Arithmetic of Function Fields

Seewoo Lee

Last updated: June 3, 2025

Abstract

This is a note for Berkeley REU happened in Summer 2025. Most of the materials are based on the Rosen's book *Number Theory in Function Fields* [1].

1 Introduction

The goal of this note is to introduce the arithmetic of function fields, which is the analogue of number theory for polynomials. Especially, our main goal is to study various evidences of the following claim:

> A theorem that holds for integers is also true for polynomials (over finite fields), and latter is often easier to prove.

For example, we will see a proof of Fermat's Last Theorem for polynomials, which only requires few pages to prove.

Dictionary between the integers and the polynomials over finite fields can be found in Table 1 of Appendix.

Notations

Let p be a prime number. We denote by $\mathbb{F}_p$ the finite field of order p, which is the field with p elements. We denote the polynomial ring $\mathbb{F}_p[T]$ by A. For each nonzero polynomial $f \in A$, we denote it's norm by $|f| = p^{\deg(f)}$, where $\deg(f)$ is the degree of f, and we set $|0| = 0$.

Exercises

1. Prove that $\mathbb{Z}$ is not a polynomial ring over a field. In other words, show that there is no field k such that $\mathbb{Z} \cong k[T]$ as rings.

2. Think about your favorite theorems in number theory, and try to find their polynomial analogues. Some of them may appear in this note, but some of them may not.

2 Basic number theory and their analogues for polynomials

In this section, we will introduce polynomial analogues of the theorems in number theory, including

- Fundamental Theorem of Arithmetic,
- Chinese Remainder Theorem,
- Fermat's Little Theorem and Euler's Theorem,
- Wilson's Theorem,

2.1 Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic states that every integer greater than 1 can be uniquely expressed as a product of prime numbers, up to the order of the factors. More fancier way to say this is that

Theorem 2.1. $\mathbb{Z}$ is a unique factorization domain (UFD).

The standard proof is based on the following implication:

Theorem 2.2. If R is a Euclidean domain (ED), then R is a principal ideal domain (PID), and hence a UFD.

Recall that R is a Euclidean domain if there exists a function $f : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ such that for any $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $f(r) < f(b)$. Intuitively, R is a Euclidean domain if we can perform the division with remainder, and the function f is a measure of the size of the elements in R. For any (not necessarily finite) field k, we can also divide a polynomial by another polynomial over k, where $\deg : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ works as the function f. This shows that:

Theorem 2.3. The polynomial ring $k[T]$ is a ED, where k is any field. Hence it is a PID, and hence a UFD.

2.2 Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) states that if $n_1, n_2, \ldots, n_k$ are pairwise coprime integers, then the system of congruences

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \ldots, \quad x \equiv a_k \pmod{n_k}$$

has a unique solution modulo $N = n_1 n_2 \cdots n_k$.

Theorem 2.4 (Chinese Remainder Theorem)**.** Let $n_1, n_2, \ldots, n_k$ be pairwise coprime integers and $a_1, a_2, \ldots, a_k$ be integers. Then the system of congruences

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \ldots, \quad x \equiv a_k \pmod{n_k}$$

has a unique solution modulo $N = n_1 n_2 \cdots n_k$. More precisely, the unique solution is given by

$$x \equiv \sum_{i=1}^{k} a_i N_i y_i \pmod{N},$$

where $N_i = N/n_i$ and y_i is the multiplicative inverse of N_i modulo n_i, i.e., $N_i y_i \equiv 1 \pmod{n_i}$.

Proof. The proof is essentially hidden in the following isomorphism:

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

The natural map from the left hand side to the right hand side is given by reducing modulo n_i for each i, and such a map is injective because $n_1, n_2, \ldots, n_k$ are pairwise coprime. Since the size of the both sides are equal, the map is also surjective, hence an isomorphism. Finding the solution to the system of congruences is equivalent to finding an element in $\mathbb{Z}/N\mathbb{Z}$ that maps to $(a_1, a_2, \ldots, a_k)$ under the isomorphism. It is enough to find solution for the equations

$$x_i \equiv 0 \pmod{n_1}, \quad x_i \equiv 0 \pmod{n_2}, \quad \cdots \quad x_i \equiv 1 \pmod{n_i}, \quad \cdots, \quad x_i \equiv 0 \pmod{n_k}$$

for each i, then the solution to the original system of congruences is given by the linear combination of the solutions to these equations. Such x_i has to be a multiple of N_i, and if we write $x_i = N_i y_i$, then we have $N_i y_i \equiv 1 \pmod{n_i}$, which means y_i is the multiplicative inverse of N_i modulo n_i. Such y_i exists and can be found by the Euclidean Algorithm, since N_i and n_i are coprime. □

For example, consider a system of congruences

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}$$

From Euclidean Algorithm, we can write $1 = 2 \cdot 3 - 1 \cdot 5$, which means $5^{-1} \equiv (-1) \pmod{3}$ and $3^{-1} \equiv 2 \pmod{5}$. Then the formula in Theorem 2.4 gives us $x \equiv 2 \cdot 5 \cdot (-1) + 3 \cdot 3 \cdot 2 \pmod{15}$, which simplifies to $x \equiv -10 + 18 \equiv 8 \pmod{15}$.

