

Arithmetic of Function Fields

Seewoo Lee

Last updated: June 7, 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* [5].

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.

Prerequisites

We assume that the readers are familiar with undergraduate level algebra (groups, rings, fields, etc.) and number theory (congruences, prime numbers, etc.).

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 $|0| = 0$.

Sage codes

There are some codes in this note, which are mostly written in Sage. Sage is a free open-source mathematics software system, which is built on top of many existing open-source packages and wrapped in a Python interface. You can run them online in SageMathCell, or install it on your computer. Especially, a lot of number-theoretic functions are implemented in Sage, so it is much

easier to experiment with it than writing your own code from scratch. For example, to check if a large number is prime, you can simply run

```
is_prime(10 ^ 9 + 7)
```

Acknowledgements

Exercise 1.0.1. 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.

Exercise 1.0.2. 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 $f : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ 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 $f(r) < f(b)$. 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 $\deg : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ 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.

Exercise 2.1.1. 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?¹

2.2 Chinese Remainder Theorem

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

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

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

¹Answer will be given in the next section.

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

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

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, \dots, 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, \dots, a_k) under the isomorphism. It is enough to find solution for the equations

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

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. \square

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 $g_1(T), g_2(T), \dots, g_k(T) \in \mathbb{F}_p[T]$ be pairwise coprime polynomials and $a_1(T), a_2(T), \dots, a_k(T) \in \mathbb{F}_p[T]$ be polynomials. Then the system of congruences

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

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 $f \equiv T^2 + 1 - T^3 \equiv T^2 + T + 1 \pmod{(T^2 + 1)T}$.

Exercise 2.2.1. 1. Find a polynomial $f \in \mathbb{F}_3[T]$ such that²

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

2. Find a polynomial $f \in \mathbb{F}_7[T]$ such that³

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

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

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. \square

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 $\varphi(n)$. \square

²Answer: $f = T^4 + T^2 + T + 2$

³Answer: $f = T^5 + 3T^2 + 2T + 1$

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

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

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 $(A/gA)^\times = (A/gA) \setminus \{0\}$, 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, \dots, p_m are distinct irreducible polynomials in A . Then

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

Exercise 2.3.1. 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

Exercise 2.3.2. Prove the original version of Fermat's little theorem from the polynomial version.⁵

⁴For example, there's a proof using induction on a . Can you generalize it to polynomials?

⁵Hint: for a prime p and an integer a not divisible by p , consider $f(T) = T + a$ and $g(T) = T$.

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. \square

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

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

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

Exercise 2.4.1. Prove Theorem 2.13.

Exercise 2.4.2. Prove the original version of Wilson's theorem from the polynomial version.⁶

Exercise 2.4.3. 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.

⁶Hint: consider $g(T) = T$.

3 Reciprocity Laws

Quadratic reciprocity is one of the most important theorem in number theory, which is the origin of all modern number theory including algebraic number theory and Langlands program. In this section, we will see the analogue of quadratic reciprocity for function fields. Especially, we will present the higher reciprocity laws, which is much more complicated for integer case.

3.1 Quadratic Reciprocity for Integers

CRT essentially tells us how to solve *linear* congruences, i.e. equations of the form $ax + b \equiv 0 \pmod{n}$. Now, let's go one step further and consider *quadratic* congruences, i.e. equations of the form $ax^2 + bx + c \equiv 0 \pmod{n}$. How can we solve such equations? Recall that we solve usual quadratic eqautions by “completing the square”, and we can do the same for congruences.⁷ Hence we can reduce to a simpler question:

For given integer a and n , when does the congruence $x^2 \equiv a \pmod{n}$ have a solution?

Although the question seems pretty simple, the answer is quite deep and also interesting. To get some intuition, let's first consider the case when $n = p$ is a prime number and $a = -1$. In other words, we want to know when the congruence $x^2 \equiv -1 \pmod{p}$ has a solution (this is equivalent to one of the exercises in Section 2). Let's just try some small primes. Here's a Sage code to check the congruence $x^2 \equiv -1 \pmod{p}$ for primes $p < 100$:

```
with_sol = []
without_sol = []
for p in primes(100):
    for a in range(p):
        if (a ^ 2 + 1) % p == 0:
            with_sol.append(p)
            break
    if a == p - 1:
        without_sol.append(p)
print("Primes with solution", with_sol)
print("Primes without solution", without_sol)
```

Here's the output of the code you should get:

```
Primes with solution [2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97]
Primes without solution [3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83]
```

Stare the lists carefully for a while. What do you notice?

⁷when n is odd and a is invertible modulo n .

