2025年臺灣國際科學展覽會
優勝作品專輯

作品編號　010041

參展科別　數學

作品名稱　Equation of Ellipse over Fp and Pairs of Quadratic Residues/Nonresidues Related to Catalan Numbers

得獎獎項　二等獎

就讀學校　Seoul Science High School
作者姓名　MINJAE KIM
HYEONGJOE CHU

作者照片

Equation of Ellipse over $\mathbb{F}_p$ and Pairs of Quadratic Residues/Nonresidues Related to Catalan Numbers

Minjae Kim, Hyeongjoe Chu, Minseop Lee

November 2024

Abstract

The equation of an ellipse and quadratic residues are well-known concepts in elementary geometry and number theory, respectively. While the properties of ellipse equations in Euclidean space have been extensively studied, many characteristics of quadratic residues, such as consecutive quadratic residues, have also been explored in past research.

In this study, we discovered the characteristic polynomial of the equation of an ellipse over finite fields $\mathbb{F}_p$, a single-variable polynomial that shares the same roots as the ellipse. Furthermore, by examining the parallels between the equation of an ellipse and the pairs of residues and nonresidues, we derived a characteristic polynomial for this concept and demonstrated its connection to the Catalan number, a significant sequence in combinatorics.

This research was conducted through the following steps. First, the power sums of the roots of the ellipse in $\mathbb{F}_p$ were calculated using the Legendre symbol and Euler's criterion. Next, the characteristic polynomial of the ellipse was determined using Newton's identity, generating functions, and Vieta's theorem. Finally, leveraging the equivalence between the equation of the ellipse and the pairs of residues and nonresidues, we established the main results connecting these two concepts with Catalan numbers.

1 Introduction

An ellipse is a well-known structure in Euclidean space defined as the set of points for which the sum of the two distances to two fixed points is a constant. Euclidean space is continuous, and the equation of an ellipse can be extended into discrete fields such as $\mathbb{F}_p$ as shown below.

$$ax^2 + by^2 \equiv 1 \pmod{p}$$

Unlike Euclidean space, the properties of elliptic equations in discrete spaces are not well studied.

This study investigates the relationship between the equation of an ellipse in $\mathbb{F}_p$ and the Catalan numbers, as well as the relationship between pairs of residues/nonresidues and polynomials that have Catalan numbers as coefficients. In this section, we aim to briefly introduce the key findings and the flow of the research.

In this paper, we will only consider elliptic equations of the form $ax^2+by^2 \equiv 1 \pmod{p}$. Additionally, we will focus solely on the properties of x, as the properties of y can be determined by exchanging a and b. Therefore, this set will be of primary interest to us.

Definition 1.1 (Solutions for the Equation of an Ellipse)**.** The set of solutions for the equation of the ellipse is defined as follows:

$$X_p(a,b) = \left\{ x \mid x \in \mathbb{F}_p, \exists y \in \mathbb{F}_p, ax^2 + by^2 \equiv 1 \pmod{p} \right\}. \tag{1}$$

First, we investigated some properties of the elements of $X_p(a,b)$. From those properties, we derived the polynomial whose solution set is $X_p(a,b)$. The polynomials are represented as follows:

Theorem 1.1 (Relation between Catalan Numbers and the Equation of an Ellipse over $\mathbb{F}_p$)**.** *For $t = \frac{1}{2}\left(p+1+\left(\frac{a}{p}\right)-\left(\frac{-ab}{p}\right)\right)$, the following equations hold: (Here, all fractions should be considered as arithmetic inverses.)*

- *If $\left(\frac{a}{p}\right) = -1$ and $\left(\frac{-b}{p}\right) = -1$,*

$$\prod_{\alpha \in X_p(a,\ b)} (x-\alpha) \equiv \sum_{i=0}^{\left[\frac{t}{2}\right]} \frac{C_{2i}}{4^{2i}} a^{-i} x^{t-2i} \pmod{p}$$

- *If $\left(\frac{a}{p}\right) = -1$ and $\left(\frac{-b}{p}\right) = 1$,*

$$\prod_{\alpha \in X_p(a,\ b)} (x-\alpha) \equiv \sum_{i=0}^{\left[\frac{t}{2}\right]} -\frac{a^{-i}}{2} \frac{C_{2i-1}}{4^{2i-1}} x^{t-2i} \pmod{p}$$

- *If $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{-b}{p}\right) = 1$,*

$$\prod_{\alpha \in X_p(a,\ b)} (x-\alpha) \equiv \sum_{i=0}^{\left[\frac{t}{2}\right]} -a^{-i} \left(\frac{C_{2i}}{4^{2i}} + \frac{C_{2i-1}}{4^{2i-1}} \right) x^{t-2i} \pmod{p}$$

- *If $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{-b}{p}\right) = -1$,*

$$\prod_{\alpha \in X_p(a,\ b)} (x-\alpha) \equiv \sum_{i=0}^{\left[\frac{t}{2}\right]} -\frac{a^{-i}}{2} \left(\frac{C_{2i-1}}{4^{2i-1}} + \frac{C_{2i-2}}{4^{2i-2}} \right) x^{t-2i} \pmod{p}$$

Since the equation of the ellipse over $\mathbb{F}_p$ is quadratic, it has a deep relationship with quadratic residues. By investigating a special ellipse equation, we found the relationship between polynomials with Catalan number coefficients and pairs of residues and nonresidues. The definitions and main results are provided below.

