbb{Z}$, we have $P(n) \mid P(n + kP(n)) - P(n)$, and hence $P(n) \mid P(n + kP(n))$. If $P(x)$ is not composite for any integer x, then $P(n + kP(n))$ is $\pm P(n)$ or 0 for all $k \in \mathbb{Z}$. P attains one of these values infinitely many times, so must be constant, a contradiction. □

One question we could ask is what values a polynomial can take modulo a given integer m as x ranges over the residues modulo m. (From Theorem 2.1 we know that the value modulo m depends only on x modulo m.) We know by the Lagrange Interpolation formula that we can manufacture a polynomial taking arbitrary values at a given set of points if we're allowed to divide—so it works for $\mathbb{R}, \mathbb{Q}$, and even $\mathbb{Z}/p\mathbb{Z}$. However Lagrange Interpolation will not work modulo m for m composite because in general we cannot divide modulo m (for example, 2 has no inverse modulo 4). For instance, Theorem 2.1 already tells us that given $P(x)$, $P(x + p)$ cannot be any residue modulo p^2; it can only be those residues that are congruent to x modulo p.

Example 2.4 (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.

Solution. **Step 1**

For $i \in \mathbb{N}$, let

$$P_i(x) = \prod_{k=1}^{i}(x - (2k - 1)).$$

(Define $P_0(x) = 1$.) By Problem 7, any polynomial with integer coefficients can be written in the form $\sum_{0 \le i \le n} c_i P_i(x)$.

Step 2

Let $a_i = \sum_{k=0}^{\infty} \left\lfloor \frac{i}{2^k} \right\rfloor$. We claim that $2^{a_i} \mid P_i(x)$ for all $i \in \mathbb{N}$ and all odd x. For a prime p and $n \in \mathbb{Z}$, denote by $v_p(n)$ the exponent of the highest power of p dividing n (by convention $v_p(0) = \infty$). For given odd x let $f(\alpha)$ be the number of values of k $(0 \le k \le i - 1)$ where $2^\alpha \mid x - 1 - 2k$. Then

$$v_2(P_i(x)) = \sum_{k=0}^{i-1} v_2(x - 1 - 2k) = \sum_{\alpha=1}^{\infty} f(\alpha)$$

since each k with $2^\alpha \mid\mid x-1-2k$ is counted α times in either sum.

Since any set of $2^{\alpha-1}$ consecutive even integers has one divisible by 2^α, any set of i consecutive even integers has at least $\left\lfloor \frac{i}{2^{\alpha-1}} \right\rfloor$ integers divisible by 2^α. Hence $f(\alpha) \geq \left\lfloor \frac{i}{2^{\alpha-1}} \right\rfloor$, and $v_2(P_i(x)) \geq \sum_{\alpha=0}^{\infty} \left\lfloor \frac{i}{2^\alpha} \right\rfloor$ as desired.

Note $a_0 = 0, a_1 = 1, a_2 = 3, a_3 = 4, a_4 = 7, a_5 = 8$, and $a_i \geq 10$ for $i \geq 6$.

Step 3

Next, we claim that if $P(x) = \sum_{0 \leq i \leq n} c_i P_i(x)$ has a complete remainder sequence then c_1 is odd. (c_0 obviously needs to be odd.) We have $4 \mid P(4k+i) - P(i)$ for any integer i; hence $r(4k+1) \equiv r(1) \pmod 4$ and $r(4k+3) \equiv r(3) \pmod 4$ for each k. In order for the remainder sequence to be complete, we need $r(1) \not\equiv r(3) \pmod 4$. But noting that $a_i \geq 2$ and $P_i(x) \equiv 0 \pmod 4$ for odd x and $i \geq 2$, we have $P(3) - P(1) \equiv c_1(P_1(3) - P_1(1)) \equiv 2c_1 \pmod 4$. Hence c_1 is odd.

