Number Theory for Polynomials

In these notes we develop the basic theory of polynomials over a field. We will use this theory to construct finite fields.

Definition: Polynomials Over a Field
Let $\mathbb{F}$ be a field. A **polynomial** over $\mathbb{F}$ is a formal sum

$$f(x) = \sum_{k=0}^{n} a_k x^k = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where $a_0, a_1, \ldots, a_n \in \mathbb{F}$, and x is an indeterminate. We will let $\mathbb{F}[x]$ denote the set of all polynomials over $\mathbb{F}$.

Note that a polynomial is defined to be a **formal sum**, not a function. For example, the polynomial

$$f(x) = x^7 - x$$

over $\mathbb{Z}_7$ has the property that $f(a) = 0$ for all $a \in \mathbb{Z}_7$, but this does not mean that f is equal to zero polynomial. In general, two polynomials are only considered equal if they have the same coefficients.

The **degree** of a polynomial f, denoted $\deg(f)$, is the largest power of x whose coefficient in $f(x)$ is nonzero. Thus, if

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

and $a_n \neq 0$, then f has degree n. In this case, $a_n x^n$ is called the **leading term** of $f(x)$, and a_n is the **leading coefficient**. A polynomial is **monic** if its leading coefficient is equal to one.

We can add and multiply polynomials in the usual fashion. Addition of polynomials in associative, commutative, has an identity (the zero polynomial), and inverses,

and multiplication of polynomials is associative, commutative, has an identity element (the constant polynomial 1), and distributes over addition. Thus the set $\mathbb{F}[x]$ of all polynomials over $\mathbb{F}$ forms a commutative ring, known as the **polynomial ring** over $\mathbb{F}$.

Finally, it is possible to divide one polynomial by another. The result is both a quotient and a remainder, as with division of integers.

Theorem 1 Polynomial Division

Let $\mathbb{F}$ be a field, and let $f, g \in \mathbb{F}[x]$, with $g \neq 0$. Then there exist a unique pair of polynomials $q, r \in \mathbb{F}[x]$ with $\deg(r) < \deg(g)$ so that

$$f(x) \;=\; q(x)\, g(x) + r(x)$$

PROOF To prove existence, we proceed by induction on $\deg(f)$. The base case is that $\deg(f) < \deg(g)$, in which case $q(x) = 0$ and $r(x) = f(x)$ suffices. Now suppose that $\deg(f) \geq \deg(g)$, say

$$f(x) \;=\; a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0 \quad \text{and} \quad g(x) \;=\; b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$$

where $a_m \neq 0$, $b_n \neq 0$, and $m \geq n$. Let

$$h(x) = f(x) - a_m b_n^{-1} x^{m-n} g(x).$$

Note that the leading terms cancel in the subtraction, so $\deg(h) < \deg(f)$. By our induction hypothesis there exist $q, r \in \mathbb{F}[x]$ with $\deg(r) < \deg(g)$ such that

$$h(x) \;=\; q(x)\, g(x) + r(x).$$

Then

$$f(x) \;=\; a_m b_n^{-1} x^{m-n} g(x) + h(x) \;=\; \big(a_m b_n^{-1} x^{m-n} + q(x)\big)\, g(x) + r(x)$$

which proves existence.

For uniqueness, suppose that

$$q_1(x)\, g(x) + r_1(x) \;= q_2(x)\, g(x) + r_2(x)$$

for some $q_1, q_2, r_1, r_2 \in \mathbb{F}[x]$ with $\deg(r_1) < \deg(g)$ and $\deg(r_2) < \deg(g)$. Rearranging gives

$$\big(q_1(x) - q_2(x)\big)\, g(x) \;=\; r_2(x) - r_1(x).$$

The right side has smaller degree than g, so it must be the case that $q_1(x) = q_2(x)$, and it follows easily that $r_1(x) = r_2(x)$. ■

The polynomial $q(x)$ is called the **quotient** of $f(x)$ divided by $g(x)$, and $r(x)$ is the **remainder**. Note that if $f(x)$ and $g(x)$ are monic polynomials then the quotient $q(x)$ must be as well, though $r(x)$ need not be.

