International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:1, No:1, 2007

The Number of Rational Points on Conics $C_{p,k} : x^2 - ky^2 = 1$ over Finite Fields $\mathbf{F}_p$

Ahmet Tekcan

***Abstract*—** Let p be a prime number, $\mathbf{F}_p$ be a finite field, and let $k \in \mathbf{F}_p^*$. In this paper, we consider the number of rational points on conics $C_{p,k} : x^2 - ky^2 = 1$ over $\mathbf{F}_p$. We proved that the order of $C_{p,k}$ over $\mathbf{F}_p$ is $p-1$ if k is a quadratic residue mod p and is $p+1$ if k is not a quadratic residue mod p. Later we derive some results concerning the sums $\sum C_{p,k}^{[x]}(\mathbf{F}_p)$ and $\sum C_{p,k}^{[y]}(\mathbf{F}_p)$, the sum of $x-$ and $y-$coordinates of all points (x, y) on $C_{p,k}$, respectively.

***Keywords*—** elliptic curve, conic, rational points.

I. Introduction

Mordell began his famous paper [7] with the words *Mathematicians have been familiar with very few questions for so long a period with so little accomplished in the way of general results, as that of finding the rational points on elliptic curves*.

The history of elliptic curves is a long one, and exciting applications for elliptic curves continue to be discovered. Recently, important and useful applications of elliptic curves have been found for cryptography [3,5,6], for factoring large integers [4], and for primality proving [1,2]. The mathematical theory of elliptic curves was also crucial in the proof of Fermat's Last Theorem [11].

Let p be any prime number and let $\mathbf{F}_p$ be a finite field. An elliptic curve E over $\mathbf{F}_p$ is defined by an equation in the Weierstrass form

$$E : y^2 = x^3 + ax + b,$$

where $a, b \in \mathbf{F}_p$ and $4a^3 + 27b^2 \neq 0$. We can view an elliptic curve E as a curve in projective plane $\mathbf{P}^2$, with a homogeneous equation $y^2z = x^3 + axz^2 + bz^3$, and one point at infinity, namely $(0, 1, 0)$. This point ∞ is the point where all vertical lines meet. We denote this point by O. The set of rational points (x, y) on E

$$E(\mathbf{F}_p) = \{(x, y) \in \mathbf{F}_p \times \mathbf{F}_p : y^2 = x^3 + ax + b\} \cup \{O\}$$

is a subgroup of E. The order of $E(\mathbf{F}_p)$, denoted by $\#E(\mathbf{F}_p)$, is defined as the number of the points on E (for the arithmetic of elliptic curves and rational points on them see [8,9,10]).

A conic C is a quadratic curve of genus 0 defined by

$$C : x^2 - ky^2 = 1$$

for $k \in \mathbf{F}_p^* = \mathbf{F}_p - \{0\}$. Similarly the set of rational points (x, y) on C

$$C(\mathbf{F}_p) = \{(x, y) \in \mathbf{F}_p \times \mathbf{F}_p : x^2 - ky^2 = 1\}$$

Ahmet Tekcan is with the Uludag University, Department of Mathematics, Faculty of Science, Bursa-TURKEY, email: tekcan@uludag.edu.tr, http://matematik.uludag.edu.tr/AhmetTekcan.htm

is a subgroup of C. The connection between elliptic curves and conics is that elliptic curves are non-singular cubic curves with a rational point of genus 1, conics are quadratic curves of genus 0. We can study plane algebraic curves over the affine plane and over the projective plane. If we want to give to elliptic curves a group law, we have to use the projective plane. Similarly, we can give conics a group law as long as we stick to the affine plane. In particular, by the Chinese Remainder Theorem we get

$$C(\mathbf{Z}/N\mathbf{Z}) \cong \prod_i C(\mathbf{Z}/p^{a_i}\mathbf{Z})$$

whenever $N = \prod_i p^{a_i}$, that is, if

$$\mathbf{Z}/N\mathbf{Z} \cong \prod_i \mathbf{Z}/p^{a_i}\mathbf{Z}.$$

The group structure of $C(\mathbf{F}_p)$ is given by

$$C(\mathbf{F}_p) \cong \begin{cases} \mathbf{Z}/(p-1)\mathbf{Z} & if(\frac{k}{p}) = 1 \\ \mathbf{Z}/(p+1)\mathbf{Z} & if(\frac{k}{p}) = -1, \end{cases}$$

where $(\frac{\cdot}{p})$ denotes the Legendre symbol.