Step 4

Since for any odd x, $P_i(x)$ is divisible by 2^{a_i}, if we mod out c_i by 2^{10-a_i}, and delete the terms with P_i for $i \geq 6$ (where $a_i \geq 10$), we get a polynomial with the same remainder sequence as P_i. If $P(x)$ gives a complete remainder sequence, then c_0 is odd, so there are 2^9 choices for it; c_1 is odd, so there are at most 2^8 choices for $c_1 \pmod{2^9}$ ($a_1 = 1$); for $2 \leq i \leq 5$ there are at most 2^{10-a_i} choices for $c_i \pmod{2^{10-a_i}}$. Hence the number of complete remainder sequences is at most

$$2^9 \cdot 2^8 \cdot \prod_{i=2}^{5} 2^{10-\alpha_i} = 2^9 \cdot 2^8 \cdot 2^7 \cdot 2^6 \cdot 2^3 \cdot 2^2 = 2^{35}.$$

□

Rather than ask about polynomials with integer coefficients, we could ask about polynomials with integer values, that is P such that $P(n)$ is an integer whenever n is an integer. It turns out that there is a nice description of such polynomials, as the following example shows.

Theorem 2.5: Let $f(x) \in \mathbb{C}[x]$. Then the following are equivalent:

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

b. For $n+1$ 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

$$f(x) = a_n \binom{x}{n} + a_{n-1} \binom{x}{n-1} + \cdots + a_0 \binom{x}{0}.$$

Here $\binom{x}{n}$ is defined as

$$\frac{x^{\underline{n}}}{n!} = \frac{x(x-1)\ldots(x-(n-1))}{n!}$$

Proof. The assertions $(a) \Rightarrow (b)$ and $(c) \Rightarrow (a)$ are clear ($\binom{x}{i}$ are integers for all integers x and nonnegative integers i, by combinatorial argument).

Suppose (b) holds. First assume that $f(x)$ takes on integer values at $0, 1, \ldots, n$. We inductively build the sequence $a_0, a_1, \ldots$ so that the polynomial

$$P_m(x) = a_m\binom{x}{m} + a_{m-1}\binom{x}{m-1} + \cdots + a_0\binom{x}{0}$$

matches the value of $f(x)$ at $x = 0, \ldots, m$. Define $a_0 = f(0)$; once $a_0, \ldots, a_m$ have been defined, let

$$a_{m+1} = f(m+1) - P_m(m+1).$$

Noting that $\binom{x}{m+1}$ equals 1 at $x = m+1$ and 0 for $0 \le x \le m$, this gives $P_{m+1}(x) = f(x)$ for $x = 0, 1, \ldots, m+1$. Now $P_n(x)$ is a degree n polynomial that agrees with $f(x)$ at $x = 0, 1, \ldots, n$, so they must be the same polynomial.

Now if f takes on integer values for any $n+1$ consecutive values $m, \ldots, m+n$, then by the argument above on $f(x-m)$, $f(x)$ takes on integer values for all x; in particular, for $x = 0, 1, \ldots, n$. Use the above argument to get the desired representation in (c). □

The key idea here in both examples that once we know that $P(x) = R(x)$ at some points $x_1, \ldots, x_n$, then we can write

$$P(x) = R(x) + (x - x_1)\cdots(x - x_n)Q(x). \tag{1}$$

When we're working over $\mathbb{Q}$ or $\mathbb{R}$, (1) doesn't put a restriction on other values of P, but when we're working over $\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z}$, then it does. For instance, if we're working over $\mathbb{Z}$ and $x_1, \ldots, x_n$ are integers, then we know $P(x)$ and $R(x)$ have to differ by a multiple of $(x - x_1)\cdots(x - x_n)$.

2.1 Problems

1. [1] Suppose P is a polynomial with integer coefficients such that $P(0)$ and $P(1)$ are both odd. Show that P has no integer root.

2. [2] (Schur) Let P be a nonconstant polynomial with integer coefficients. Prove that the set of primes dividing $P(n)$ for some integer n is infinite.

3. [2] Polynomial $P(x)$ has integer coefficients, and satisfies $P(2) = 18$ and $P(3) = 20$. Find all possible integer roots of $P(x) = 0$.