Definition 1.2 (Pairs of Residues/Nonresidues)**.** The sets of pairs of residues/nonresidues are defined as follows:

$$A_p = \left\{ x \mid \left(\frac{x}{p}\right) = 1, \left(\frac{1-x}{p}\right) = 1 \right\} \tag{2}$$

$$B_p = \left\{ x \mid \left(\frac{x}{p}\right) = 1, \left(\frac{1-x}{p}\right) = -1 \right\} \tag{3}$$

$$\Gamma_p = \left\{ x \mid \left(\frac{x}{p}\right) = -1, \left(\frac{1-x}{p}\right) = 1 \right\} \tag{4}$$

$$\Delta_p = \left\{ x \mid \left(\frac{x}{p}\right) = -1, \left(\frac{1-x}{p}\right) = -1 \right\} \tag{5}$$

Definition 1.3 (Polynomials with Catalan Number Coefficients)**.** For an odd prime p, $P_1(x)$ and $P_2(x)$ are defined as follows:

$$P_1(x) = \sum_{i=0}^{\left[\frac{p-1}{4}\right]} 4^{-2i} C_{2i} x^i \tag{6}$$

$$P_2(x) = \sum_{i=0}^{\left[\frac{p+1}{4}\right]} 4^{-2i-1} C_{2i-1} x^i \tag{7}$$

Theorem 1.2 (Relation between Catalan Numbers and Pairs of Residues/Nonresidues)**.** *For a prime $p > 3$:*

$$\prod_{\alpha \in A_p \cup \{1\}} (x-\alpha) \equiv 4^{-1} \left(3\left(\frac{-1}{p}\right) + 1\right) (P_1(x) + P_2(x)) \pmod{p} \tag{8}$$

$$\prod_{\alpha \in B_p \cup \{1\}} (x-\alpha) \equiv 4^{-1} \left(3\left(\frac{-1}{p}\right) + 1\right) (xP_1(x) + P_2(x)) \pmod{p} \tag{9}$$

$$\prod_{\alpha \in \Gamma_p} (x-\alpha) \equiv 4^{-1} \left(-\left(\frac{-1}{p}\right) + 3\right) P_1(x) \pmod{p} \tag{10}$$

$$\prod_{\alpha \in \Delta_p} (x-\alpha) \equiv 4^{-1} \left(-\left(\frac{-1}{p}\right) + 3\right) P_2(x) \pmod{p} \tag{11}$$

2 Power Sums of Solutions of Ellipse over $\mathbb{F}_p$

From now on, we consider p as an odd prime number and a, b as two integers that are relatively prime with p, where $p \nmid a, b$.

Definition 2.1. An alternative set of solutions for the equation of the ellipse is defined as follows:

$$X'_p(a,b) = \left\{x^2 \mid x \in X_p(a,b), x^2 \not\equiv 0, a^{-1} \pmod{p}\right\} \tag{12}$$

Definition 2.2. For an integer $k \geq 0$, the power sums of the elements of $X_p(a,b)$ are defined as follows: (Note that $p_0 = |X_p(a,b)|$)

$$p_k = \sum_{x \in X_p(a,b)} x^k \tag{13}$$

First, we will derive the formula for p_0 and then generalize the formula to p_k.

Lemma 2.1. *For a non-negative integer $k < \frac{p-1}{2}$, the equation below holds:*

$$\sum_{x=1}^{p-1} x^k \left(\frac{ax+b}{p}\right) \equiv 0 \pmod{p} \tag{14}$$

Proof. By Euler's criterion [4],

$$\sum_{x=1}^{p-1} x^k \left(\frac{ax+b}{p}\right) \equiv \sum_{x=1}^{p-1} x^k (ax+b)^{\frac{p-1}{2}} \pmod{p}.$$

Since every term on the right-hand side has a degree lower than $p-1$, the sum of each term with the same degree vanishes. Therefore, the equation holds. □

Lemma 2.2. *The following equation holds:*

$$\sum_{x=1}^{p-1} \left(\frac{ax^2+bx}{p}\right) = -\left(\frac{a}{p}\right) \tag{15}$$

Proof. Since p is an odd prime number,

$$\left(\frac{ax^2+bx}{p}\right) = \left(\frac{x^{-1}}{p}\right)\left(\frac{ax+b}{p}\right) = \left(\frac{a+bx^{-1}}{p}\right).$$

Note that $\{a+bx^{-1} \mid 1 \leq x \leq p-1\} \cup \{a\}$ is a complete residue system modulo p. Finally, from Lemma 2.1,

$$\sum_{x=1}^{p-1} \left(\frac{ax^2+bx}{p}\right) = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) - \left(\frac{a}{p}\right) = -\left(\frac{a}{p}\right).$$

□

Definition 2.3. The function $\chi_{p,a,b}(x)$ is defined as follows:

$$\chi_{p,a,b}(x) = \left(1 + \left(\frac{x}{p}\right)\right)\left(1 + \left(\frac{-ab^{-1}x + b^{-1}}{p}\right)\right). \tag{16}$$

Lemma 2.3. *The equation below holds:*

$$\chi_{p,a,b}(x) = \begin{cases} 4 & \text{if } x \in X'_p(a,b), \\ 1 + \left(\frac{b}{p}\right) & \text{if } x \equiv 0 \pmod{p}, \\ 1 + \left(\frac{a}{p}\right) & \text{if } x \equiv a^{-1} \pmod{p}, \\ 0 & \text{otherwise.} \end{cases} \tag{17}$$