What is a polynomial analogue of the Chinese Remainder Theorem? We simply replace integers with polynomials over a finite field, and we get the following theorem.

Theorem 2.5 (Chinese Remainder Theorem for Polynomials)**.** Let $g_1(T), g_2(T), \ldots, g_k(T) \in \mathbb{F}_p[T]$ be pairwise coprime polynomials and $a_1(T), a_2(T), \ldots, a_k(T) \in \mathbb{F}_p[T]$ be polynomials. Then the system of congruences

$$f \equiv a_1 \pmod{g_1}, \quad f \equiv a_2 \pmod{g_2}, \quad \ldots, \quad f \equiv a_k \pmod{g_k}$$

has a unique solution modulo $G = g_1 g_2 \cdots g_k$. More precisely, the unique solution is given by

$$f \equiv \sum_{i=1}^{k} a_i G_i b_i \pmod{G},$$

where $G_i = G/g_i$ and b_i is the multiplicative inverse of G_i modulo g_i, i.e., $G_i b_i \equiv 1 \pmod{g_i}$.

Using the exact same method, we can solve a system of congruences. For example, consider

$$\begin{cases} f \equiv 1 \pmod{T} \\ f \equiv T \pmod{T^2+1} \end{cases}$$

We can write $1 = (-T) \cdot T + 1 \cdot (T^2+1)$ (hence T and T^2+1 are coprime), which means $(T^2+1)^{-1} \equiv 1 \pmod{T}$ and $T^{-1} \equiv -T \pmod{T^2+1}$. Then the formula in Theorem 2.5 gives us $f \equiv 1 \cdot (T^2+1) \cdot 1 + T \cdot T \cdot (-T) \pmod{(T^2+1)T}$, which simplifies to $f \equiv T^2 + 1 - T^3 \equiv T^2 + T + 1 \pmod{(T^2+1)T}$.

2.3 Fermat's Little Theorem and Euler's Theorem

Ferma's *Little* (not last!) Theorem states the following:

Theorem 2.6 (Fermat's Little Theorem)**.** Let p be a prime number and a an integer not divisible by p. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Here is a proof using group theory.

Proof. Consider the group $G = (\mathbb{Z}/p\mathbb{Z})^\times$. The order of G is $p-1$, and the order of the subgroup generated by a is a divisor of $p-1$. Thus, by Lagrange's theorem, we have $a^{p-1} \equiv 1 \pmod{p}$, as desired. □

Euler's theorem is a generalization of Fermat's Little Theorem, which considers general moduli. To state Euler's theorem, we need to define the *Euler's totient function* $\varphi(n)$, which counts the number of integers from 1 to n that are coprime to n.

Theorem 2.7 (Euler's Theorem)**.** Let n be a positive integer and a an integer coprime to n. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof. Proof is similar to the proof of Theorem 2.6, where we consider the group $G = (\mathbb{Z}/n\mathbb{Z})^\times$ which has order $\varphi(n)$. □

One may ask how to compute $\varphi(n)$. By CRT again (but for unit groups), we have an isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{k_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_m^{k_m}\mathbb{Z})^\times,$$

where $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ is the prime factorization of n. Thus, we can compute $\varphi(n)$ as

$$\varphi(n) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \cdots \varphi(p_m^{k_m}),$$

hence we only need to compute $\varphi(p^k)$ for a prime p and a positive integer k. This counts the number of integers from 1 to p^k that are coprime to p^k, or equivalently multiples of p, which is $p^k - p^{k-1} = p^{k-1}(p-1)$. This gives us the formula

Theorem 2.8. For an integer $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$, we have

$$\varphi(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right). \tag{1}$$

What is a polynomial analogue of Fermat's Little Theorem and Euler's Theorem? Based on Table 1, prime will be replaced by irreducible polynomial. Unfortunately, it does not make sense to take exponentiation of a polynomial by another polynomial. However, since $\varphi(n)$ was defined as a size of the group $(\mathbb{Z}/n\mathbb{Z})^\times$, we can define a polynomial analogue of $\varphi(g)$ as the size of the group $(A/gA)^\times$. Especially, if g is irreducible, then $(A/gA)^\times = (A/gA)\backslash\{0\}$, which has size $|g| - 1$. The exact same argument as the proof of Theorem 2.6 and Theorem 2.7 works for polynomials, and we get the following theorems.

Theorem 2.9 (Fermat's Little Theorem for Polynomials)**.** Let $f, g \in A$ be polynomials, where g is irreducible and f is not divisible by g. Then

$$f^{|g|-1} \equiv 1 \pmod{g}.$$

Theorem 2.10 (Euler's Theorem for Polynomials)**.** Let $f, g \in A$ be coprime polynomials. Then

$$f^{\varphi(g)} \equiv 1 \pmod{g}.$$

The formula (1) also generalizes to polynomials.