The answer is:

Theorem 3.1. Let p be a prime number. Then the congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

Proof. The case $p = 2$ is trivial, so we assume p is odd. Assume that the equation has a solution x . Then $x^4 \equiv (-1)^2 \equiv 1 \pmod{p}$, so x is an element of order 4 in $(\mathbb{Z}/p\mathbb{Z})^\times$. By Lagrange's theorem, the order of x must divide $p - 1$, so $4 \mid (p - 1) \Leftrightarrow p \equiv 1 \pmod{4}$.

Conversely, assume $p \equiv 1 \pmod{4}$ and let $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ be a generator of the group. Then $g^{(p-1)/4}$ is an element of order 4, so we can set $x = g^{(p-1)/4}$ and $(x^2)^2 \equiv x^4 \equiv 1 \pmod{p}$. Since $x^2 \not\equiv 1 \pmod{p}$, we have $x^2 \equiv -1 \pmod{p}$. \square

It is amazing that the solvability of the congruence equation is simply given by a congruence condition on the prime p .

Let's try other a , say $a = 3$. Here's a Sage code to check the congruence $x^2 \equiv 3 \pmod{p}$ for primes $p < 100$:

```
with_sol = []
without_sol = []
for p in primes(100):
    for a in range(p):
        if (a ^ 2 - 3) % p == 0:
            with_sol.append(p)
            break
    if a == p - 1:
        without_sol.append(p)
print("Primes with solution", with_sol)
print("Primes without solution", without_sol)
```

Here's the output of the code you should get:

```
Primes with solution [2, 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97]
Primes without solution [5, 7, 17, 19, 29, 31, 41, 43, 53, 67, 79, 89]
```

Again, the question is: what do you notice? The answer is slightly more complicated than the previous case, and you need to observe the numbers modulo 12.

Theorem 3.2. Let p be a prime number. Then the congruence $x^2 \equiv 3 \pmod{p}$ has a solution if and only if $p = 2, 3$ or $p \equiv 1, 11 \pmod{12}$.

To answer the question for general a , we need to introduce the Legendre symbol.

Definition 3.3 (Legendre symbol). Let p be a prime and a be an integer. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 \pmod{p} \\ 1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1 & \text{otherwise.} \end{cases} \quad (2)$$

Do not confuse it with fraction. By definition, it tells you whether the congruence $x^2 \equiv a \pmod{p}$ has a solution or not. But it does not tell you how to compute the symbol. The following theorem gives a way to compute the Legendre symbol for odd primes.

Theorem 3.4 (Euler's criterion). Let p be an odd prime and a be an integer. Then

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}. \quad (3)$$

Proof. If $a \equiv 0 \pmod{p}$, then the result is trivial. Recall that the group \mathbb{F}_p^\times is cyclic of order $p-1$. Let g be a generator of the group. Then every nonzero element $a \in \mathbb{F}_p^\times$ can be written as $a \equiv g^k \pmod{p}$ for some integer k . The equation is solvable if and only if k is even modulo $p-1$. \square

Theorem 3.5 (Quadratic reciprocity). Let p and q be distinct odd prime numbers. Then

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}. \quad (4)$$

Especially, the congruence $x^2 \equiv p \pmod{q}$ has a solution if and only if the congruence $x^2 \equiv q \pmod{p}$ has a solution, except when $p \equiv q \equiv 3 \pmod{4}$.

There are tons of proofs of this theorem, and we will not give a proof here. You can refer to an archive of proofs by Lemmermeyer [4], or a book by Baumgart [1].

We also need the following supplementary results to compute the Legendre symbol completely.

Theorem 3.6. For odd prime p , we have

$$\begin{aligned} \left(\frac{-1}{p}\right) &= (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases} \\ \left(\frac{2}{p}\right) &= (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv 1, 7 \pmod{8} \\ -1 & p \equiv 3, 5 \pmod{8} \end{cases} \end{aligned}$$

Proof. We already proved the first in Theorem 3.1. For the second here is a proof brought from [6, Theorem]. Let $\alpha \in \mathbb{F}_{p^2}$ be a primitive 8-th root of unity (note that $p^2 - 1$ is divisible by 8 for any odd p). then $\alpha^4 = -1$ and $y = \alpha + \alpha^{-1}$ satisfies $y^2 = 2 + \alpha^2 + \alpha^{-2} = 2$. By binomial expansion, we have $y^p = \alpha^p + \alpha^{-p}$ modulo p , hence $y^p = y$ for $p \equiv \pm 1 \pmod{8}$ and this gives $\left(\frac{2}{p}\right) = 1$ for such p . If $p \equiv \pm 3 \pmod{8}$, then $y^p = -y \Leftrightarrow y^{p-1} = -1$, hence $\left(\frac{2}{p}\right) = y^{p-1} = -1$.⁸ \square

We can use quadratic reciprocity to prove Theorem 3.2.