Number Theory with Polynomials

Because polynomial division is so similar to integer division, many of the basic definitions and theorems of elementary number theory work for polynomials. We begin with the following definition.

Definition: Divisibility
Let $\mathbb{F}$ be a field, and let $f, g \in \mathbb{F}[x]$. We say that f **divides** g, denoted

$$f(x) \mid g(x)$$

if there exists an $q \in F[x]$ so that $g(x) = f(x)\,q(x)$.

A few notes about this definition:

1. This definition obeys all of the familiar rules for divisibility. For example,

   $$f(x) \mid g(x) \quad \text{and} \quad f(x) \mid h(x) \qquad \Rightarrow \qquad f(x) \mid g(x) + h(x)$$

   for any $f, g, h \in \mathbb{F}[x]$. Similarly,

   $$f(x) \mid g(x) \quad \text{and} \quad g(x) \mid h(x) \qquad \Rightarrow \qquad f(x) \mid h(x).$$

2. Any nonzero constant $c \in \mathbb{F}^\times$ divides every polynomial, since

   $$f(x) \;=\; c\left(c^{-1} f(x)\right).$$

   Thus nonzero constants play the same role for polynomials that 1 and -1 play in the integers.

In the same way that it often makes sense to restrict to positive integers when discussing divisibility of integers, it often makes sense to restrict to monic polynomials when discussing divisibility of polynomials.

Definition: Greatest Common Divisor
Let $\mathbb{F}$ be a field, and let $f(x), g(x) \in \mathbb{F}[x]$, not both zero. A **greatest common divisor** of $f(x)$ and $g(x)$ is a monic polynomial $d(x) \in \mathbb{F}[x]$ of maximum degree that divides both $f(x)$ and $g(x)$.

We can use the Euclidean algorithm to compute the greatest common divisor of two polynomials, just as though they were integers, and this lets us prove the following theorem.

Theorem 2 Bézout's Lemma

Let $\mathbb{F}$ be a field, and let $f(x)$ and $g(x)$ be polynomials over $\mathbb{F}$, not both zero. Then $f(x)$ and $g(x)$ have a unique greatest common divisor $d(x)$, and there exist polynomials $a(x)$ and $b(x)$ over $\mathbb{F}$ so that

$$a(x)\,f(x) + b(x)\,g(x) \;=\; d(x).$$

PROOF Suppose without loss of generality that $\deg(g) \leq \deg(f)$. We proceed by induction on $\deg(g)$. The base case is that g is the zero polynomial, in which case the only greatest common divisor is $d(x) = a_n^{-1} f(x)$, where a_n is the leading coefficient of f, and

$$a_n^{-1}\,f(x) + 0\,g(x) \;=\; d(x).$$

Now suppose that $g \neq 0$. Then there exist $q(x), r(x) \in \mathbb{F}[x]$ with $\deg(r) < \deg(g)$ so that

$$f(x) \;=\; q(x)\,g(x) + r(x).$$

Note that any common divisor of $f(x)$ and $g(x)$ is also a common divisor of $g(x)$ and $r(x)$, and vice-versa. By our induction hyopothesis, $g(x)$ and $r(x)$ have a unique greatest common divisor $d(x)$, so this is the unique greatest common divisor of $f(x)$ and $g(x)$ as well. Moreover, by our induction hypothesis there exist polynomials $a(x)$ and $b(x)$ so that

$$a(x)\,g(x) + b(x)\,r(x) \;=\; d(x).$$

Since $r(x) = f(x) - q(x)\,g(x)$, it follows that

$$b(x)\,f(x) + \big(a(x) - b(x)\,q(x)\big)g(x) \;=\; d(x). \qquad \blacksquare$$

This lets us prove the analog of prime factorization for polynomials. We begin by introducing the analog of prime numbers.

Definition: Irreducible Polynomial
Let $\mathbb{F}$ be a field, and let $f(x)$ be a monic polynomial over $\mathbb{F}$ with $\deg(f) \geq 1$. We say that $f(x)$ is **irreducible** if the only monic divisors of $f(x)$ are 1 and $f(x)$.