4. [3] (Putnam 2008) Let p be prime. Let $h(x)$ be a polynomial with integer coefficients such that $h(0), h(1), \ldots, h(p^2 - 1)$ are distinct modulo p^2. Show that $h(0), h(1), \ldots, h(p^3 - 1)$ are distinct modulo p^3.

5. [4] (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 $Q(t) = t$.

6. [4] (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

$$\text{lcm}[1, 2, \ldots, \deg(f)] \cdot \frac{f(m) - f(n)}{m - n}$$

is an integer.

7. [2] (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 (i.e. invertible), 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 $p_i(x) = x^{\underline{i}} = x(x-1)\cdots(x-i+1)$.

8. [2.5] How many polynomials of degree at most 5 with integer coefficients satisfy $0 \le P(x) < 120$ for $x = 0, 1, 2, 3, 4, 5$?

9. [4] (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 $m > n \ge 0$,

   (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.

10. [5] (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 variant: if n is not divisible hy the square of a prime)

11. [5] (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

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

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

12. [5] Suppose $f(x)$ is a polynomial of degree d taking integer values such that

$$m - n \mid f(m) - f(n)$$

for all pairs of integers (m, n) satisfying $0 \le m, n \le d$. Is it necessarily true that

$$m - n \mid f(m) - f(n)$$

for all pairs of integers (m, n)?

3 Polynomials in Number Theory

We give an interesting application of polynomials to number theory. Recall the following.

Theorem 3.1 (Vieta's Theorem)**:** 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 $s_j = (-1)^j \frac{a_{n-j}}{a_n}$.

Theorem 3.2 (Wolstenholme)**:** Prove that $\binom{pa}{pb} \equiv \binom{a}{b} \pmod{p^3}$ for prime $p \ge 5$.

Proof. By Fermat's Little Theorem, $x^{p-1} \equiv 1 \pmod{p}$. Thus in $\mathbb{Z}/p\mathbb{Z}$,

$$x^{p-1} - 1 \equiv \prod_{i=1}^{p-1} (x - i) \pmod{p}. \tag{2}$$

Write $(x-1)^{\underline{p-1}} = \sum_{i=0}^{p-1} a_i x^i$. Then matching coefficients on both sides of (2) gives

$$a_i \equiv 0 \pmod{p} \text{ for all } 1 \le i < p-1. \tag{3}$$

Since $p \ge 5$, letting $x = p$ gives

$$(p-1)! = (x-1)^{\underline{p-1}} = p^{p-1} + \left(\sum_{i=2}^{p-2} a_i p^i \right) + a_1 p + (p-1)!$$

since $(-1)(-2)\cdots(-p+1) = (-1)^{p-1}(p-1)! = (p-1)!$. Subtracting $(p-1)!$ on both sides,

$$0 = p^{p-1} + \left(\sum_{j=2}^{p-2} a_i p^i \right) + a_1 p.$$

Using (3), $p^3 \mid a_i p^i$ for $2 \le i < p-1$. Hence, since $p \ge 5$, $p^3 \mid p^{p-1} + \sum_{i=2}^{p-2} a_i p^i$. Since p^3 divides the LHS, $p^3 \mid a_1 p$ and $p^2 \mid a_1$. Now $p^3 \mid (kp)^{p-1} + \left(\sum_{i=2}^{p-2} a_i (kp)^i \right)$ as well and we get

$$\begin{aligned}
(kp-1)^{\underline{p-1}} &= (x-1)^{\underline{p-1}}|_{x=pk} \\
&= (kp)^{p-1} + \left(\sum_{j=2}^{p-1} a_i (kp)^i \right) + a_1 kp + (p-1)! \\
&\equiv (p-1)! \pmod{p^3}.
\end{aligned} \tag{4}$$