Proof. Let's verify the equation case by case. If $x \in X'_p(a,b)$, the equation holds since $\left(\frac{x}{p}\right) = \left(\frac{-ab^{-1}x+b^{-1}}{p}\right) = 1$ by Definition 2.1. In the cases where $x \equiv 0 \pmod{p}$ or $x \equiv a^{-1} \pmod{p}$, the equation holds because $1+\left(\frac{a^{-1}}{p}\right) = 1+\left(\frac{a}{p}\right)$ and $1 + \left(\frac{b^{-1}}{p}\right) = 1 + \left(\frac{b}{p}\right)$. For all other cases, one of $\left(\frac{x}{p}\right)$ or $\left(\frac{-ab^{-1}x+b^{-1}}{p}\right)$ is -1, so the value is 0. □

Theorem 2.4. *The zero-power sum (number of solutions) is represented as follows:*

$$p_0 = \frac{1}{2}\left\{p + 1 + \left(\frac{a}{p}\right) - \left(\frac{-ab}{p}\right)\right\}. \tag{18}$$

Proof. By Lemma 2.3, $|X'_p(a,b)|$ is equal to:

$$\frac{1}{4}\sum_{1\le x\le p-1, p\nmid x-a^{-1}} \chi_{p,a,b}(x) =$$

$$\frac{1}{4}\left\{\sum_{x=1}^{p-1}\left(1+\left(\frac{x}{p}\right)\right)\left(1+\left(\frac{-ab^{-1}x+b^{-1}}{p}\right)\right) - 1 - \left(\frac{a}{p}\right)\right\}.$$

Using Lemmas 2.1 and 2.2, we have:

$$\frac{1}{4}\sum_{x=1}^{p-1}\left(1+\left(\frac{x}{p}\right)\right)\left(1+\left(\frac{-ab^{-1}x+b^{-1}}{p}\right)\right) =$$

$$\frac{1}{4}\sum_{x=1}^{p-1}\left(1+\left(\frac{x}{p}\right)+\left(\frac{-ab^{-1}x+b^{-1}}{p}\right)+\left(\frac{-ab^{-1}x^2+b^{-1}x}{p}\right)\right) =$$

$$\frac{1}{4}\left\{p - 1 - \left(\frac{b}{p}\right) - \left(\frac{-ab}{p}\right)\right\}.$$

Hence:

$$|X'_p(a,b)| = \frac{1}{4}\left\{p - 2 - \left(\frac{a}{p}\right) - \left(\frac{b}{p}\right) - \left(\frac{-ab}{p}\right)\right\}.$$

If $x^2 \not\equiv 0, a^{-1} \pmod{p}$, then $x \in X_p(a,b) \Leftrightarrow x^2 \in X'_p(a,b)$. Therefore, we can calculate p_0 as follows:

$$p_0 = 2 \cdot |X'_p(a,b)| + \frac{1}{2}\left(1+\left(\frac{b}{p}\right)\right) + 1 + \left(\frac{a}{p}\right).$$

Substituting the value of $|X'_p(a,b)|$, we get:

$$p_0 = \frac{1}{2}\left\{p + 1 + \left(\frac{a}{p}\right) - \left(\frac{-ab}{p}\right)\right\}.$$

□

Lemma 2.5. *For a positive integer $k < \frac{p-1}{2}$, the following equation holds:*

$$\sum_{x=1}^{p-1} x^k \left(\frac{ax^2+bx}{p}\right) \equiv -\binom{\frac{p-1}{2}}{k}\left(\frac{a}{p}\right)(a^{-1}b)^k \pmod{p} \tag{19}$$

Proof. By Euler's criterion [4],

$$\sum_{x=1}^{p-1} x^k \left(\frac{ax^2+bx}{p}\right) \equiv \sum_{x=1}^{p-1} x^k (ax^2+bx)^{\frac{p-1}{2}} \pmod{p}.$$

Since the degree of the right-hand side is lower than $\frac{3(p-1)}{2}$, sums of terms with degrees other than $p-1$ vanish. For the terms of degree $p-1$, by Fermat's Little Theorem, the value matches the right-hand side of the desired equation. □

Theorem 2.6. *For $p > 3$ and a positive integer $k < \frac{p-1}{2}$, the following equations hold:*

$$\begin{aligned} p_{2k-1} &\equiv 0, \\ p_{2k} &\equiv a^{-k}\left\{-2^{-(2k+1)}\binom{2k}{k}\left(\frac{-ab}{p}\right) + \frac{1}{2}\left(1+\left(\frac{a}{p}\right)\right)\right\}. \pmod{p} \end{aligned} \tag{20}$$

Proof. It follows that $p_{2k-1} \equiv 0$ because if $x \in X_p(a,b)$, then $-x \in X_p(a,b)$. The formula for the even power sums is now shown. The power sums of $X'_p(a,b)$ can be simplified as follows using Lemmas 2.1, 2.3, and 2.5:

$$\begin{aligned} \sum_{x \in X'_p(a,b)} x^k &\equiv \frac{1}{4}\left\{\sum_{x=1}^{p-1} x^k \chi_{p,a,b}(x) - a^{-k}\left(1+\left(\frac{a}{p}\right)\right)\right\} \\ &\equiv \frac{1}{4}\left\{\sum_{x=1}^{p-1} x^k \left(\frac{-ab^{-1}x^2+b^{-1}x}{p}\right) - a^{-k}\left(1+\left(\frac{a}{p}\right)\right)\right\} \\ &\equiv -\frac{a^{-k}}{4}\left\{(-1)^k\binom{\frac{p-1}{2}}{k}\left(\frac{-ab}{p}\right) + 1 + \left(\frac{a}{p}\right)\right\} \pmod{p}. \end{aligned}$$