EXAMPLE 1 Irreducible Polynomials over $\mathbb{C}$ and $\mathbb{R}$

The only irreducible polynomials over $\mathbb{C}$ are the monic linear polynomials

$$\{x - a \mid a \in \mathbb{C}\}.$$

By the fundamental theorem of algebra, every monic polynomial over $\mathbb{C}$ can be expressed as a product of these irreducible polynomials.

Over $\mathbb{R}$, every monic linear polynomial is irreducible, as are quadratic polynomials like $x^2 + 1$. Indeed, any quadratic polynomial of the form $x^2 + bx + c$ for which $b^2 - 4c < 0$ is irreducible over $\mathbb{R}$. It is not hard to show that these are the only irreducible polynomials over $\mathbb{R}$. For if $f(x)$ is any polynomial over $\mathbb{R}$, then either f has a real root, in which case it has a linear factor, or it has at least one pair of complex conjugate roots $a \pm bi$, in which case

$$\big(x - (a + bi)\big)\big(x - (a - bi)\big) = x^2 - 2ax + (a^2 + b^2)$$

is a factor of $f(x)$. ■

EXAMPLE 2 Irreducible Polynomials Over $\mathbb{Z}_2$

There are two linear polynomials over $\mathbb{Z}_2$ (namely x and $x + 1$), both of which are irreducible. There are four quadratic polynomials:

$$x^2, \qquad x^2 + x, \qquad x^2 + 1, \qquad x^2 + x + 1.$$

However,

$$x^2 = (x)(x), \qquad x^2 + x = x(x + 1), \qquad \text{and} \qquad x^2 + 1 = (x + 1)(x + 1)$$

so the only irreducible quadratic polynomial over $\mathbb{Z}_2$ is $x^2 + x + 1$.

There are also eight cubic polynomials over $\mathbb{Z}_2$, of which six can be factored:

$$x^3, \quad x^2(x + 1), \quad x(x + 1)^2, \quad (x + 1)^3, \quad x(x^2 + x + 1), \quad (x + 1)(x^2 + x + 1).$$

The remaining two are irreducible:

$$x^3 + x + 1 \qquad \text{and} \qquad x^3 + x^2 + 1.$$

This process continues, and indeed there are irreducible polynomials of every degree over $\mathbb{Z}_2$. This is not easy to prove, but it *is* easy to prove that there are infinitely many irreducible polynomials. In particular, if $p_1(x), \ldots, p_n(x)$ are irreducible, then $p_1(x) \cdots p_n(x) + 1$ is not divisible by any $p_i(x)$, so it must be divisible by an irreducible polynomial not on this list. ■

EXAMPLE 3 Irreducible Quadratics Over $\mathbb{Z}_p$

If p is prime, then a quadratic of the form $x^2 - a$ is irreducible over $\mathbb{Z}_p$ if and only if a is a quadratic non-residue modulo p. More generally, every quadratic polynomial over $\mathbb{Z}_p$ can be written as $(x + b)^2 - a$ for some $a, b \in \mathbb{Z}_p$, and such a polynomial is irreducible if and only if a is a quadratic non-residue. Thus there are exactly

$$\frac{p(p-1)}{2}$$

irreducible quadratic polynomials over $\mathbb{Z}_p$, since there are p choices for b and $(p-1)/2$ choices for a. ■

Lemma 3 Euclid's Lemma for Polynomials

Let $\mathbb{F}$ be a field, let $p(x)$ be an irreducible polynomial over $\mathbb{F}$, and let $f, g \in \mathbb{F}[x]$. If $p(x) \mid f(x)\,g(x)$, then either $p(x) \mid f(x)$ or $p(x) \mid g(x)$.

PROOF Suppose that $p(x) \mid f(x)\,g(x)$ but $p(x) \nmid f(x)$. Then the greatest common divisor of $p(x)$ and $f(x)$ must be 1, so by Bézout's lemma there exist polynomials $a(x)$ and $b(x)$ over $\mathbb{F}$ so that

$$a(x)\,p(x) + b(x)\,f(x) \;=\; 1.$$

Multiplying through by $g(x)$ gives

$$a(x)\,g(x)\,p(x) + b(x)\,f(x)\,g(x) \;=\; g(x).$$

Then $p(x)$ divides the left side since $p(x) \mid f(x)\,g(x)$, and hence $p(x) \mid g(x)$. ■

Irreducible factorization of polynomials follows immediately.