Now,

$$\begin{aligned}
\binom{pa}{pb} &= \frac{(pa)^{\underline{pb}}}{(pb)!} \\
&= \frac{\prod_{i=a-b+1}^{a} [(pi)(pi-1)^{\underline{p-1}}]}{\prod_{i=1}^{b} [(pi)(pi-1)^{\underline{p-1}}]} \\
&= \frac{a^{\underline{b}}}{b!} \left[\prod_{i=1}^{b} \frac{[p(i+a-b)-1]^{\underline{p-1}}}{(pi-1)^{\underline{p-1}}} \right]
\end{aligned} \tag{5}$$

By (4), $[p(i+a-b)-1]^{\underline{p-1}} \equiv (pi-1)^{\underline{p-1}} \pmod{p^3}$. Hence (5) becomes $\binom{a}{b}$ modulo p^3, as needed. □

3.1 Problems

1. [3] Prove that for prime $p \geq 5$,
$$p^2 | (p-1)! \left(1 + \frac{1}{2} + \cdots + \frac{1}{p-1}\right).$$

2. [3.5] (APMO 2006/3) Prove that for prime $p \geq 5$, $\binom{p^2}{p} \equiv p \pmod{p^5}$.

3. [3.5] (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.

4. [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.[1]

5. [4-5] (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.

4 Unique Factorization

We prove that when K be a field, unique factorization holds in $K[x]$. It is the same strategy used to prove that integers can be factored uniquely. (For definitions of ring, field, and integral domain, see Lecture 8.)

First, we define what exactly unique factorization means. Let R be an integral domain.

Definition 4.1: An element $a \in R$ is **irreducible** if it is not a unit, and its only factors are units and associates. A unit is an invertible element in R, while an associate of a is a unit times a.

For the positive integers we often just say a is irreducible if $a \neq 1$, and its only factors are 1 and itself. However, if we work with the integers, then there will also be the factors -1 and $-a$, and we don't want to view these as different. For example, 5 is irreducible over the integers because its only factors are units, ± 1, and associates, ± 5.

Definition 4.2: A **unique factorization domain (UFD)** is a integral domain where factoring terminates and every nonzero, nonunit element factors uniquely into irreducible elements. That is, if
$$a = p_1 \dots p_m = q_1 \dots q_n,$$
and $p_1, \dots, p_m, q_1, \dots, q_n$ are irreducible elements, then $m = n$ and we can reorder the q_i's so that p_i is an associate of q_i, for each i.

[1] Hint: A polynomial of degree n over a field (such as $\mathbb{Z}/p\mathbb{Z}$) can have at most n zeros.

For example, we regard $6 = 2 \cdot 3 = -2 \cdot -3$ as the same factorization.

Unique factorization doesn't hold for all domains—for example, consider $\mathbb{Z}[\sqrt{-5}]$, that is, numbers of the form $a + b\sqrt{-5}$. Then

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$$

are two factorizations of 6 into irreducible elements.

The notion of a prime is related to that of an irreducible element. People use them as synonyms in elementary math—because they coincide for the integers—but the distinction between them will be quite important for us.

Definition 4.3: A prime in R is an element p, not a unit, such that if $p|ab$ then $p|a$ or $p|b$.

This tells us that if a prime p divides a, then *no matter how we factor* a, we can't avoid p dividing one element of a. The connection between primes, irreducibles, and unique factorization is given by the following.

Lemma 4.4: If R is a ring where factoring terminates, and every irreducible element is prime, then R is a UFD. Conversely, in a UFD, every irreducible element is prime.

Proof. Suppose $a = p_1 \dots p_m = q_1 \dots q_n$ are two factorizations into irreducible elements. Since p_1 is irreducible, it is prime, and hence must divide one of the q_i. Since q_i is irreducible, its only factors are units and associates, so p_1 must be associated with q_i. Then we can cancel them, leaving a unit. Repeating this process, every factor in the left factorization is paired with one in the right factorization.

For the converse, suppose p is irreducible and $p|ab$. Then $pd = ab$ for some d. Factoring a, b, and d shows that p must divide one of the factors of a or b by unique factorizaton. □

(Note that primes are always irreducible, because if $p = ab$ were a proper factorization, then $p \nmid a$ and $p \nmid b$.)

The main strategy for proving unique factorization is the following.