Proof of Theorem 3.2. By Theorem 3.5, we have

$$\left(\frac{3}{p}\right) \left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)(3-1)}{4}} = (-1)^{\frac{p-1}{2}} \Leftrightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right).$$

We can compute each factor on the right-hand side separately, which are

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & p \equiv 1 \pmod{3} \\ -1 & p \equiv 2 \pmod{3} \end{cases},$$

⁸It may look random to consider such y , but this can be thought as an analogue of the identity of complex numbers $\sqrt{2} = e^{2\pi i/8} + e^{-2\pi i/8}$ in finite fields.

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases}.$$

By combining these two congruences, we can see that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv 1, 11 \pmod{12} \\ -1 & p \equiv 5, 7 \pmod{12} \end{cases}$$

for $p \neq 2, 3$. □

Exercise 3.1.1. When $p \equiv 1 \pmod{4}$, we know that the congruence $x^2 \equiv -1 \pmod{p}$ has a solution by Theorem 3.1. Show that $x = \left(\frac{p-1}{2}\right)!$ becomes a solution.⁹

Exercise 3.1.2. Prove Theorem 3.2 without using quadratic reciprocity, by adapting the proof of Theorem 3.6. Here's a sketch of a proof:

1. Show that, for any prime $p > 3$, there is a 12-th root of unity β in \mathbb{F}_{p^2} .
2. Show that $z = \beta + \beta^{-1}$ satisfies $z^2 = 3$.
3. Show that $z^p = z$ if and only if $p \equiv 1, 11 \pmod{12}$, and $z^p = -z$ if and only if $p \equiv 5, 7 \pmod{12}$. Conclude that $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv 1, 11 \pmod{12}$.

It is natural to ask if one can generalize this proof to other primes. This essentially gives a proof of quadratic reciprocity, and the correct analogue of y or z would be the *Gauss sum*.

Exercise 3.1.3. Characterize the prime p such that the congruence $x^2 \equiv 5 \pmod{p}$ has a solution.¹⁰

Exercise 3.1.4. For a prime p and integers a, b, c , give a necessary and sufficient condition for the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ to have a solution.

- Exercise 3.1.5.**
1. Find all prime $p < 100$ where the congruence $x^3 - 3x + 1 \equiv 0 \pmod{p}$ has a solution. Can you find a pattern? If you are brave enough, try to prove it.¹¹
 2. Find all prime $p < 100$ where the congruence $x^3 - x - 1 \equiv 0 \pmod{p}$ has a solution. Can you find a pattern?
 3. Consider a power series

$$A(T) = T \prod_{n \geq 1} (1 - T^n)(1 - T^{23n}) = \sum_{n \geq 1} a_n T^n \in \mathbb{Z}[[T]].$$

Compute the first 100 coefficients of $A(T)$, and check if there's any relation between the p -th coefficients a_p and the congruence $x^3 - x - 1 \equiv 0 \pmod{p}$.¹²

3.2 Quadratic Reciprocity for Polynomials

Let's move on to the polynomial case. We are going to ask the same question as before:

⁹Hint: Wilson's theorem.

¹⁰Hint: Use quadratic reciprocity. Answer will be given modulo 5.

¹¹Hint: modulo 9. To prove it, one can use the fact that the roots of $x^3 - 3x - 1$ are $2 \cos(2\pi/9), 2 \cos(4\pi/9), 2 \cos(8\pi/9)$, and try to express them in terms of 9-th roots of unity.

¹²Answer: it has a solution in \mathbb{F}_p if and only if $a_p \in \{0, 2\}$, when $p \neq 23$. Buzzword: Artin representation and modular form of weight 1, Nonabelian class field theory.

For given polynomial $f \in A$ and irreducible polynomial P , when does the congruence $x^2 \equiv f \pmod{P}$ have a solution?

We are going to adapt the exact same strategy as before. **For this section, we assume that p is an odd prime.** Characteristic 2 case is slightly more complicated, and we will not discuss it here. You can refer to Keith Conrad's note [2] for more details for $p = 2$.

Define the *Legendre symbol* for polynomials as follows:

Definition 3.7 (Legendre symbol for polynomials). Let $P \in A$ be an irreducible polynomial and $f \in A$ be a polynomial. The *Legendre symbol* $\left(\frac{f}{P}\right)$ is defined as follows:

$$\left(\frac{f}{P}\right) = \begin{cases} 0 & f \equiv 0 \pmod{P} \\ 1 & \text{if } x^2 \equiv f \pmod{P} \text{ has a solution in } A/PA, \\ -1 & \text{otherwise.} \end{cases} \quad (5)$$

We have Euler's criterion for polynomials as well.

