

Arithmetic of Function Fields

Seewoo Lee

Last updated: June 14, 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*.

Contents

Introduction	3
1.1 Prerequisites	3
1.2 Notations	3
1.3 SageMath	3
Basic number theory and their analogues for polynomials	4
2.1 Fundamental Theorem of Arithmetic	4
2.2 Chinese Remainder Theorem	4
2.3 Fermat's Little Theorem and Euler's Theorem	6
2.4 Wilson's Theorem	8
Reciprocity Laws	9
3.1 Quadratic Reciprocity for Integers	9
3.2 Quadratic Reciprocity for Polynomials	12
How many primes?	16
4.1 Prime number theorem and Riemann zeta function	16
4.2 Counting irreducible polynomials with zeta function	19
4.3 Counting other things	22
Appendix	23
A.1 Dictionary between integers and polynomials	23
A.2 Handbook of Galois theory for finite fields	24
A.3 Handbook of Sage functions	25

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.

1.1 Prerequisites

We assume that the readers are familiar with undergraduate level algebra (groups, rings, fields, etc.), number theory (congruences, prime numbers, etc.), and a bit of complex analysis. Some of the theory of finite fields will be reviewed in Appendix A.2.

1.2 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 its norm by $|f| = p^{\deg(f)}$, where $\deg(f)$ is the degree of f , and we set $|0| = 0$.