Theorem 4 Irreducible Factorization of Polynomials

Let $\mathbb{F}$ be a field, and let $f(x)$ be a monic polynomial over $\mathbb{F}$. Then there exist irreducible polynomials $q_1(x), \ldots, q_n(x)$ such that

$$f(x) \;=\; q_1(x)\,q_2(x)\,\cdots\,q_n(x).$$

Moreover, $q_1(x), \ldots, q_n(x)$ are unique up to reordering of the factors.

For example, it follows from this theorem that every polynomial over $\mathbb{R}$ can be factored into irreducible linear and quadratic factors, and this factorization is unique up to reordering of the factors.

Modular Arithmetic

We can define modular arithmetic for polynomials in much the same way as we do for numbers.

Definition: Congruence Modulo $m(x)$
Let $\mathbb{F}$ be a field, let $f(x), g(x) \in \mathbb{F}[x]$, and let $m(x)$ be a monic polynomial over $\mathbb{F}$. We say that $f(x)$ and $g(x)$ are **congruent modulo $m(x)$**, denoted

$$f(x) \equiv g(x) \pmod{m(x)},$$

if $m(x)$ divides the difference $f(x) - g(x)$.

It is easy to prove that congruence modulo $m(x)$ is an equivalence relation on $\mathbb{F}[x]$. There is a simple way of describing the congruence classes modulo $m(x)$.

Proposition 5 Congruence Classes Modulo $m(x)$

Let $\mathbb{F}$ be a field, and let $m(x)$ be a monic polynomial over $\mathbb{F}$. Then for every $f(x) \in \mathbb{F}[x]$, there exists a unique $r(x) \in \mathbb{F}[x]$ such that $\deg(r) < \deg(m)$ *and*

$$f(x) \equiv r(x) \pmod{m(x)}.$$

PROOF Let $f(x) \in \mathbb{F}[x]$. Since $m \neq 0$, there exist polynomials $q(x)$ and $r(x)$ over $\mathbb{F}$ with $\deg(r) < \deg(m)$ so that

$$f(x) = q(x)\, m(x) + r(x)$$

Then $f(x) \equiv r(x) \pmod{m(x)}$, as desired.

To prove uniqueness, suppose that $r_1(x)$ and $r_2(x)$ are polynomials over $\mathbb{F}$ with $\deg(r_1) < \deg(m)$ and $\deg(r_2) < \deg(m)$ such that

$$f(x) \equiv r_1(x) \pmod{m(x)} \qquad \text{and} \qquad f(x) \equiv r_2(x) \pmod{m(x)}.$$

Then $r_1(x) \equiv r_2(x) \pmod{m(x)}$, so $m(x)$ divides $r_1(x) - r_2(x)$. But $r_1(x) - r_2(x)$ has smaller degree than $m(x)$, so $r_1(x) - r_2(x)$ must be zero, and hence $r_1(x) = r_2(x)$. ■

If $\mathbb{F}$ is a field and $m(x)$ is a monic polynomial over $\mathbb{F}$, we let $\mathbb{F}[x]/\big(m(x)\big)$ denote the set of all congruence classes of polynomials modulo $m(x)$. Then $\mathbb{F}[x]/\big(m(x)\big)$ forms a ring under the operations of addition and multiplication modulo $m(x)$.

EXAMPLE 4 Real Polynomials Modulo $x^2 + 1$

Consider the ring $\mathbb{R}[x]/\big(x^2+1\big)$. By Proposition 5, for every polynomial $f(x)$ over $\mathbb{R}$ there exist $a, b \in \mathbb{R}$ so that

$$f(x) \equiv a + bx \pmod{x^2+1}.$$

That is, the elements of $\mathbb{R}[x]/\big(x^2+1\big)$ are precisely the polynomials of the form $a+bx$ for $a, b \in \mathbb{R}$. But observe that

$$x^2 \equiv -1 \pmod{x^2+1}.$$

It follows that $\mathbb{R}[x]/\big(x^2+1\big)$ is isomorphic to the ring $\mathbb{C}$ of complex numbers. ■

Corollary 6 Number of Congruence Classes

Let p be a prime number, and let $m(x)$ be a monic polynomial in $\mathbb{Z}_p[x]$ of degree n. Then the ring $\mathbb{Z}_p[x]/\big(m(x)\big)$ has exactly p^n elements.

