

# Arithmetic of Function Fields

Seewoo Lee

Last updated: June 2, 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 for integers is true for polynomials (over finite fields), and 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.

Here's a dictionary between the integers and the polynomials over finite fields.

| $\mathbb{Z}$              | $\mathbb{F}_p[T]$                  |
|---------------------------|------------------------------------|
| prime                     | irreducible                        |
| $2 =  \mathbb{Z}^\times $ | $p - 1 =  \mathbb{F}_p[T]^\times $ |

Table 1: Integers and Polynomials.

## 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

- the 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 unique factorization domain (UFD).

Recall that  $R$  is a Euclidean domain if there exists a function  $f : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$  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  $f(r) < f(b)$ .

### 2.2 Chinese Remainder Theorem

### 2.3 Fermat's Little Theorem and Euler's Theorem

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

**Theorem 2.3** (Fermat's Little Theorem). Let  $p$  be a prime number and  $a$  an integer not divisible by  $p$ . Then

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

There are several ways to prove this theorem (for example, see the [wikipedia page](#) on different proofs), and we will give 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.  $\square$

## 2.4 Wilson's Theorem

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

**Theorem 2.4** (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.  $\square$

### Exercises

1. Let  $p = 3$  and  $f(T) = T^2 + 1$ ,  $g(T) = T^3 - T + 1$ .
  - (a) Prove that  $f(T)$  and  $g(T)$  are irreducible in  $\mathbb{F}_3[T]$ .
  - (b) Prove that  $f(T)$  and  $g(T)$  are coprime in  $\mathbb{F}_3[T]$ , by finding polynomials  $a(T)$  and  $b(T)$  in  $\mathbb{F}_3[T]$  such that  $1 = a(T)f(T) + b(T)g(T)$ .
  - (c) Find all polynomials  $h(T)$  in  $\mathbb{F}_3[T]$  such that

$$\begin{cases} h(T) \equiv 1 \pmod{f(T)} \\ h(T) \equiv T \pmod{g(T)} \end{cases}$$

2. Prove the polynomial version of Wilson's Theorem. See [1, p. 6, Corollary 2].
3. Prove the original version of Fermat's little theorem from the polynomial version.<sup>1</sup>
4. Prove the original version of Wilson's theorem from the polynomial version.<sup>2</sup>

---

<sup>1</sup>Hint: for a prime  $p$  and an integer  $a$  not divisible by  $p$ , consider  $f(T) = T + a$  and  $g(T) = T$ .

<sup>2</sup>Hint: consider  $g(T) = T$ .

## References

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