II. The Number Of Rational Points on Conics $C_{p,k} : x^2 - ky^2 = 1$ Over $\mathbf{F}_p$.

Let $\mathbf{F}_p$ be a finite field, $k \in \mathbf{F}_p^*$ and let Q_p denote the set of quadratic residues mod p. In this paper, we will determine the number of rational points on conics

$$C_{p,k} : x^2 - ky^2 = 1$$

over $\mathbf{F}_p$. Later we derive some results concerning the sums

$$\sum C_{p,k}^{[x]}(\mathbf{F}_p) \quad and \quad \sum C_{p,k}^{[y]}(\mathbf{F}_p),$$

the sum of $x-$ and $y-$coordinates of all points (x, y) on $C_{p,k}$, respectively. Then we have the following theorem.

Theorem 2.1: The order of $C_{p,k} : x^2 - ky^2 = 1$ over $\mathbf{F}_p$ is

$$\#C_{p,k}(\mathbf{F}_p) = \begin{cases} p-1 & if\ (\frac{k}{p}) = 1 \\ \\ p+1 & if\ (\frac{k}{p}) = -1. \end{cases}$$

Proof: We consider the proof in two cases according to $p \equiv 1, 3(mod\, 4)$.

Case 1: Let $p \equiv 1(mod\, 4)$. Then we have two cases:

(i) Let $(\frac{k}{p}) = 1$. If $x = 0$, then

$$ky^2 \equiv -1\ (mod\, p) \quad \Leftrightarrow \quad y^2 \equiv \frac{-1}{k}\ (mod\, p)$$
$$\Leftrightarrow \quad y \equiv \pm\sqrt{\frac{-1}{k}}\ (mod\, p).$$

Then we get $(\frac{-1}{k}) = 1$ since $(\frac{k}{p}) = 1$. Therefore $\sqrt{\frac{-1}{k}} \in \mathbf{F}_p$. So there are two points $(0, \pm\sqrt{\frac{-1}{k}})$ on $C_{p,k}$. If $y = 0$, then

$$x^2 \equiv 1 \ (mod\, p) \Leftrightarrow x \equiv \pm 1 \ (mod\, p).$$

Therefore there are two points $(\pm 1, 0)$ on $C_{p,k}$. So we have four points on $C_{p,k}$.

Let $L_p = \{2, 3, \ldots, p-2\} \subset \mathbf{F}_p$. Then there are $\frac{p-5}{2}$ points x in L_p such that $\frac{x^2-1}{k}$ is a square. Let $\frac{x^2-1}{k} = t^2$ for some $t \in \mathbf{F}_p^*$. Then

$$y^2 \equiv t^2 \ (mod\, p) \Leftrightarrow y \equiv \pm t \ (mod\, p).$$

If (x, t) is a point on $C_{p,k}$, then $(x, -t)$ is also a point on $C_{p,k}$. Therefore, when $\frac{x^2-1}{k}$ is a square for $x \in L_p$, then there are two points $(x, \pm t)$ on $C_{p,k}$. So there are

$$2\left(\frac{p-5}{2}\right) = p - 5$$

points on $C_{p,k}$ for $x \in L_p$. We know that there are four points $(0, \pm\sqrt{\frac{-1}{k}})$ and $(\pm 1, 0)$ on $C_{p,k}$. Hence there are total $p - 5 + 4 = p - 1$ rational points on $C_{p,k}$.

(ii) Let $(\frac{k}{p}) = -1$. If $x = 0$, then

$$\begin{aligned} ky^2 \equiv -1 \ (mod\, p) \quad &\Leftrightarrow \quad y^2 \equiv \frac{-1}{k} \ (mod\, p) \\ &\Leftrightarrow \quad y \equiv \pm\sqrt{\frac{-1}{k}} \ (mod\, p). \end{aligned}$$

