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 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.

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

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 unique factorization domain (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 $f(r) < f(b)$.

2.2 Chinese Remainder Theorem

2.3 Fermat's Little Theorem and Euler's Theorem

Ferma'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

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

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 2.4 (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 2.3, where we consider the group $G = (\mathbb{Z}/n\mathbb{Z})^\times$ which has order $\varphi(n)$. □

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.

Theorem 2.5 (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 2.6 (Euler's Theorem for Polynomials)**.** Let $f, g \in A$ be coprime polynomials. Then

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

2.4 Wilson's Theorem

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

Theorem 2.7 (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 nonzero elements in A/gA.

Theorem 2.8 (Wilson's Theorem for Polynomials)**.** 1 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. 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. There are several different proofs of Theorem 2.3, e.g. see wikipedia page. Choose your favorite argument and try to generalize it to prove 2.5.[1]

3. Prove Theorem 2.8.

4. Prove the original version of Fermat's little theorem from the polynomial version.[2]

5. Prove the original version of Wilson's theorem from the polynomial version.[3]

Appendix

	$\mathbb{Z}$	$A = \mathbb{F}_p[T]$
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.

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

References

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