Using the fact that $x^2 \equiv k$ has $1 + \left(\frac{k}{p}\right)$ solutions:

$$\begin{aligned} p_{2k} &\equiv 2 \cdot \sum_{x \in X'_p(a,b)} x^k + a^{-k} \cdot \left(1+\left(\frac{a}{p}\right)\right) \\ &\equiv -2^{-1}a^{-k}\left\{(-1)^k\binom{\frac{p-1}{2}}{k}\left(\frac{-ab}{p}\right) - 1 - \left(\frac{a}{p}\right)\right\} \pmod{p}. \end{aligned}$$

Since:

$$(-1)^k \binom{\frac{p-1}{2}}{k} \equiv \frac{\frac{1-p}{2} \cdots \frac{2k-1-p}{2}}{k!} \equiv 2^{-k} \frac{(2k-1)\cdots 1}{k!} \equiv 2^{-2k} \binom{2k}{k} \pmod{p},$$

the desired equation holds. □

3 Characteristic Polynomial of Ellipse over $\mathbb{F}_p$

In this section, we derive the characteristic polynomial of an ellipse over $\mathbb{F}_p$, which contains the roots of the ellipse, using a generating function based on the properties of the roots investigated.

Definition 3.1. For the ellipse $ax^2 + by^2 \equiv 1 \pmod{p}$, a monic polynomial f in $\mathbb{F}_p$ is called the characteristic polynomial of x when $x \in X_p(a, b)$ if and only if $f(x) = 0$.

Definition 3.2. The greatest common divisor of all characteristic polynomials of the ellipse with respect to x is referred to as the minimal characteristic polynomial of x for the ellipse.

Definition 3.3 (Catalan Number)**.** For $n \geq 0$, the n-th Catalan number is defined as:

$$C_n = \frac{1}{n+1} \binom{2n}{n}.$$

Definition 3.4. The functions $F(x)$ and $C(x)$ denote the generating functions of the sequences $\binom{2n}{n}$ and C_n, respectively.

Definition 3.5. If $M(x)$ is the generating function of the sequence a_n, then $M_2(x)$ is defined as the generating function of the sequence a_{2n}.

Theorem 3.1. *The following equation holds:*

$$M_2(x) = \frac{M(\sqrt{x}) + M(-\sqrt{x})}{2}.$$

Proof. This follows directly by calculation. □

Theorem 3.2. *The formulas for $F(x)$ and $C(x)$ are as follows:*

$$F(x) = \frac{1}{\sqrt{1-4x}}, \quad C(x) = \frac{1-\sqrt{1-4x}}{2x}.$$

Proof. See [1]. □

Using these formulas and Theorem 3.1, we can derive the formulas for $F_2(x)$ and $C_2(x)$.

Definition 3.6. For the elements of $X_p(a,b) = \{x_1, x_2, \ldots, x_t\}$, the elementary symmetric polynomial of the roots of the ellipse is defined as:

$$\sigma_k = \sum_{1 \le i_1 < \ldots < i_k \le |X_p(a,b)|} x_{i_1} \cdots x_{i_k}.$$

Theorem 3.3 (Newton's Identity)**.** *For a non-negative integer $k \le |X_p(a,b)|$, the following relationship holds:*

$$k\sigma_k = \sum_{i=1}^{k} (-1)^{i-1} \sigma_{k-i} p_i.$$

Proof. See [5] or [3]. □

Theorem 3.4. *For a non-negative integer $k < \frac{p-1}{2}$, $\sigma_{2k+1} = 0$ holds.*

Proof. We prove the theorem using mathematical induction. By Theorem 2.6, $\sigma_1 = p_1 = 0$. Assuming the expression holds for all $k \le n-1$, we can express σ_{2n+1} using Newton's identities:

$$(2n+1)\sigma_{2n+1} = \sum_{i=1}^{2n+1} (-1)^{i-1} \sigma_{2n+1-i} p_i.$$

From Theorem 2.6 and the inductive assumption, it follows that for odd i, $p_i = 0$ and $\sigma_i = 0$. Thus, $\sigma_{2n+1} = 0$, completing the proof. □

Theorem 3.5. *For the non-negative integer $k < \frac{p-1}{2}$, the following equation holds:*

$$\sigma_{2k} \equiv \begin{cases} a^{-k} 2^{-4k} C_{2k} & \text{if } \left(\frac{-b}{p}\right) = -1, \left(\frac{a}{p}\right) = -1, \\ -a^{-k} 2^{-(4k-1)} C_{2k-1} & \text{if } \left(\frac{-b}{p}\right) = 1, \left(\frac{a}{p}\right) = -1, \\ -a^{-k} 2^{-4k} \left(C_{2k} + 4C_{2k-1}\right) & \text{if } \left(\frac{-b}{p}\right) = 1, \left(\frac{a}{p}\right) = 1, \\ -a^{-k} 2^{-4k} \left(2C_{2k-1} + 8C_{2k-2}\right) & \text{if } \left(\frac{-b}{p}\right) = -1, \left(\frac{a}{p}\right) = 1, \end{cases} \pmod{p}$$

Proof. From Theorem 2.6, when $\left(\frac{-ab}{p}\right) = 1$ and $\left(\frac{a}{p}\right) = -1$, the equations

$$p_{2k+1} \equiv 0 \pmod{p}, \quad p_{2k} \equiv -a^{-k} 2^{-(2k+1)} \binom{2k}{k} \pmod{p}$$

hold.