1.3 SageMath

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)
```

Several useful Sage functions are listed in Appendix A.3.

Acknowledgements

Exercise 1.3.1. 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 1.3.2. 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 $p \leq 100$, 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. sage

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

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

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

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

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 (g is not necessarily irreducible). 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

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

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.  For each p and d , compute $\prod_{0 \leq \deg(f) < d} f + 1$. Can you find any pattern?

Exercise 2.4.4. 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. Here are two suggestions:

1. 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 $(A/gA)^\times$.

2. If a polynomial $g(T) \in \mathbb{F}_p[T]$ of degree d satisfies

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

then $g(T)$ is irreducible over \mathbb{F}_p .

Prove or disprove these claims.

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.

3.1 Quadratic Reciprocity for Integers

CRT 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 equations 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? 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 $4 \mid (p - 1) \Leftrightarrow p \equiv 1 \pmod{4}$.

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

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

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

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 [7], or a book by Baumgart [2].

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 [13, 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

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

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 $p \neq 2, 3$. \square

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

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.

⁹Hint: Wilson's theorem.

Exercise 3.1.2.  Compute the Legendre symbol $\left(\frac{563}{661}\right)$, by

1. brute-force checking all integers x modulo 661, or
2. using Euler's criterion, or
3. using quadratic reciprocity, or
4. using kronecker in Sage.


Exercise 3.1.3. 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 3.1.4. Characterize the prime p such that the congruence $x^2 \equiv 5 \pmod{p}$ has a solution.¹⁰

Exercise 3.1.5. 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 3.1.6. 

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:

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

¹¹Hint: modulo 9. To prove it, we notice the fact that the roots of $x^3 - 3x + 1$ are $2 \cos(2\pi/9), 2 \cos(4\pi/9), 2 \cos(8\pi/9)$, by double angle formula. Then 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 $p \neq 23$. Buzzwords: 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 [3] 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:

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

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

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

Exercise 3.2.1. Prove Theorem 3.8 by adapting the proof of Theorem 3.4.¹³

One interesting corollary of Euler's criterion is the following:

Corollary 3.9. Let $P \in A$ be an irreducible polynomial of even degree. Then $\left(\frac{c}{P}\right) = 1$ for any nonzero constant $c \in \mathbb{F}_p$.

Proof. Write

$$\frac{|P|-1}{2} = \frac{p^{\deg P} - 1}{2} = (p-1) \cdot \frac{(p^{\deg P-1} + p^{\deg P-2} + \dots + 1)}{2}$$

where the second factor of the last equation is an integer since $\deg P$ is even and p is odd. By Euler's criterion and $c^{p-1} = 1$, we have

$$\left(\frac{c}{P}\right) = c^{\frac{|P|-1}{2}} = c^{(p-1) \cdot \frac{(p^{\deg P-1} + p^{\deg P-2} + \dots + 1)}{2}} = 1.$$

□

Exercise 3.2.2. Let $p = 7$ and $P(T) = T^2 + T + 3$, which is irreducible modulo 7. Find a polynomial $f \in \mathbb{F}_7[T]$ such that $f^2 \equiv 3 \pmod{P}$.

Theorem 3.10 (Quadratic reciprocity for polynomials). Let $P, Q \in A$ be distinct irreducible polynomials. Then

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

¹³Hint: Use the fact that $A/P A$ is a finite field of order $|P| = p^{\deg P}$.

Proof. This proof is due to Carlitz, which can be found in Rosen's book [11, p. 25, Theorem 3.3] or Conrad's note [4, 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 is 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 .