1. Show that the ring R in question (here, $K[x]$) admits **division with remainder**, with some measure of size so that the remainder is smaller than the quotient.

2. Show that if we have division of remainder, then **greatest common divisors** exist, and moreover that they have the nice property given by Bézout's Theorem.

3. Show that this implies that all irreducible elements are prime, and hence R is a UFD.

The advantage of such an abstract approach lies in the fact that it works for a variety of different number systems. In particular, once we've shown items 2 and 3, then given any ring, we only have to show that we can have division with remainder, and it will follow that it is a UFD. This simultaneously shows unique factorization for $\mathbb{Z}$, $K[x]$, and even $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$.[2]

In the language of abstract algebra, the above steps are phrased as follows:

1. R is an Euclidean domain.

[2]The converse is not true; a UFD is not necessarily a PID or Euclidean domain. For example $\mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$ is a UFD but not an Euclidean domain.

2. An Euclidean domain is a principal ideal domain.

3. A principal ideal domain is a unique factorization domain.

We now carry out this program.

4.1 Step 1: Euclidean domains

Definition 4.5: An integral domain R is an **Euclidean domain** if there is a function $|\cdot| : R \to \mathbb{N}_0$ (called the norm) such that the following hold.

1. $|a| = 0$ iff $a = 0$.

2. For any nonzero $a, b \in R$ there exist $q, r \in R$ such that $b = aq + r$ and $|r| < |a|$.

Note that both the integers $\mathbb{Z}$ and $K[x]$ are Euclidean domains. The norm on $\mathbb{Z}$ is simply the absolute value, while the norm on $K[x]$ is the degree of the polynomial. Theorem 1.1 shows that $K[x]$ is an Euclidean domain.

4.2 Step 2: Euclidean domain $\Longrightarrow$ PID

We'd like to prove Bézout's Theorem for an Euclidean domain, that given a, b in R there exists a greatest common divisor g and s, t so that $as + bt = g$. Rather than thinking of this as an equation in variables s, t, we can think of it as an equation in sets (a) and (b), where (x) denotes the set of multiples of x. For two sets S, T we define $S + T = \{s + t | s \in S, t \in T\}$; then it turns out what we want is

$$(a) + (b) = (g).$$

(See Lemma 4.8 below.)

Definition 4.6: An **ideal** in a ring R is a subset I such that if $a, b \in I$ then $ra, a+b \in I$ for any $r \in R$. A principal ideal is an ideal generated by one element, that is, there is a a such that $I = \{ra | r \in R\}$. We write $I = (a)$.

A **principal ideal domain** (PID) is a integral domain where every ideal is principal.

Theorem 4.7: An Euclidean domain is a PID.

Proof. Let R be an Euclidean domain, $I \subseteq R$ and ideal, and b be the nonzero element of smallest norm in I. Suppose $a \in I$. Then we can write $a = qb + r$ with $0 \leq r < |b|$, but since b has minimal nonzero norm, $r = 0$ and $b|a$. Thus $I = (b)$ is principal. □

Lemma 4.8: A PID satisfies Bézout's Theorem.

Proof. Let R be a PID. Since every ideal in R is principal, for every a, b (not both 0) we have $(a) + (b) = (d)$ for some $d \in R$. (Note the sum of two ideals is an ideal—check this for yourself.) This says there exist $s, t \in R$ such that

$$as + bt = d.$$

From this, any divisor of a, b must divide d. Furthermore, d must divide both a and b since $a = a + 0$ and $b = 0 + b$ are both in $(a) + (b) = (d)$. In other words, d is the greatest common divisor of a, b. □

4.3 Step 3: PID $\Longrightarrow$ UFD

Theorem 4.9: A PID is a UFD.

Proof. Suppose p is irreducible; we show p is prime. Suppose $p|ab$ but p does not divide a. Then using Bezout's Theorem and the fact that a and p are relatively prime, we get $as + pt = 1$ for some s, t. Multiply by b to get

$$abs + ptb = b.$$

Since $p|ab|abs, p|ptb$, we have $p|b$. This shows that irreducible elements are prime in $\mathbb{Z}$.