We prove the theorem using mathematical induction. For $k = 0$, $\sigma_0 = 1$, so the equation is satisfied. Assuming the equation holds for all $k \le n-1$, Newton's identities give:

$$2n\sigma_{2n} \equiv -\sum_{i=0}^{n-1} \sigma_{2i} p_{2n-2i} \equiv 2^{-1} (16a)^{-n} \sum_{i=0}^{n-1} 2^{2(n-i)} C_{2i} \binom{2n-2i}{n-i} \pmod{p}.$$

The generating function for $2^{2i}\binom{2i}{i}$ is $F(4x)$, and the generating function for C_{2i} is $C_2(x)$. From the calculations, we know:

$$F(4x)C_2(x) = 2F_2(x) - C_2(x),$$

and the sequence corresponding to this product is $\binom{4n+1}{2n}$. Thus:

$$\binom{4n+1}{2n} = \sum_{i=0}^{n} 2^{2(n-i)} C_{2i} \binom{2n-2i}{n-i} = C_{2n} + \sum_{i=0}^{n-1} 2^{2(n-i)} C_{2i} \binom{2n-2i}{n-i}.$$

Substituting this back, we find:

$$2n\sigma_{2n} \equiv 2^{-1}\,(16a)^{-n} \left\{ \binom{4n+1}{2n} - C_{2n} \right\} \equiv 2^{-1}(16a)^{-n} \frac{4n}{2n+1} \binom{4n}{2n} \pmod{p}.$$

Simplifying further and multiplying both sides by $(2n)^{-1}$, the expression holds for $k = n$, completing the proof by induction.

When $\left(\frac{-ab}{p}\right) = -1$ and $\left(\frac{a}{p}\right) = -1$, from Theorem 2.6,

$$p_{2k} \equiv a^{-k} 2^{-(2k+1)} \binom{2k}{k} \pmod{p}.$$

Mathematical induction will be used to prove the given expression. For $k = 0$, $\sigma_0 = 1$, so the equation holds. Assuming the expression holds for $k \leq n-1$, Newton's identities and the inductive hypothesis yield:

$$2n\sigma_{2n} \equiv -\sum_{i=0}^{n-1} \sigma_{2i} p_{2n-2i} \equiv (16a)^{-n} \sum_{i=0}^{n-1} 2^{2(n-i)} C_{2i-1} \binom{2n-2i}{n-i} \pmod{p}.$$

The generating function corresponding to the sequence $2^{2i}\binom{2i}{i}$ is $F(4x)$, and the generating function for $2C_{2i-1}$ is

$$G(x) = \sqrt{x}\left(C(\sqrt{x}) - C(-\sqrt{x})\right) - 1.$$

Furthermore, $F(4x)G(x) = -F_2(x)$, and the sequence corresponding to this function is $-\binom{4n}{2n}$. Using the properties of generating functions,

$$-\binom{4n}{2n} = 2C_{2n-1} + 2\sum_{i=0}^{n-1} 2^{2(n-i)} C_{2i-1} \binom{2n-2i}{n-i}.$$

Thus, the summation simplifies to:

$$2n\sigma_{2n} \equiv -2^{-1}\,(16a)^{-n} \left\{ 2C_{2n-1} + \binom{4n}{2n} \right\} \equiv -2^{-1}(16a)^{-n} 8n \cdot C_{2n-1} \pmod{p}.$$

Multiplying both sides by $(2n)^{-1}$, the expression holds for $k = n$. By induction, the expression holds for all $0 \leq k < \frac{p-1}{2}$.

When $\left(\frac{-ab}{p}\right) = 1$ and $\left(\frac{a}{p}\right) = 1$, from Theorem 2.6,

$$p_{2k} \equiv -a^{-k}2^{-(2k+1)}\binom{2k}{k} + a^{-k} \pmod{p}.$$

Using mathematical induction as before, for $k = 0$, $\sigma_0 = 1$, so the equation holds. Assuming the expression holds for $k \leq n-1$, Newton's identities and the inductive hypothesis yield:

$$\begin{aligned}
2n\sigma_{2n} &\equiv -\sum_{i=0}^{n-1} \sigma_{2i} p_{2n-2i} \\
&\equiv (16a)^{-n} \sum_{i=0}^{n-1} 2^{4(n-i)} \left(C_{2i} + 4C_{2i-1}\right) \\
&\quad - (16a)^{-n} \sum_{i=0}^{n-1} 2^{2(n-i)} \left(2^{-1}C_{2i} + 2C_{2i-1}\right) \binom{2n-2i}{n-i} \pmod{p}.
\end{aligned}$$

The third summation, previously calculated, is:

$$\sum_{i=0}^{n-1} 2^{2(n-i)} \left(2^{-1}C_{2i} + 2C_{2i-1}\right) \binom{2n-2i}{n-i} = -8n \cdot C_{2n-1} + 2n \cdot C_{2n}.$$

The generating function for 2^{4i} is $\frac{1}{1-16x}$, and the generating function for $C_{2i} + 4C_{2i-1}$ is $C_2(x) + 2G(x)$. Furthermore:

$$\frac{C_2(x) + 2G(x)}{1-16x} = \frac{1}{4\sqrt{x}} \left(\frac{1}{\sqrt{1+4\sqrt{x}}} - \frac{1}{\sqrt{1-4\sqrt{x}}} \right) = C_2(x) - 2F_2(x),$$

and the sequence corresponding to this function is $-\binom{4n+1}{2n}$. Using the properties of generating functions:

$$-\binom{4n+1}{2n} = \sum_{i=0}^{n-1} 2^{4(n-i)} \left(C_{2i} + 4C_{2i-1}\right) + C_{2n} + 4C_{2n-1}.$$

Thus, the summation simplifies to:

$$\begin{aligned}
2n\sigma_{2n} &\equiv (16a)^{-n} \left\{ -\binom{4n+1}{2n} - C_{2n} - 4C_{2n-1} + 8n \cdot C_{2n-1} - 2n \cdot C_{2n} \right\} \\
&\equiv (16a)^{-n} \left\{ -2\binom{4n}{2n} - 4C_{2n-1} + 8n \cdot C_{2n-1} - 2n \cdot C_{2n} \right\} \\
&\equiv -(16a)^{-n}(2n \cdot C_{2n} + 8n \cdot C_{2n-1}) \pmod{p}.
\end{aligned}$$

Multiplying both sides by $(2n)^{-1}$, the expression holds for $k = n$. By induction, the expression holds for all $0 \leq k < \frac{p-1}{2}$.