PROOF If $r(x)$ is a polynomial over $m(x)$ of degree less than n, then $r(x)$ can be written

$$r(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_0, \ldots, a_{n-1} \in \mathbb{Z}_p$. There are p choices for each of $a_0, \ldots, a_{n-1}$, and thus there are exactly p^n such polynomials. ■

EXAMPLE 5 The Field with Four Elements

Consider the ring $\mathbb{Z}_2[x]/\big(x^2+x+1\big)$. Since x^2+x+1 has degree 2, this ring has exactly $2^2 = 4$ elements, namely 0, 1, x, and $x+1$. But note that 1 is its own multiplicative inverse, and

$$x(x+1) = x^2 + x \equiv 1 \pmod{x^2+x+1},$$

so x and $x+1$ are multiplicative inverses. Thus $\mathbb{Z}_2[x]/\big(x^2+x+1\big)$ is a field with four elements. ■

The following theorem lets us construct finite fields using polynomials.

Theorem 7 Constructing Finite Fields

Let $\mathbb{F}$ be a field, and let $m(x)$ be an irreducible polynomial over $\mathbb{F}[x]$. Then $\mathbb{F}[x]/\big(m(x)\big)$ is a field.

PROOF We must show that every element of $\mathbb{F}[x]/\big(m(x)\big)$ has a multiplicative inverse modulo $m(x)$. So let $r(x)$ be a nonzero polynomial over $\mathbb{F}$, and suppose that $\deg(r) < \deg(m)$. Since $m(x)$ is irreducible, then greatest common divisor of $r(x)$ and $m(x)$ must be 1. By Bézout's lemma, there exist polynomials $a(x)$ and $b(x)$ so that

$$a(x)\,r(x) + b(x)\,m(x) \;=\; 1.$$

Then

$$a(x)\,r(x) \;\equiv\; 1 \;\big(\mathrm{mod}\; m(x)\big),$$

so $a(x)$ is a multiplicative inverse for $r(x)$ in $\mathbb{F}[x]/\big(m(x)\big)$. ■

In particular, if p is prime and $m(x)$ is an irreducible polynomial over $\mathbb{Z}_p$ of degree n, then $\mathbb{Z}_p[x]/\big(m(x)\big)$ is a field with p^n elements.

EXAMPLE 6 The Field with Eight Elements

Recall that the polynomial x^3+x+1 is irreducible over $\mathbb{Z}_2$. Then $\mathbb{Z}_2[x]/\big(x^3+x+1\big)$ should be a field with $2^3 = 8$ elements. Specifically, the elements of $\mathbb{Z}_2[x]/\big(x^3+x+1\big)$ are

$$0, \quad 1, \quad x, \quad x+1, \quad x^2, \quad x^2+1, \quad x^2+x, \quad x^2+x+1,$$

and it is easy to check that

$$x\big(x^2+1\big) \;\equiv\; 1, \qquad x^2\big(x^2+x+1\big) \;\equiv\; 1, \qquad \text{and} \qquad (x+1)(x^2+x) \;\equiv\; 1$$

modulo x^3+x+1. ■

EXAMPLE 7 The Field with p^2 Elements

Let p be an odd prime, and let a be a quadratic non-residue modulo p. Then $x^2 - a$ is an irreducible polynomial over $\mathbb{Z}_p$, so $\mathbb{Z}_p[x]/\big(x^2 - a\big)$ is a field with p^2 elements, namely

$$\{b + cx \mid b, c \in \mathbb{Z}_p\}.$$

Note that

$$x^2 \equiv a \ \big(\text{mod } x^2 - a\big)$$

so x is a square root of a. Thus $\mathbb{Z}_p[x]/\big(x^2 - a\big)$ can be thought of as a field obtained from $\mathbb{Z}_p$ by adjoining a square root of a, with elements of the form

$$\big\{b + c\sqrt{a} \;\big|\; b, c \in \mathbb{Z}_p\big\}. \qquad \blacksquare$$