One can generalize it to higher order reciprocity laws. Since the proof is very similar to the quadratic case, we only state the result here. Details can be found in [11, Chapter 3].

Theorem 3.11 (d -th power reciprocity law). Let $d \geq 2$ be an integer dividing $p - 1$. For $f \in A$ and irreducible polynomials $P \in A$, define $\left(\frac{f}{P}\right)$ be a unique element of \mathbb{F}_p^\times such that

$$\left(\frac{f}{P}\right)_d = f^{\frac{|P|-1}{d}} \pmod{P}. \quad (9)$$

Then for distinct irreducible polynomials $P, Q \in A$, we have

$$\left(\frac{P}{Q}\right)_d = (-1)^{\frac{p-1}{d} \deg P \deg Q} \left(\frac{Q}{P}\right)_d. \quad (10)$$

Exercise 3.2.3.  Decide if the following congruence equations in X have a solution.

1. $X^2 = T^2 + 3T + 3 \pmod{T^3 + T + 1}$ in $\mathbb{F}_5[T]$.
2. $X^2 \equiv 6T^2 + T + 1 \pmod{T^3 + T^2 + T + 5}$ in $\mathbb{F}_7[T]$.
3. $X^2 + TX + T + 1 \equiv 0 \pmod{T^3 + T^2 - 1}$ in $\mathbb{F}_3[T]$.

Exercise 3.2.4. Let p be an odd prime and $P \in A$ be an irreducible polynomial of degree d . Show that $X^2 \equiv -1 \pmod{P}$ has a solution if and only if d is even or $p \equiv 1 \pmod{4}$. Can you give an explicit formula for a solution in terms of p and P ?

Exercise 3.2.5. 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.

Exercise 3.2.6. Let $f \in A$ be a nonsquare polynomial. Show that $\left(\frac{f}{P}\right) = -1$ for infinitely many irreducible polynomial $P \in A$.¹⁴

¹⁴See [4, Theorem 4.5].

4 How many primes?

In this section, we will study several questions on counting numbers and polynomials, e.g. number of prime numbers / irreducible polynomials up to certain bounds. Over integers, many of such problems are wide open. However, the polynomial analogue of these problems are often much easier to prove. Especially, both of the sides uses certain *zeta functions* or *L-functions* to count certain objects, which becomes much simpler in the polynomial case.

4.1 Prime number theorem and Riemann zeta function

We start with the most important fact about prime numbers, proven by Euclid few hundred years ago.

Theorem 4.1 (Euclid). There are infinitely many prime numbers.

Proof. Suppose that there are finitely many prime numbers p_1, p_2, \dots, p_n . Consider the number $N = p_1 p_2 \cdots p_n + 1$. Then N is not divisible by any of the prime numbers p_i , so it must be either prime or divisible by some other prime number. This contradicts our assumption that there are only finitely many prime numbers. \square

Once we know that there are infinitely many prime numbers, we can ask the following question:

For given real number $x > 0$, how many prime numbers are there less than or equal to x ?


We follow the standard notation and denote the number of prime numbers less than or equal to x by $\pi(x)$. Hadamard and de la Vallée-Poussin proved independently in 1896 that

Theorem 4.2 (Prime number theorem). We have

$$\pi(x) \sim \frac{x}{\log x},$$

where \sim means that the ratio of the two sides tends to 1 as x tends to infinity.

In other words, the density of prime numbers among integers is approximately $\frac{1}{\log x}$, which tends to 0 as x tends to infinity.

Exercise 4.1.1.  Plot the graphs of the functions $\pi(x)$ and $\frac{x}{\log x}$ for $x \in [1, 10^6]$.¹⁵

Although there are some elementary proofs by Selberg [12] and Erdős [6], the original proofs and the most of other proofs (e.g. Newman's proof [9, 16]) uses *Riemann zeta function*. In [10], Riemann defined the zeta function:

Definition 4.3 (Riemann zeta function). The *Riemann zeta function* is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

for complex numbers s with $\Re(s) > 1$.

¹⁵Hint: Sage has `prime_pi`.

Exercise 4.1.2. Why it converges for $\Re(s) > 1$?

By writing $\zeta(s)$ as an integral, Riemann showed that it can be analytically (more precisely, meromorphically) continued to the whole complex plane, except for a simple pole at $s = 1$.

Theorem 4.4. 1. $\zeta(s)$ can be analytically continued to a meromorphic function on the whole complex plane, with a simple pole at $s = 1$ with residue 1.

2. Define the *completed zeta function* as

$$\xi(s) = \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s), \quad (11)$$

where $\Gamma(s)$ is the gamma function. Then $\xi(1-s) = \xi(s)$ for all $s \in \mathbb{C} \setminus \{0, 1\}$.

Proof. See Apostol [1] or Stein–Shakarchi [14]. □

This allow us to state the infamous *Riemann Hypothesis*:

Conjecture 4.5 (Riemann Hypothesis). All *non-trivial* zeros of $\zeta(s)$ lie on the critical line $\Re(s) = \frac{1}{2}$.

Here the *trivial* zeros are the negative even integers, i.e. $s = -2, -4, -6, \dots$

But why Riemann zeta function is related to prime numbers? The following theorem by Euler is the key.