Theorem 2.11. Let $g(T) = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ be a polynomial in A, where $p_1, p_2, \ldots, p_m$ are distinct irreducible polynomials in A. Then

$$\varphi(g) = |g| \prod_{i=1}^{m} \left(1 - \frac{1}{|p_i|}\right).$$

2.4 Wilson's Theorem

Another interesting theorem on prime numbers is Wilson's theorem:

Theorem 2.12 (Wilson's Theorem)**.** Let p be a prime number. Then

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. Consider the group $G = (\mathbb{Z}/p\mathbb{Z})^\times$. The left hand side is the product of all elements in G. Now, we can pair up each element $a \in G$ with its inverse a^{-1}, except for the case when $a = a^{-1}$, which happens if and only if $a^2 \equiv 1 \pmod{p} \Leftrightarrow a \equiv \pm 1 \pmod{p}$. Thus the product of all elements in G is $\equiv 1 \cdot (-1) \equiv -1 \pmod{p}$, as desired. □

What is a polynomial analogue of Wilson's theorem? Note that the left hand side of Wilson's theorem is the product of all nonzero elements in $\mathbb{F}_p$, so it might be reasonable to define "factorial" $(g-1)!$ of an irreducible polynomial $g(T) \in \mathbb{F}_p[T]$ as the product of all elements in $(A/gA)^\times$.

Theorem 2.13 (Wilson's Theorem for Polynomials)**.** Let p be a prime number and $A = \mathbb{F}_p[T]$ the polynomial ring over the finite field $\mathbb{F}_p$. Let $g(T) \in A$ be an irreducible polynomial of degree d. Then

$$\prod_{0 \le \deg(f) \le d} f \equiv -1 \pmod{g}.$$

Note that the left hand side only depends on the degree of $g(T)$. Especially, (LHS) + 1 is divisible by any irreducible polynomial $g(T)$ of degree d.

Exercises

1. (a) Find a polynomial $f \in \mathbb{F}_3[T]$ such that[1]

$$\begin{cases} h \equiv T+2 \pmod{T^2+1} \\ h \equiv T^2+T \pmod{T^3-T^2+T+2} \end{cases}$$

   (b) Find a polynomial $f \in \mathbb{F}_7[T]$ such that[2]

$$\begin{cases} f \equiv 5T^2+3T+6 \pmod{T^3+2T^2+3T+2} \\ f \equiv T^3+1 \pmod{T^4+3T^3+2T^2+1} \\ f \equiv T^4-T+2 \pmod{T^2+3T+1} \end{cases}$$

   You can try to write a code to find such a polynomial.

[1] Answer: $f = T^4+T^2+T+2$
[2] Answer: $f = T^5+3T^2+2T+1$

2. For each prime $p \leq 20$, determine if the polynomial $T^2 + 1$ is irreducible over $\mathbb{F}_p$ or not. Can you find a pattern?[3]

3. There are several different proofs of Theorem 2.6, e.g. see wikipedia page. Choose your favorite argument (other than the one used in Theorem 2.6) and try to generalize it to prove 2.9.[4]

4. Prove Theorem 2.13.

5. Prove the original version of Fermat's little theorem from the polynomial version.[5]

6. Prove the original version of Wilson's theorem from the polynomial version.[6]

7. It is known that the following converse of Wilson's theorem holds: if a natural number n satisfies $(n-1)! \equiv -1 \pmod{n}$, then n is a prime number. We can consider a polynomial analogue of this converse: if a polynomial $g(T) \in \mathbb{F}_p[T]$ of degree d satisfies

$$\prod_{\substack{0 \leq \deg(f) \leq d \\ \gcd(f,g)=1}} f \equiv -1 \pmod{g},$$

then $g(T)$ is irreducible over $\mathbb{F}_p$. Here the left hand side is the product of all elements in $(A/gA)^\times$. Prove or disprove this claim.

[3] Answer will be given later.
[4] For example, there's a proof using induction on a. Can you generalize it to polynomials?
[5] Hint: for a prime p and an integer a not divisible by p, consider $f(T) = T + a$ and $g(T) = T$.
[6] Hint: consider $g(T) = T$.

Appendix

Here we summarize the dictionary between the integers and the polynomials over finite fields.

	$\mathbb{Z}$	$A = \mathbb{F}_p[T]$
indecomposable	prime	irreducible
number of units	$2 = \#(\mathbb{Z}^\times)$	$p-1 = \#(\mathbb{F}_p[T]^\times) = \#(\mathbb{F}_p^\times)$
absolute value	$\lvert n\rvert = \#(\mathbb{Z}/n\mathbb{Z})$	$\lvert f\rvert = \#(A/fA) = p^{\deg(f)}$
Euler φ function	$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$	$\varphi(f) = \#(A/fA)^\times$

Table 1: Integers and Polynomials.

References

[1] Rosen, M. *Number theory in function fields*, vol. 210. Springer Science & Business Media, 2013.