When $\left(\frac{-ab}{p}\right) = -1$ and $\left(\frac{a}{p}\right) = 1$, from Theorem 2.6,

$$p_{2k} \equiv a^{-k} 2^{-(2k+1)} \binom{2k}{k} + a^{-k} \pmod{p}.$$

We proceed by mathematical induction as before. For $k = 0$, $\sigma_0 = 1$, so the equation holds. Assuming that the expression holds for $k \leq n-1$, we apply Newton's identities and the inductive hypothesis:

$$\begin{aligned} 2n\sigma_{2n} &\equiv -\sum_{i=0}^{n-1} \sigma_{2i} p_{2n-2i} \\ &\equiv (16a)^{-n} \sum_{i=0}^{n-1} 2^{4(n-i)} \left(2C_{2i-1} + 8C_{2i-2}\right) \\ &\quad + (16a)^{-n} \sum_{i=0}^{n-1} 2^{2(n-i)} \left(C_{2i-1} + 4C_{2i-2}\right) \binom{2n-2i}{n-i} \pmod{p}. \end{aligned}$$

The summation in the third line of the equation was calculated earlier:

$$\sum_{i=0}^{n-1} 2^{2(n-i)} \left(C_{2i-1} + 4C_{2i-2}\right) \binom{2n-2i}{n-i} = -4n \cdot C_{2n-1} + (16n-16) \cdot C_{2n-2}.$$

The generating function corresponding to the sequence 2^{4i} is $\frac{1}{1-16x}$, and the generating function for $2C_{2i-1} + 8C_{2i-2}$ is $G(x) + 8xC_2(x)$. Furthermore:

$$\frac{8xC_2(x) + G(x)}{1-16x} = \frac{1}{2}\left\{-C_2(x) + \frac{C_2(x) + 2G(x)}{1-16x}\right\} = -F_2(x),$$

and the sequence corresponding to this function is $-\binom{4n}{2n}$. Using the properties of generating functions:

$$-\binom{4n}{2n} = \sum_{i=0}^{n-1} 2^{4(n-i)} \left(2C_{2i-1} + 8C_{2i-2}\right) + 2C_{2n-1} + 8C_{2n-2}.$$

Thus, the summation simplifies as:

$$\begin{aligned} 2n\sigma_{2n} &\equiv (16a)^{-n} \left\{-8n \cdot C_{2n-1} - 8C_{2n-2} - 4n \cdot C_{2n-1} + (16n-16) \cdot C_{2n-2}\right\} \\ &\equiv -(16a)^{-n} (4n \cdot C_{2n-1} + 16n \cdot C_{2n-2}) \pmod{p}. \end{aligned}$$

Multiplying both sides by $(2n)^{-1}$, the expression holds for $k = n$. By mathematical induction, the given expression holds for all $0 \leq k < \frac{p-1}{2}$. □

Remark. At Theorem 3.5, we used the notation $C_{-1} = -\frac{1}{2}$ and $C_{-2} = 0$. These values satisfy the analytical extension of the Catalan number as described in [2].

From Theorems 3.4 and 3.5, we have derived the elementary symmetric polynomials in terms of the roots of the ellipse defined by $ax^2 + by^2 \equiv 1 \pmod{p}$. Therefore, using Vieta's theorem, we can now determine the minimal characteristic polynomial of the ellipse as defined in Definition 3.2 and prove Theorem 1.1.

Proof. By Vieta's theorem, the minimal characteristic polynomial of the ellipse can be written as:

$$\prod_{\alpha \in X_p(a,b)} (x - \alpha) \equiv \sum_{i=0}^{\left[\frac{t}{2}\right]} \sigma_{2i} x^{t-2i}.$$

Substituting the result from Theorem 3.5, we can derive the four equations stated in Theorem 1.1. □

4 Relation of the Characteristic Polynomial and the Pairs of Quadratic Residues/Nonresidues

Lemma 4.1. *For an odd prime p, the following hold:*

$$C_{\frac{p-1}{2}} \equiv 2\left(\frac{-1}{p}\right) \pmod{p} \quad \textit{and} \quad C_{\frac{p-3}{2}} \equiv -4^{-1}\left(\frac{-1}{p}\right) \pmod{p}.$$

Proof. We calculate $C_{\frac{p-1}{2}}$ as follows:

$$C_{\frac{p-1}{2}} \equiv \frac{2}{p+1}\binom{p-1}{\frac{p-1}{2}} \equiv \frac{2(p-1)!}{\left(\frac{p-1}{2}\right)!^2} \pmod{p}.$$

Using the result:

$$\left(\frac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p-1}{2}}(p-1)! \pmod{p},$$

we combine these equations to obtain:

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

Similarly, for $C_{\frac{p-3}{2}}$, we calculate:

$$C_{\frac{p-3}{2}} \equiv \frac{2}{p-1}\binom{p-3}{\frac{p-3}{2}} \equiv \frac{-2(p-3)!}{\left(\frac{p-3}{2}\right)!^2} \pmod{p}.$$