It remains to show factoring terminates.[3] Otherwise, there would be an infinite sequence of nonassociated elements $a_1, a_2, \ldots \in R$ such that $a_{i+1}|a_i$. Then $(a_1) \subset (a_2) \subset \cdots$. However, $\bigcup_{i\geq 1}(a_i)$ is an ideal, so it is principal, say generated by b. Then $b \in (a_i)$ for some i; this implies that $(b) = (a_i)$. Hence $(a_i) = (a_{i+1}) = \cdots$, a contradiction.

Since irreducible elements are prime and every nonzero element of R factors into irreducibles, R is a UFD. □

Corollary 4.10: $\mathbb{Z}$ and $K[x]$ are UFDs.

4.4 Gauss's argument

We've shown that $K[x]$ is a UFD, but the argument above does not show that $\mathbb{Z}[x]$ is a UFD, because division with remainder fails for $\mathbb{Z}[x]$. We will need a further argument. The basic idea is that a polynomial factors in $\mathbb{Z}[x]$ the same way it does in $\mathbb{Q}[x]$, except with its factors adjusted by constants so the coefficients are in $\mathbb{Z}$.

Let R be a UFD and let K be the field of fractions of R. That is, K consists of the numbers $\frac{a}{b}$ where $a, b \in R$ and $b \neq 0$, and we say $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$. For example, $\mathbb{Q}$ is the field of fractions for $\mathbb{Z}$.

Definition 4.11: A nonzero polynomial $f \in R[x]$ is said to be **primitive** if all its coefficients do not have a common proper divisor; equivalently, there does not exist a prime $p \in R$ such that $p|f$.

Lemma 4.12: If R is an integral domain, then so is $R[x]$.

Proof. Take any $p, q \in R[x]$ not equal to 0. We can write

$$p = \sum_{i=0}^{m} a_i x^i,\ a_m \neq 0$$
$$q = \sum_{i=0}^{n} b_i x^i,\ b_n \neq 0$$

Then the leading coefficient of pq is $a_m b_n x^{m+n}$. It is nonzero because since R is an integral domain, $a_m, b_n \neq 0$ imply that $a_m b_n \neq 0$. Hence $pq \neq 0$. This shows that $R[x]$ is an integral domain. □

[3]This argument is not needed for our purposes: Both $\mathbb{Z}$ and $K[x]$ are Euclidean domains, and factoring must terminate for them because factors always have smaller norm (absolute value and degree, respectively).

Lemma 4.13 (Gauss's lemma)**:** (A) An element of R is prime in $R[x]$ iff it is a prime in R. Hence if a prime p of R divides a product fg of polynomials in $R[x]$, then $p|f$ or $p|g$. (B) The product of primitive polynomials in $R[x]$ is primitive.

Proof. If $p \in R$ is nonzero, and a prime in $R[x]$, then it is a prime in the subring R.

Conversely, let p be any prime element in R. Then $R/(p)$ is an integral domain[4] so by lemma 4.12, $R/(p)[x]$ is an integral domain.

Suppose $p|fg$ for $f, g \in R[x]$. Then in $R/(p)[x]$, $\overline{fg} = \overline{f}\overline{g} = 0$. Since $R/(p)[x]$ is an integral domain, either $\overline{f} = 0$ or $\overline{g} = 0$. In other words, either $p|f$ or $p|g$ in $R[x]$. Thus p is a prime in $R[x]$.

If f, g are primitive, then $p \nmid f$ and $p \nmid g$ for all primes $p \in R$. Since p is also prime in $R[x]$, $p \nmid fg$. Hence fg is not divisible by any prime in R, and it is primitive. □

Lemma 4.14: Every nonconstant polynomial $f \in K[x]$ can be written uniquely (up to multiplication by units) in the form $f = cf_0$, where $c \in K$ and f_0 is a primitive polynomial in $R[x]$.