Theorem 4.6 (Euler factorization). The Riemann zeta function can be expressed as an infinite product over all prime numbers p :

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}, \quad (12)$$

for $\Re(s) > 1$.

Proof. This essentially follows from the fundamental theorem of arithmetic (Theorem 2.1). More precisely, using geometric series we can rewrite the right hand side as

$$\prod_p \frac{1}{1 - p^{-s}} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots \right)$$

and Theorem 2.1 implies that each term $\frac{1}{n^s}$ in the left hand side in (12) appears exactly once in the right hand side. □

Let's return to the prime number theorem. The main idea of the proof(s) is in two steps:

1. Reduce the problem to the following claim: $\zeta(s)$ is non-vanishing for $\Re(s) = 1$ and $s \neq 1$.
2. Prove the above claim.

Here we give a sketch of the proof of 2. By taking logarithmic derivative of (12), we get

$$\log \zeta(s) = - \sum_p \log(1 - p^{-s}) = \sum_p \sum_{k \geq 1} \frac{p^{-ks}}{k}.$$

If $s = x + iy$, we get

$$|\zeta(x + iy)| = \exp \left(\sum_p \sum_{k \geq 1} \frac{\cos(ky \log p)}{kp^{kx}} \right)$$

and

$$|\zeta(x)^3 \zeta(x + iy)^4 \zeta(x + 2iy)| = \exp \left(\sum_p \sum_{k \geq 1} \frac{3 + 4 \cos(ky \log p) + \cos(2ky \log p)}{kp^{kx}} \right) \quad (13)$$

for all $x > 1$. Now, one can prove the inequality

$$3 + 4 \cos \theta + \cos(2\theta) \geq 0 \quad (14)$$

for any $\theta \in \mathbb{R}$, which shows that the right hand side of (13) is at least 1. Assume that $\zeta(1 + iy) = 0$ for some y . Then one can derive a contradiction from (13) by considering the limit as $x \rightarrow 1^+$, where the left hand side tends to 0 while the right hand is bounded below by 1.

Exercise 4.1.3. Prove (14).

So we can approximate $\pi(x)$ by $\frac{x}{\log x}$, but how good is this approximation? More precisely, what is the growth of the error term? First of all, there's a better approximation than $\frac{x}{\log x}$ suggested by Dirichlet, which is *logarithmic integral*:

$$\text{Li}(x) := \int_2^x \frac{dt}{\log t}. \quad (15)$$

In terms of growth, $\frac{x}{\log x}$ and $\text{Li}(x)$ are asymptotically equivalent (see Exercise 4.1.4 below). However, $\text{Li}(x)$ gives much better approximation than $\frac{x}{\log x}$. In [5], de la Vallée-Poussin proved that the error term $\pi(x) - \text{Li}(x)$ is bounded by

$$|\pi(x) - \text{Li}(x)| = O(xe^{-c\sqrt{\log x}})$$


for some constant $c > 0$. Koch [15] showed that, *assuming the Riemann Hypothesis*, we obtain the improved bound

$$|\pi(x) - \text{Li}(x)| = O\left(\sqrt{x} \log x\right) \quad (16)$$

which in fact turned out to be equivalent to the Riemann Hypothesis.

Exercise 4.1.4. Prove that $\text{Li}(x) \sim \frac{x}{\log x}$ as $x \rightarrow \infty$. More precisely, show that

$$\text{Li}(x) \sim \frac{x}{\log x} \sum_{k \geq 0} \frac{k!}{(\log x)^k} = \frac{x}{\log x} + \frac{x}{(\log x)^2} + \frac{2x}{(\log x)^3} + \dots \quad (17)$$

Exercise 4.1.5.  Plot the graphs of the functions $\pi(x)$, $\text{Li}(x)$, and $\frac{x}{\log x}$ for $x \in [1, 10^6]$, and observe that $\text{Li}(x)$ is much closer to $\pi(x)$ than $\frac{x}{\log x}$. Also, compare $\pi(x)$ and $\text{Li}(x)$ - do you have any conjecture on the difference?¹⁶

¹⁶You may find that $\pi(x) < \text{Li}(x)$ when x is not too small, and it is tempting to conjecture that $\pi(x) < \text{Li}(x)$ for sufficiently large x . However, this is not true. In fact, Littlewood [8] proved that the sign of $\pi(x) - \text{Li}(x)$ changes infinitely many times, although the smallest number $x > 10$ such that $\pi(x) < \text{Li}(x)$ (known as Skewes's number) is probably very huge.

4.2 Counting irreducible polynomials with zeta function

How about polynomials? First of all, there are infinitely many irreducible polynomials:

Theorem 4.7. For each prime p , there are infinitely many irreducible polynomials over \mathbb{F}_p .

Exercise 4.2.1. Prove Theorem 4.7. You can follow the argument of Theorem 4.1 above, or give more interesting proof.

Now, we can ask more interesting question, i.e. number of irreducible polynomials of certain degree.

For a given prime p and integer n , how many irreducible monic polynomials of degree n in $A = \mathbb{F}_p[T]$?

We will fix p , and denote the number of such polynomials as a_n . When n is small, we can get nice formulas.

Proposition 4.8.

$$a_2 = \frac{p^2 - p}{2}. \quad (18)$$

Proof. One can count number of *reducible* monic polynomials, and subtract from the total number of monic quadratic polynomials, which is simply p^2 (you have p choices for each c_0 and c_1 in $f(T) = T^2 + c_1T + c_0$). If $f(T)$ is not irreducible, then it should factor as $f(T) = (T - \alpha)(T - \beta)$ for some $\alpha, \beta \in \mathbb{F}_p$. Now, there are p cases where $\alpha = \beta$, and $\binom{p}{2}$ cases where $\alpha \neq \beta$. This gives