Then we get $(\frac{-1}{k}) = -1$. Therefore $\sqrt{\frac{-1}{k}} \notin \mathbf{F}_p$. So there are no points on $C_{p,k}$. If $y = 0$, then

$$x^2 \equiv 1 \ (mod\, p) \Leftrightarrow x \equiv \pm 1 \, (mod\, p).$$

Therefore there are two points $(\pm 1, 0)$ on $C_{p,k}$. So we have two points on $C_{p,k}$. It is easily seen that there are $\frac{p-1}{2}$ points x in L_p such that $\frac{x^2-1}{k}$ is a square. Let $\frac{x^2-1}{k} = t^2$ for some $t \in \mathbf{F}_p^*$. Then

$$y^2 \equiv t^2 \, (mod\, p) \Leftrightarrow y \equiv \pm t \, (mod\, p).$$

If (x, t) is a point on $C_{p,k}$, then so is $(x, -t)$. Therefore, when $\frac{x^2-1}{k}$ is a square for $x \in L_p$, then there are two points $(x, \pm t)$ on $C_{p,k}$. So there are

$$2\left(\frac{p-1}{2}\right) = p - 1$$

points on $C_{p,k}$. We know that there are two points $(\pm 1, 0)$ on $C_{p,k}$. Hence there are total $p - 1 + 2 = p + 1$ rational points on $C_{p,k}$.

Case 2: Let $p \equiv 3 (mod\, 4)$. Then we have two cases:

(i) Let $(\frac{k}{p}) = 1$. If $x = 0$, then

$$\begin{aligned} ky^2 \equiv -1 \, (mod\, p) \quad &\Leftrightarrow \quad y^2 \equiv \frac{-1}{k} \, (mod\, p) \\ &\Leftrightarrow \quad y \equiv \pm\sqrt{\frac{-1}{k}} \, (mod\, p). \end{aligned}$$

Then we get $(\frac{-1}{k}) = -1$ since -1 is not a quadratic residue mod p. Therefore $\sqrt{\frac{-1}{k}} \notin \mathbf{F}_q$. So there are no points on $C_{p,k}$. If $y = 0$, then

$$x^2 \equiv 1 \, (mod\, p) \Leftrightarrow x \equiv \pm 1 \, (mod\, p).$$

Therefore there are two points $(\pm 1, 0)$ on $C_{p,k}$. Note that there are $\frac{p-3}{2}$ points x in L_p such that $\frac{x^2-1}{k}$ is a square. Let $\frac{x^2-1}{k} = t^2$ for some $t \in \mathbf{F}_p^*$. Then

$$y^2 \equiv t^2 \, (mod\, p) \Leftrightarrow y \equiv \pm t \, (mod\, p).$$

If (x, t) is a point on $C_{p,k}$, then so is $(x, -t)$. Therefore, when $\frac{x^2-1}{k}$ is a square for $x \in L_p$, then there are two points $(x, \pm t)$ on $C_{p,k}$. So there are

$$2\left(\frac{p-3}{2}\right) = p - 3$$

points on $C_{p,k}$ for $x \in L_p$. We know that there are two points $(\pm 1, 0)$ on $C_{p,k}$. Hence there are total $p - 3 + 2 = p - 1$ rational points on $C_{p,k}$.

(ii) Let $(\frac{k}{q}) = -1$. If $x = 0$, then

$$\begin{aligned} ky^2 \equiv -1 \, (mod\, p) \quad &\Leftrightarrow \quad y^2 \equiv \frac{-1}{k} \, (mod\, p) \\ &\Leftrightarrow \quad y \equiv \pm\sqrt{\frac{-1}{k}} \, (mod\, p). \end{aligned}$$

Then we get $(\frac{-1}{k}) = 1$ since k is not a quadratic residue mod p. Therefore $\sqrt{\frac{-1}{k}} \in \mathbf{F}_q$. So there are two points $(0, \pm\sqrt{\frac{-1}{k}})$ on $C_{p,k}$. If $y = 0$, then

$$x^2 \equiv 1 \, (mod\, p) \Leftrightarrow x \equiv \pm 1 \, (mod\, p).$$

Therefore there are two points $(\pm 1, 0)$ on $C_{p,k}$. Similarly it can be shown that there are $\frac{p-3}{2}$ points x in L_p such that $\frac{x^2-1}{k}$ is a square. Let $\frac{x^2-1}{k} = t^2$ for some $t \in \mathbf{F}_p^*$. Then

$$y^2 \equiv t^2 \, (mod\, p) \Leftrightarrow y \equiv \pm t \, (mod\, p).$$

If (x, t) is a point on $C_{p,k}$, then so is $(x, -t)$. Therefore, when $\frac{x^2-1}{k}$ is a square for $x \in L_p$, then there are two points $(x, \pm t)$ on $C_{p,k}$. So there are

$$2\left(\frac{p-3}{2}\right) = p - 3$$

points on $C_{p,k}$ for $x \in L_p$. We know that there are four points $(0, \pm\sqrt{\frac{-1}{k}})$ and $(\pm 1, 0)$ on $C_{p,k}$. Hence there are total $p - 3 + 4 = p + 1$ rational points on $C_{p,k}$. ■