Proof. Each coefficient a_i of f is in the form $\frac{p_i}{q_i}$, where $p_i, q_i \in R$. We can find a nonzero $t \in R$ such that t is divisible by each denominator (for, example, take t to be the product of the denominators). Then we can write

$$tf = f_1,$$

where $f_1 \in R[x]$. Let $s \in R$ be a greatest common divisor of the coefficients of f_1. Then we have

$$f = \frac{s}{t} f_0$$

in $K[x]$ where $f_0 \in R[x]$ and the coefficients of f_0 have no common divisor. This gives the desired representation.

Next we check uniqueness. Suppose

$$f = cf_0 = c'f_0',$$

where $c, c' \in K$ and $f_0, f_0' \in R[x]$ are primitive. Multiply by an element of R to "clear denominators," to reduce to the case where $c, c' \in R$. Now take any prime $p|c$. Since p is prime in $R[x]$, $p|c'$ or $p|f_0'$. The second is impossible since f_0' is primitive. Hence $p|c'$, and we can cancel p. Continuing in this way, we get that c and c' share the same prime factors with the same multiplicities. Hence c, c' are associates. □

Lemma 4.15: Let f_0 be a primitive polynomial and let $g \in R[x]$. If $f_0|g$ in $K[x]$ then $f_0|g$ in $R[x]$.

Proof. If $f_0|g$ in $K[x]$, then we can write $g = f_0 h$ where $h \in K[x]$. We need to show $h \in R[x]$. By lemma 4.14, we can write $h = ch_0$, where $c \in K$ and h_0 is primitive. Then $g = cf_0h_0$. By lemma 4.13, the product f_0h_0 of primitive polynomials is primitive. We

[4]If I is an ideal, then R/I is the quotient ring: Two elements a, b in R are considered to be the same in R/I if they differ by an element in I. Keep in mind the example $R = \mathbb{Z}$; then $R/(p)$ is simply the integers modulo p.

Now $R/(p)$ is an integral domain, because if $ab = 0$ in $R/(p)$, then $ab \in (p)$, i.e. p divides one of a, b. But since p is prime either $p|a$ or $p|b$, which translates back into $a = 0$ or $b = 0$ in $R/(p)$.

can write $c = \frac{s}{t}$, where $s, t \in R$ have no common factors. If a prime p in R divides the denominator t then $p \nmid s$ so $p | f_0 h_0$, contradicting the fact that $f_0 h_0$ is primitive. Hence t is a unit, and $c \in R$. Then $h = ch_0 \in R[x]$, so $f_0 | g$ in $R[x]$.

□

Lemma 4.16: Let f be a nonzero element of $R[x]$. Then f is an irreducible element of $R[x]$ iff it is an irreducible element of R or a primitive irreducible polynomial in $K[x]$.

Proof. If $f \in R$, then the only factors of f in $R[x]$ are in R, so f is irreducible in R iff it is irreducible in $R[x]$. This proves the lemma for $f \in R$. Now suppose $f \notin R$.

If $f \in R[x]$ is a primitive polynomial irreducible in $K[x]$, then it is irreducible in $R[x]$.

If $f \in R[x]$ is not primitive, then it is reducible in $R[x]$. Thus it suffices to show if $f \in R[x]$ is reducible in $K[x]$, then it is reducible in $R[x]$. Suppose $f \in R[x]$, and $f = gh$ is a proper factorization of f in $K[x]$. We can write $g = cg_0, h = c'h_0$ where $c, c' \in K$ and g_0, h_0 are primitive. Since g_0 and h_0 are both primitive, so is $g_0 h_0$. Then $f = cc'(g_0 h_0)$, so by uniqueness in lemma 4.14, cc' must be in R (and is the gcd of the coefficients of f). Thus $f = (cc')g_0 h_0$ is a proper factorization of f in $R[x]$ as well, as needed. □

Theorem 4.17: The ring $R[x]$ is a unique factorization domain.

Proof. It suffices to show that every irreducible element f of $R[x]$ is a prime element, and that factoring terminates. By Lemma 4.16, f is either irreducible in R or a primitive irreducible polynomial in $K[x]$. In the first case f is prime in R (R is a UFD) and hence prime in $R[x]$ by Lemma 4.13.