$$a_2 = p^2 - p - \binom{p}{2} = \frac{p^2 - p}{2}.$$

□

Exercise 4.2.2. Prove

$$a_3 = \frac{p^3 - p}{3}. \quad (19)$$

You may need to exclude the polynomials $f(T)$ which factor as 1) products of three linear polynomials, or 2) products of linear and irreducible quadratic polynomial.

It seems that we may even able to find a nice formula for a_n . To do this, we will define a *zeta function* for polynomials, which is similar to the Riemann zeta function but much simpler.

Definition 4.9 (Zeta function for A). We define *zeta function* as

$$\zeta_A(s) = \sum_{0 \neq f \text{ monic}} \frac{1}{|f|^s} \quad (20)$$

which converges for $\Re(s) > 1$.

We have a simple formula for ζ_A :

Proposition 4.10. We have

$$\zeta_A(s) = \frac{1}{1 - p^{1-s}}. \quad (21)$$

Proof. We can group the sum in (20) by degree, since $|f|$ only depends on degree of f . Since there are p^d -many monic polynomials of degree d , we have

$$\zeta_A(s) = \sum_{d \geq 1} \frac{p^d}{p^{ds}} = \sum_{d \geq 0} p^{d(1-s)} = \frac{1}{1 - p^{1-s}}.$$

□

Especially, it has a simple pole at $s = 1$ with residue $1/\log p$, and analytic continuation is clear from the formula. Also, there are no zeros of $\zeta_A(s)$, so Riemann Hypothesis for polynomials is trivially true. Note that the notation ζ_A somehow emphasizes A , since we will eventually study more general “zeta functions” for other polynomial rings (“extensions” of A), where the Riemann Hypothesis is more interesting (but still true).

What about Euler factorization? Since A is also UFD, the same argument as in Theorem 4.6 gives us

Theorem 4.11 (Euler factorization for polynomials). We have

$$\zeta_A(s) = \prod_{P \text{ monic irred}} (1 - |P|^{-s})^{-1}. \quad (22)$$

As in Proposition 4.10, we can group the product in (22) by degree, which gives

$$\zeta_A(s) = \prod_{d \geq 1} (1 - p^{-ds})^{-a_d}. \quad (23)$$

By comparing (21) and (23), we can deduce the following formula for a_n :

Theorem 4.12. We have

$$p^n = \sum_{d|n} d a_d. \quad (24)$$

Proof. Let $u = p^{-s}$, so

$$\frac{1}{1 - pu} = \prod_{d \geq 1} (1 - u^d)^{-a_d}. \quad (25)$$

By taking logarithmic derivative, we have

$$\frac{p}{1 - pu} = \sum_{d \geq 1} a_d \frac{du^{d-1}}{1 - u^d} \Leftrightarrow \frac{pu}{1 - pu} = \sum_{d \geq 1} a_d \frac{du^d}{1 - u^d}. \quad (26)$$

Using geometric series, we can rewrite the equations as

$$\sum_{n \geq 1} p^n u^n = \sum_{d \geq 1} d a_d \sum_{k \geq 1} u^{dk} = \sum_{n \geq 1} \left(\sum_{d|n} d a_d \right) u^n. \quad (27)$$

Now, we can compare the coefficients of u^n on both sides and get (24). □

We can *invert* this formula to get a formula for a_n . Such a process is called *Möbius inversion* - before we state the general formula, we will first give small examples that may leads to the general formula (in other words, *you can invent Möbius inversion formula yourself*). Let $b_n := n a_n$. For $n = 1, 2, 3, 4, 6, 12$, (24) gives us the following equations:

$$p = b_1,$$

$$\begin{aligned}
p^2 &= b_1 + b_2, \\
p^3 &= b_1 + b_3, \\
p^4 &= b_1 + b_2 + b_4, \\
p^6 &= b_1 + b_2 + b_3 + b_6, \\
p^{12} &= b_1 + b_2 + b_3 + b_4 + b_6 + b_{12}.
\end{aligned}$$

From these equations, we can compute b_n recursively:

$$\begin{aligned}
b_1 &= p, \\
b_2 &= p^2 - p, \\
b_3 &= p^3 - p, \\
b_4 &= p^4 - p^2, \\
b_6 &= p^6 - p^3 - p^2 + p, \\
b_{12} &= p^{12} - p^6 - p^4 + p^2.
\end{aligned}$$

Let's see how we actually computed b_6 and b_{12} . b_6 can be written as

$$\begin{aligned}
b_6 &= p^6 - (b_1 + b_2 + b_3) \\
&= p^6 - (b_1 + b_3) - (b_1 + b_2) + b_1 \\
&= p^6 - p^3 - p^2 + p.
\end{aligned}$$

Similarly, we can compute b_{12} as

$$\begin{aligned}
b_{12} &= p^{12} - (b_1 + b_2 + b_3 + b_4 + b_6) \\
&= p^{12} - (b_1 + b_2 + b_3 + b_6) - (b_1 + b_2 + b_4) - (b_1 + b_2) \\
&= p^{12} - p^6 - p^4 + p^2.
\end{aligned}$$

This may remind you the principle of inclusion-exclusion, and indeed, we can write the general formula as follows: for $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$,

$$\begin{aligned}
b_n &= p^n - \sum_{d|n, d < n} b_d \\
&= p^n - (b_1 + \cdots + b_{n/p_1}) - (b_1 + \cdots + b_{n/p_2}) - \cdots - (b_1 + \cdots + b_{n/p_k}) \\
&\quad + (b_1 + \cdots + b_{n/p_1 p_2}) + (b_1 + \cdots + b_{n/p_1 p_3}) + \cdots \\
&\quad \dots \\
&= p^n - p^{n/p_1} - p^{n/p_2} - \cdots - p^{n/p_k} + p^{n/(p_1 p_2)} + p^{n/(p_1 p_3)} + \cdots
\end{aligned}$$

This gives us the following formula for a_n :

Corollary 4.13. For a given prime p and integer n , we have

$$a_n = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}, \quad (28)$$

where μ is the Möbius function, defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \text{ with } k \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases} \quad (29)$$