Using the result:

$$\left(\frac{p-3}{2}\right)!^2 \equiv (-1)^{\frac{p-3}{2}}(p-1)! \cdot (-4) \pmod{p},$$

we combine these equations to obtain:

$$C_{\frac{p-3}{2}} \equiv 4^{-1}(-1)^{\frac{p-3}{2}} \equiv -4^{-1}\left(\frac{-1}{p}\right) \pmod{p}.$$

□

Using the extended definition of the Catalan number as previously described in Section 3, we derive the following theorem:

Theorem 4.2. *For a prime $p > 3$,*

$$P_1(x) = \frac{1}{2}\left(\left(\frac{-1}{p}\right) + 3\right) \prod_{k \in \Gamma_p} (x - k).$$

Proof. Consider the equation $g^{-1}x^2 - g^{-1}y^2 \equiv 1 \pmod{p}$. By Theorem 2.4, the number of solutions is $\frac{p-1}{2}$. Excluding 0, the solutions of the ellipse can be written as $\pm a_1, \pm a_2, \ldots, \pm a_t$, where $t = \left[\frac{p-1}{4}\right]$. By Theorem 3.5, the characteristic polynomial of this ellipse is:

$$\sum_{i=0}^{t} 4^{-2i} g^i C_{2i} x^{\frac{p-1}{2}-2i} = x^{\frac{p-1}{2}-2t} \prod_{i=1}^{t} (x^2 - a_i^2).$$

Substituting $\frac{g}{x^2} = X$ and rearranging the equation gives:

$$P_1(X) = A \prod_{i=1}^{t} (X - a_i^{-2} g),$$

where $A = (-1)^t a_1^2 \cdots a_t^2 g^{-t}$. By comparing the highest-order terms on both sides, we find:

$$A \equiv 4^{-2t} C_{2t} \pmod{p}.$$

When $p = 4t+1$, $16^t \equiv 2^{p-1} \equiv 1 \pmod{p}$, and $C_{2t} \equiv 2 \pmod{p}$, which gives $A \equiv 2 \pmod{p}$. When $p = 4t+3$, $16^t \equiv 4^{-1} \pmod{p}$, and $C_{2t} \equiv 4^{-1} \pmod{p}$, which gives $A \equiv 1 \pmod{p}$. Thus, in general:

$$A \equiv \frac{1}{2}\left(\left(\frac{-1}{p}\right) + 3\right).$$

Since $\Gamma_p = \{a_1^{-2} g, \ldots, a_t^{-2} g\}$ by the definition of the ellipse equation, the theorem is proved. □

Theorem 4.3. *For a prime $p > 3$,*

$$P_2(x) = \frac{1}{2}\left(\left(\frac{-1}{p}\right) - 3\right) \prod_{k \in \Delta_p} (x - k).$$

Proof. Consider $g^{-1}x^2 - y^2 \equiv 1 \pmod{p}$. By Theorem 2.4, the number of solutions is $\frac{p+1}{2}$. Excluding 0, the solutions of the ellipse can be represented as $\pm a_1, \pm a_2, \ldots, \pm a_t$, where $t = \left[\frac{p+1}{4}\right]$. By Theorem 3.5, the characteristic polynomial of this ellipse is:

$$\sum_{i=0}^{t} -2 \cdot 4^{-2i} g^i C_{2i-1} x^{\frac{p+1}{2}-2i} = x^{\frac{p+1}{2}-2t} \prod_{i=1}^{t} (x^2 - a_i^2).$$

Substituting $\frac{g}{x^2} = X$ and rearranging the equation gives:

$$P_2(X) = -2A \prod_{i=1}^{t} (X - a_i^{-2} g),$$

where $A = (-1)^t a_1^2 \cdots a_t^2 g^{-t}$. By a process similar to Theorem 4.2, we obtain:

$$-2A \equiv \frac{1}{2}\left(\left(\frac{-1}{p}\right) - 3\right).$$

Since $\Delta_p = \{a_1^{-2} g, \ldots, a_t^{-2} g\}$ by the definition of the ellipse equation, the theorem is proved. □

Theorem 4.4. *For a prime $p > 3$,*

$$P_1(x) + P_2(x) = \frac{1}{2}\left(3\left(\frac{-1}{p}\right) - 1\right) \prod_{k \in A_p \cup \{1\}} (x - k).$$

Proof. Consider $x^2 - y^2 \equiv 1 \pmod{p}$. By Theorem 2.4, the number of solutions is $\frac{p+1}{2}$. Excluding 0, the solutions of the ellipse can be represented as $\pm a_1, \pm a_2, \ldots, \pm a_t$, where $t = \left[\frac{p+1}{4}\right]$. By Theorem 3.5, the characteristic polynomial of this ellipse is:

$$\sum_{i=0}^{t} -4^{-2i}(C_{2i} + 4C_{2i-1}) x^{\frac{p+1}{2}-2i} = x^{\frac{p+1}{2}-2t} \prod_{i=1}^{t} (x^2 - a_i^2).$$

Substituting $\frac{1}{x^2} = X$ and rearranging the equation gives:

$$\sum_{i=0}^{t} \left(4^{-(2i-1)} C_{2i-1} + 4^{-2i} C_{2i}\right) X^i = -A \prod_{i=1}^{t} (X - a_i^{-2}),$$

where $A = (-1)^t a_1^2 \cdots a_t^2$. Since $C_{\frac{p+1}{2}} \equiv 0 \pmod{p}$, the left-hand side matches $P_1(x) + P_2(x)$.