Example 2.1: Let $p = 7$. Then $Q_7 = \{1, 2, 4\}$. The rational points on conics $C_{7,k} : x^2 - ky^2 = 1$ over $\mathbf{F}_7$ are

$$\begin{aligned}
C_{7,1}(\mathbf{F}_7) &= \left\{ \begin{array}{c} (1,0), (3,1), (3,6), (4,1), \\ (4,6), (6,0) \end{array} \right\} \\
C_{7,2}(\mathbf{F}_7) &= \left\{ \begin{array}{c} (1,0), (3,2), (3,5), (4,2), \\ (4,5), (6,0) \end{array} \right\} \\
C_{7,3}(\mathbf{F}_7) &= \left\{ \begin{array}{c} (0,3), (0,4), (1,0), (2,1), \\ (2,6), (5,1), (5,6), (6,0) \end{array} \right\} \\
C_{7,4}(\mathbf{F}_7) &= \left\{ \begin{array}{c} (1,0), (3,3), (3,4), (4,3), \\ (4,4), (6,0) \end{array} \right\} \\
C_{7,5}(\mathbf{F}_7) &= \left\{ \begin{array}{c} (0,2), (0,5), (1,0), (2,3), \\ (2,4), (5,3), (5,4), (6,0) \end{array} \right\} \\
C_{7,6}(\mathbf{F}_7) &= \left\{ \begin{array}{c} (0,1), (0,6), (1,0), (2,2), \\ (2,5), (5,2), (5,5), (6,0) \end{array} \right\}.
\end{aligned}$$

Example 2.2: Let $p = 13$. Then $Q_{13} = \{1, 3, 4, 9, 10, 12\}$. The rational points on conics $C_{13,k} : x^2 - ky^2 = 1$ over $\mathbf{F}_{13}$ are

$$C_{13,1}(\mathbf{F}_{13}) = \left\{ \begin{array}{c} (0,5),(0,8),(1,0),(2,4), \\ (2,9),(6,3),(6,10),(7,3), \\ (7,10),(11,4),(11,9),(12,0) \end{array} \right\}$$

$$C_{13,2}(\mathbf{F}_{13}) = \left\{ \begin{array}{c} (1,0),(3,2),(3,11),(4,1), \\ (4,12),(5,5),(5,8),(8,5), \\ (8,8),(9,1),(9,12),(10,2), \\ (10,11),(12,0) \end{array} \right\}$$

$$C_{13,3}(\mathbf{F}_{13}) = \left\{ \begin{array}{c} (0,2),(0,11),(1,0),(2,1), \\ (2,12),(6,4),(6,9),(7,4), \\ (7,9),(11,1),(11,12),(12,0) \end{array} \right\}$$

$$C_{13,4}(\mathbf{F}_{13}) = \left\{ \begin{array}{c} (0,4),(0,9),(1,0),(2,2), \\ (2,11),(6,5),(6,8),(7,5), \\ (7,8),(11,2),(11,11),(12,0) \end{array} \right\}$$

$$C_{13,5}(\mathbf{F}_{13}) = \left\{ \begin{array}{c} (1,0),(3,5),(3,8),(4,4), \\ (4,9),(5,6),(5,7),(8,6), \\ (8,7),(9,4),(9,9),(10,5), \\ (10,8),(12,0) \end{array} \right\}$$

$$C_{13,6}(\mathbf{F}_{13}) = \left\{ \begin{array}{c} (1,0),(3,6),(3,7),(4,3), \\ (4,10),(5,2),(5,11),(8,2), \\ (8,11),(9,3),(9,10), \\ (10,6),(10,7),(12,0) \end{array} \right\}$$

$$C_{13,7}(\mathbf{F}_{13}) = \left\{ \begin{array}{c} (1,0),(3,4),(3,9),(4,2), \\ (4,11),(5,3),(5,10),(8,3), \\ (8,10),(9,2),(9,11), \\ (10,4),(10,9),(12,0) \end{array} \right\}$$