Exercise 4.2.3. Complete the proof of Corollary 4.13.


Note that (28) gives an *exact* formula for a_n . This also gives an analogue of the prime number theorem for polynomials: the dominating term of a_n is

$$\frac{p^n}{n} = \frac{p^n}{\log_p p^n},$$

where p^n is equal to the number of monic polynomials of degree n over \mathbb{F}_p . Moreover, the error term is bounded by $O\left(\frac{p^{n/2}}{n}\right)$, so we get

$$a_n = \frac{p^n}{\log_p p^n} + O\left(\frac{\sqrt{p^n}}{\log_p p^n}\right). \quad (30)$$

which has a similar form as Koch's bound (16) (or even better!).

Exercise 4.2.4.  Let $p = 3$. For each $1 \leq n \leq 10$, find the number of irreducible monic polynomials of degree n over \mathbb{F}_3 , by using the factorization of $T^{3^n} - T$. Check that the results match with the formula (28).

Exercise 4.2.5. Prove the following non-asymptotic version (30):


$$\left| a_n - \frac{p^n}{n} \right| \leq \frac{p^{n/2}}{n}$$

Exercise 4.2.6. For each p and d , prove that the polynomial

$$\left(\prod_{0 \leq \deg(f) < d} f \right) + 1$$

is equal to a constant multiple of the product of all monic irreducible polynomials of degree d over \mathbb{F}_p . What is the constant?

Exercise 4.2.7. Prove that the polynomial $T^p - T - 1$ is irreducible over \mathbb{F}_p for all prime p .¹⁷

Exercise 4.2.8.  For a given prime p and an integer n , design an algorithm to find an irreducible polynomial of degree n over \mathbb{F}_p ? (This is not an easy question.)

Exercise 4.2.9. What would be a good analogue of the logarithmic integral $\text{Li}(x)$ for polynomials?

4.3 Counting other things

¹⁷Such a polynomial is called *Artin-Schreier polynomial*.

A Appendix

A.1 Dictionary between integers and polynomials

Here we summarize the dictionary between the integers and the polynomials over finite fields. Here all g, g_1, g_2, \dots on the A -side are all irreducible polynomials over \mathbb{F}_p . Also, we omit all the technical assumptions for each theorem, which can be found in the main text.

	\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	$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$	$\varphi(f) = \#(A/fA)^\times$
Fermat's little theorem	$a^{p-1} \equiv 1 \pmod{p}$	$f^{ g -1} \equiv 1 \pmod{g}$
Euler's theorem	$a^{\varphi(n)} \equiv 1 \pmod{n}$	$f^{\varphi(f_0)} \equiv 1 \pmod{f_0}$
Wilson's theorem	$(p-1)! \equiv -1 \pmod{p}$	$\prod_{f \in (A/gA)^\times} f \equiv -1 \pmod{g}$
Quadratic reciprocity	$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$	$\left(\frac{g_1}{g_2}\right) \left(\frac{g_2}{g_1}\right) = (-1)^{\frac{ g_1 -1}{2} \frac{ g_2 -1}{2}}$
Riemann Zeta function	$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$	$\zeta_A(s) = \sum_{f \neq 0, \text{ monic}} \frac{1}{ f ^s}$
Euler factorization	$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$	$\zeta_A(s) = \prod_{g, \text{ irreducible}} (1 - g ^{-s})^{-1}$
Möbius function	$\mu(p_1 \cdots p_k) = (-1)^k$	$\mu(g_1 \cdots g_k) = (-1)^k$

Table 1: Integers and Polynomials.

A.2 Handbook of Galois theory for finite fields

Theorem A.1. Let p be a prime number, and let n be a positive integer. Up to isomorphism, there is a unique finite field of order p^n , which we denote by \mathbb{F}_{p^n} . It can be constructed as a splitting field of the polynomial $T^{p^n} - T$ over \mathbb{F}_p .

Exercise A.2.1. 1. Let $p = 3$. Prove that both $g_1(T) = T^2 + 1$ and $g_2(T) = T^2 + T + 2$ are irreducible polynomials over \mathbb{F}_3 .

2. Find all isomorphisms between the finite fields $\mathbb{F}_3[T]/(g_1(T))$ and $\mathbb{F}_3[T]/(g_2(T))$. In other words, find all polynomials $h(T) \in \mathbb{F}_3[T]/(g_2(T))$ such that $g_1(h(T))$ is a multiple of $g_2(T)$. Then the map $T \mapsto h(T)$ gives an isomorphism between the two finite fields.¹⁸

Theorem A.2. Let $S_p(d)$ be the set of all monic irreducible polynomials of degree d over \mathbb{F}_p . Then the following holds:

$$T^{p^n} - T = \prod_{d|n} \prod_{f \in S_p(d)} f(T). \quad (31)$$

In other words, the polynomial $T^{p^n} - T$ is equal to the product of all monic irreducible polynomials of degree d over \mathbb{F}_p , where d divides n .

Exercise A.2.2. Prove that the product of all monic irreducible polynomials of degree 3 over \mathbb{F}_p is

$$T^{(p^2+p)(p-1)} + \dots + T^{2(p-1)} + T^{p-1} + 1.$$

Can you generalize this to other degrees?

Theorem A.3. The Galois group $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n , generated by the Frobenius automorphism $\sigma : x \mapsto x^p$.

¹⁸Hint: There are exactly two such polynomials (modulo $g_2(T)$).

A.3 Handbook of Sage functions

Here we give some useful Sage functions for working with finite fields and polynomials. First, finite fields can be defined as follows:

```
k = GF(3)
```

This defines the finite field \mathbb{F}_3 . If you want to define a finite field of order p^n , you can write as

```
k.<a> = GF(3^2, 'a')
```

where 'a' is the name of the generator of the field.

References

- [1] APOSTOL, T. M. *Introduction to analytic number theory*. Springer Science & Business Media, 2013.
- [2] BAUMGART, O. *The quadratic reciprocity law: A collection of classical proofs*. Birkhäuser, 2015.
- [3] CONRAD, K. Quadratic reciprocity in characteristic 2. <https://kconrad.math.uconn.edu/blurbs/ugradnumthy/QRchar2.pdf>. Accessed: 2025-06-05.
- [4] CONRAD, K. Quadratic reciprocity in odd characteristic. <https://kconrad.math.uconn.edu/blurbs/ugradnumthy/QRcharp.pdf>. Accessed: 2025-06-05.
- [5] DE LA VALLÉE POUSSIN, C. Sur la fonction $\zeta(s)$ de Riemann et le nombre des nombres premiers inférieurs à une limite donnée. *Mémoires de l'Académie royale de Belgique* 59, 1 (1899), 1–74.
- [6] ERDÖS, P. On a new method in elementary number theory which leads to an elementary proof of the prime number theorem. *Proceedings of the National Academy of Sciences* 35, 7 (1949), 374–384.
- [7] LEMMERMEYER, F. Proofs of the Quadratic Reciprocity Law. https://web.archive.org/web/20250106010310/https://www.mathi.uni-heidelberg.de/%7Eflemmermeyer/qrg_proofs.html. Accessed: 2025-06-05.
- [8] LITTLEWOOD, J. E. Sur la distribution des nombres premiers. *CR Acad. Sci. Paris* 158, 1869 (1914), 1872.
- [9] NEWMAN, D. J. Simple analytic proof of the prime number theorem. *The American Mathematical Monthly* 87, 9 (1980), 693–696.
- [10] RIEMANN, B. Ueber die Anzahl der Primzahlen unter einer gegebenen Grosse. *Ges. Math. Werke und Wissenschaftlicher Nachlaß* 2, 145–155 (1859), 2.
- [11] ROSEN, M. *Number theory in function fields*, vol. 210. Springer Science & Business Media, 2013.
- [12] SELBERG, A. An elementary proof of the prime-number theorem. *Annals of Mathematics* 50, 2 (1949), 305–313.
- [13] SERRE, J.-P. *A course in arithmetic*, vol. 7. Springer Science & Business Media, 2012.
- [14] STEIN, E. M., AND SHAKARCHI, R. *Complex analysis*, vol. 2. Princeton University Press, 2010.
- [15] VON KOCH, H. Sur la distribution des nombres premiers. *Acta Mathematica* 24, 1 (1901), 159.
- [16] ZAGIER, D. Newman’s short proof of the prime number theorem. *The American mathematical monthly* 104, 8 (1997), 705–708.