In the second case, f is primitive irreducible in $K[x]$, thus a prime in $K[x]$, since $K[x]$ is a UFD. Hence $f|g$ or $f|h$ in $K[x]$. By Lemma 4.15, $f|g$ or $f|h$ in $R[x]$. This shows f is prime.

A polynomial $f \in R[x]$ can only be the product of at most $\deg(f)$ many polynomials p_i of positive degree in $R[x]$ because the sum of the degrees of the p_i must equal $\deg(f)$. Factor terminates for the factors of f in R because factoring terminates in the UFD R, and the primes in R dividing f are the primes dividing every coefficient of f.

Hence $R[x]$ is a UFD. □

Corollary 4.18: $\mathbb{Z}[x]$ is a UFD.

If R is a UFD then $R[x_1, \ldots, x_n]$ is a UFD.

Proof. Since $\mathbb{Z}$ is a UFD, so is $\mathbb{Z}[x]$. The second statement follows from Theorem 4.17 by induction. □

4.5 More Proofs

Theorem 4.19 (Chinese Remainder Theorem)**:** If polynomials $Q_1, \ldots, Q_n \in K[x]$ are pairwise relatively prime, then the system $P \equiv R_i \pmod{Q_i}, 1 \leq i \leq n$ has a unique solution modulo $Q_1 \cdots Q_n$.

Proof. Let $Q = Q_1 \cdots Q_n$. Note Q_i and $\frac{Q}{Q_i}$ are relatively prime. Hence by Bézout's Theorem there exist f_i and g_i so that

$$f_i Q_i + g_i \frac{Q}{Q_i} = 1.$$

Now

$$(1 - q_i f_i)R_i = R_i g_i \frac{Q}{Q_i}$$

is congruent to R_i modulo Q_i, and zero modulo Q_j for $j \neq i$. Hence

$$P = \sum_{i=1}^{n} (1 - q_i f_i) R_i$$

is the desired polynomial.

For uniqueness, suppose P_1 and P_2 satisfy the conditions of the problem. Then $P_1 - P_2$ is zero modulo Q_i. Since the Q_i are pairwise relatively prime, $P_1 - P_2 \equiv 0 \pmod{Q_1 \cdots Q_n}$. □

Theorem 4.20 (Rational Roots Theorem)**:** Suppose that R is a UFD and K its fraction field. (For instance, take $R = \mathbb{Z}$ and $K = \mathbb{Q}$.) Suppose $f(x) = a_n x^n + \cdots + a_0 \in R[x]$ and $a_n \neq 0$. Then all roots of f in K are in the form

$$\frac{\text{factor of } a_0}{\text{factor of } a_n}.$$

In particular, if $a_n = \pm 1$, then all roots of f in K are actually in R.

Proof. Write $x = \frac{r}{s}$ in simplest terms. Then multiplying through by s^n gives

$$a_n \left(\frac{r}{s}\right)^n + \cdots + a_1 \left(\frac{r}{s}\right) + a_0 = 0$$
$$a_n r^n = -s(a_{n-1} r^{n-1} + \cdots + a_1 r s^{n-2} + a_0 s^{n-1}).$$

Since s and r have no common factor, s must divide a_n. (This uses the fact that R is a UFD—how?). Rewriting as

$$a_0 s^n = -r(a_n r^{n-1} + \cdots + a_1 s^{n-1})$$

makes it clear r divides a_0. □

Remark 4.21: In particular, if $a_n = 1$, then all roots of f in K are in R. A ring is said to be normal if whenever $t \in K$ is a root of a monic polynomial in $R[x]$, then $t \in R$. Thus the above shows that UFDs are normal.

4.6 Problems

1. (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.)

2. For a field K, let $K(x)$ be the field of rational functions, that is,

$$K(x) = \left\{ \frac{p}{q} \mid p, q \in K[x] \right\}.$$

Let f and g be rational functions such that $f(g(x)) = x$. Prove that f and g are both in the form $\frac{ax+b}{cx+d}$ with $ad \neq bc$.