Theorem 3.8 (Euler's criterion for polynomials). Let $P \in A$ be an irreducible polynomial and $f \in A$ be a polynomial. Then

$$\left(\frac{f}{P}\right) = f^{\frac{|P|-1}{2}} \pmod{P}. \quad (6)$$

Proof. □

Theorem 3.9 (Quadratic reciprocity for polynomials). Let $P, Q \in A$ be distinct irreducible polynomials. Then

$$\left(\frac{P}{Q}\right) \left(\frac{Q}{P}\right) = (-1)^{\frac{|P|-1}{2} \cdot \frac{|Q|-1}{2}}. \quad (7)$$

Proof. This proof is due to Carlitz, which can be found in Rosen's book [5, p. 25, Theorem 3.3] and Conrad's note [3, Section 3]. Let k/\mathbb{F}_p be a (finite) field contains all roots of P and Q . Let $d_P = \deg P$ and $d_Q = \deg Q$. We will first show that (7) is equivalent to:

$$\left(\frac{P}{Q}\right) = (-1)^{\frac{(p-1)d_P d_Q}{2}} \left(\frac{Q}{P}\right). \quad (8)$$

From $|P| = p^{d_P}$,

$$\frac{|P|-1}{2} = \frac{p^{d_P}-1}{2} = \frac{p-1}{2} \cdot (p^{d_P-1} + p^{d_P-2} + \dots + 1) \equiv \frac{(p-1)d_P}{2} \pmod{2},$$

since p is odd. Similar congruence holds for Q , hence

$$\frac{|P|-1}{2} \cdot \frac{|Q|-1}{2} \equiv \frac{(p-1)d_P}{2} \cdot \frac{(p-1)d_Q}{2} \equiv \frac{p-1}{2} \cdot d_P d_Q \pmod{2}.$$

Note that $n^2 \equiv n \pmod{2}$ for any integer n .

Now, let $\alpha, \beta \in k$ be roots of P and Q , respectively. Then all the zeros of P and Q are given by the p -powers of α and β (images of Frobenius map): they factor as

$$P(T) = \prod_{i=0}^{d_P-1} (T - \alpha^{p^i}), \quad Q(T) = \prod_{j=0}^{d_Q-1} (T - \beta^{p^j}).$$

By Euler's criterion for polynomials and properties of finite fields, we have

$$\begin{aligned}
\left(\frac{P}{Q}\right) &\equiv P(T)^{\frac{|Q|-1}{2}} \pmod{Q(T)} \\
&\equiv P(T)^{\frac{p-1}{2}(1+p+\dots+p^{d_Q-1})} \pmod{Q(T)} \\
&\equiv (P(T)P(T)^p \dots P(T)^{p^{d_Q-1}})^{\frac{p-1}{2}} \pmod{Q(T)} \\
&\equiv (P(T)P(T^p) \dots P(T^{p^{d_Q-1}}))^{\frac{p-1}{2}} \pmod{Q(T)}
\end{aligned}$$

If we set $T = \beta$ for the last congruence, it becomes

$$\prod_{i=0}^{d_P-1} \prod_{j=0}^{d_Q-1} (\beta^{p^j} - \alpha^{p^i})^{\frac{p-1}{2}} \in \{\pm 1\}$$

Now we can swap α and β , which gives $\left(\frac{Q}{P}\right)$ up to a sign

$$(-1)^{\frac{(p-1)d_P d_Q}{2}}$$

which exactly matches with the exponent of (-1) in (8). \square

Note that the proof is very specific for polynomials over finite fields, and it does not work for integer case. There are *some* proofs of similar taste, which writes the product $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$ as other function that is symmetric in p and q .

Exercise 3.2.1. For an irreducible polynomial $P \in A$ and polynomials $f, g, h \in A$, give a necessary and sufficient condition for the congruence $fx^2 + gx + h \equiv 0 \pmod{P}$ to have a solution (in A).

4 How many primes?

A Appendix

A.1 Dictionary between integers and polynomials

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	$ n = \#(\mathbb{Z}/n\mathbb{Z})$	$ f = \#(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.

A.2 Handbook of Galois theory for finite fields

References

- [1] BAUMGART, O. *The quadratic reciprocity law: A collection of classical proofs*. Birkhäuser, 2015.
- [2] CONRAD, K. Quadratic reciprocity in characteristic 2. <https://kconrad.math.uconn.edu/blurbs/ugradnumthy/QRchar2.pdf>. Accessed: 2025-06-05.
- [3] CONRAD, K. Quadratic reciprocity in odd characteristic. <https://kconrad.math.uconn.edu/blurbs/ugradnumthy/QRsharp.pdf>. Accessed: 2025-06-05.
- [4] LEMMERMEYER, F. Proofs of the Quadratic Reciprocity Law. https://web.archive.org/web/20250106010310/https://www.mathi.uni-heidelberg.de/%7Eflemmeryer/qrg_proofs.html. Accessed: 2025-06-05.
- [5] ROSEN, M. *Number theory in function fields*, vol. 210. Springer Science & Business Media, 2013.
- [6] SERRE, J.-P. *A course in arithmetic*, vol. 7. Springer Science & Business Media, 2012.