By a process similar to Theorem 4.3, we find:

$$-A \equiv \frac{1}{2}\left(3\left(\frac{-1}{p}\right) + 1\right) \pmod{p}.$$

Finally, since $A_p \cup \{1\} = \{a_1^{-2}, \ldots, a_t^{-2}\}$ by the definition of the ellipse equation, the theorem is proved. □

Theorem 4.5. *For a prime $p > 3$,*

$$xP_1(x) + P_2(x) = \frac{1}{2}\left(3\left(\frac{-1}{p}\right) + 1\right) \prod_{k \in B_p \cup \{1\}} (x - k).$$

Proof. Consider $x^2 - g^{-1}y^2 \equiv 1 \pmod{p}$. By Theorem 2.4, the number of solutions is $\frac{p+3}{2}$. Excluding 0, the solutions of the ellipse can be represented as $\pm a_1, \pm a_2, \ldots, \pm a_t$, where $t = \left[\frac{p+3}{4}\right]$. By Theorem 3.5, the characteristic polynomial of this ellipse is:

$$\sum_{i=0}^{t} -4^{-2i}\left(2C_{2i-1} + 8C_{2i-2}\right) x^{\frac{p+3}{2}-2i} = x^{\frac{p+3}{2}-2t} \prod_{i=1}^{t} (x^2 - a_i^2).$$

Substituting $\frac{1}{x^2} = X$ and rearranging the equation gives:

$$\sum_{i=0}^{t} \left(4^{-(2i-1)}C_{2i-1} + 4^{-(2i-2)}C_{2i-2}\right) X^i = -2A \prod_{i=1}^{t} (X - a_i^{-2}),$$

where $A = (-1)^t a_1^2 \cdots a_t^2$. Since $C_{\frac{p+1}{2}} \equiv 0 \pmod{p}$, the left-hand side matches $xP_1(x) + P_2(x)$.

By a process similar to Theorem 4.3, we find:

$$-2A \equiv \frac{1}{2}\left(3\left(\frac{-1}{p}\right) + 1\right).$$

Finally, since $B_p \cup \{1\} = \{a_1^{-2}, \ldots, a_t^{-2}\}$ by the definition of the ellipse equation, the theorem is proved. □

Now, it is straightforward to see that Theorems 4.2–4.5 are equivalent to Theorem 1.3. These theorems provide meaningful corollaries about the properties of polynomials with coefficients as Catalan numbers.

Corollary 4.5.1. *For a prime $p > 3$,*

$$P_1(x) \cdot P_2(x) = -2\left(x^{\frac{p-1}{2}} + 1\right),$$
$$xP_1(x)^2 + P_2(x)^2 = -4\left(x^{\frac{p+1}{2}} + 1\right).$$

Proof. The first equation follows directly since $\Gamma_p \cup \Delta_p$ is the set of quadratic nonresidues. Additionally, since $A_p \cup B_p \cup \{1\}$ is the set of quadratic residues, the following equation holds:

$$\left(xP_1(x) + P_2(x)\right)\left(P_1(x) + P_2(x)\right) = -2(x-1)\left(x^{\frac{p-1}{2}} - 1\right).$$

The second equation can then be derived by rearranging these equations. □

5 Conclusion

Our research has clarified the number-theoretical connections between the equation of an ellipse over finite fields, Catalan numbers, and pairs of residues and nonresidues. Firstly, we determined the power sums of the solutions to the equation of the ellipse using the properties of the Legendre symbol. Subsequently, we identified the characteristic polynomial of the equation of the ellipse by applying Newton's identity. By examining four distinct ellipse equations under conditions on $\left(\frac{a}{p}\right)$ and $\left(\frac{-ab}{p}\right)$, we established relationships between the pairs of residues/nonresidues and the two polynomials $P_1(x)$ and $P_2(x)$. These results demonstrate the Catalan number's role as a powerful tool for uncovering new aspects of mathematical theory, particularly within finite fields $\mathbb{F}_p$.

In Section 3, it was shown that the Catalan number can represent the exact roots of an ellipse in finite fields $\mathbb{F}_p$. Pell's equation over $\mathbb{F}_p$, as stated below, serves as a notable example of the Catalan number's significance since it is a special case of an ellipse:

$$x^2 - ny^2 \equiv 1 \pmod{p}.$$

Furthermore, in Section 4, we discovered that the Catalan number can also represent all pairs of residues and nonresidues.

This study not only provides a deeper understanding of the interplay between Catalan numbers and finite field theory but also opens new pathways for exploring the applications of Catalan numbers in number theory and beyond.

References

[1] H Alzer and GV Nagy. Some identities involving central binomial coefficients and catalan numbers. *Integers*, 20:A59, 2020.

[2] Wen-Hui Li, Jian Cao, Da-Wei Niu, Jiao-Lian Zhao, and Feng Qi. An analytic generalization of the catalan numbers and its integral representation. *arXiv preprint arXiv:2005.13515*, 2020.

[3] DG Mead. Newton's identities. *The American mathematical monthly*, 99(8):749–751, 1992.

[4] Ivan Niven, Herbert S Zuckerman, and Hugh L Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, 1991.

[5] Doron Zeilberger. A combinatorial proof of newton's identities. *Discrete mathematics*, 49(3), 1984.

【評語】010041

The motivation of this work stems from solving a modular p elliptic equation. Treating these solutions as roots, the resulting polynomial under modulo p has coefficients related to Catalan numbers. On the other hand, based on whether r or 1-r is a quadratic residue modulo p, the solutions can be divided into four categories. In each category, the numbers treated as roots form a polynomial under modulo p, which is also related to Catalan numbers. The authors demonstrate exceptional mathematical ability, and the work showcases creativity. It is suggested that future research could explore whether these equations have specific applications in related mathematical fields.