$$C_{13,8}(\mathbf{F}_{13}) = \left\{ \begin{array}{c} (1,0),(3,1),(3,12),(4,6), \\ (4,7),(5,4),(5,9),(8,4), \\ (8,9),(9,6),(9,7),(10,1), \\ (10,12),(12,0) \end{array} \right\}$$

$$C_{13,9}(\mathbf{F}_{13}) = \left\{ \begin{array}{c} (0,6),(0,7),(1,0),(2,3), \\ (2,10),(6,1),(6,12),(7,1), \\ (7,12),(11,3),(11,10), \\ (12,0) \end{array} \right\}$$

$$C_{13,10}(\mathbf{F}_{13}) = \left\{ \begin{array}{c} (0,3),(0,10),(1,0),(2,5), \\ (2,8),(6,6),(6,7), \\ (7,6),(7,7),(11,5), \\ (11,8),(12,0) \end{array} \right\}$$

$$C_{13,11}(\mathbf{F}_{13}) = \left\{ \begin{array}{c} (1,0),(3,3),(3,10),(4,5), \\ (4,8),(5,1),(5,12),(8,1), \\ (8,12),(9,5),(9,8), \\ (10,3),(10,10),(12,0) \end{array} \right\}$$

$$C_{13,12}(\mathbf{F}_{13}) = \left\{ \begin{array}{c} (0,1),(0,12),(1,0),(2,6), \\ (2,7),(6,2),(6,11), \\ (7,2),(7,11),(11,6), \\ (11,7),(12,0) \end{array} \right\}.$$

Let $[x]$ and $[y]$ denote the $x-$ and $y-$ coordinates of (x,y) on $C_{p,k}$, respectively, and let $\sum C_{p,k}^{[x]}(\mathbf{F}_p)$ and $\sum C_{p,k}^{[y]}(\mathbf{F}_p)$ denote the sum of $x-$and $y-$coordinates of all rational points (x,y) on $C_{p,k}$, respectively. Then we have the following two results.

Theorem 2.2: The sum of $[x]$ on $C_{p,k}$ is

$$\sum C_{p,k}^{[x]}(\mathbf{F}_p) = \begin{cases} \frac{p^2-3p}{2} & if \begin{cases} p \equiv 1\,(mod\,4) \\ and\ (\frac{k}{p}) = 1 \end{cases} \\ \frac{p^2+p}{2} & if \begin{cases} p \equiv 1\,(mod\,4) \\ and\ (\frac{k}{p}) = -1 \end{cases} \\ \frac{p^2-p}{2} & if p \equiv 3\,(mod\,4). \end{cases}$$

Proof: Let $p \equiv 1\,(mod\,4)$ and let $(\frac{k}{p}) = 1$. We proved in Theorem 2.1 that there are $\frac{p-5}{2}$ points x in L_p such that $\frac{x^2-1}{k}$ is a square. If x is a point such that $\frac{x^2-1}{k}$ is a square, then $-x = p - x$ is also a point such that $\frac{x^2-1}{k}$ is a square. Therefore, the total of $x-$coordinates of these points is p. There are $\frac{p-5}{2}$ points in L_p such that $\frac{x^2-1}{k}$ is a square. So the sum of $x-$coordinates of all points (x,y) on $C_{p,k}$ is $p(\frac{p-5}{2}) = \frac{p^2-5p}{2}$. When $y = 0$, we have two points $(1,0)$ and $(p-1,0)$ on $C_{p,k}$, and the sum of $x-$coordinates of these two points is p. Hence the sum of $x-$coordinates of all points (x,y) on $C_{p,k}$ is

$$\frac{p^2-5p}{2} + p = \frac{p^2-3p}{2}.$$

Let $p \equiv 1\,(mod\,4)$ and $(\frac{k}{p}) = -1$. Then there are $\frac{p-1}{2}$ points x such that $\frac{x^2-1}{k}$ is a square. If x is a point such that $\frac{x^2-1}{k}$ is a square, then $-x = p - x$ is also a point such that $\frac{x^2-1}{k}$ is a square. Therefore, the total of $x-$coordinates of these points is p. There are $\frac{p-1}{2}$ points in L_p such that $\frac{x^2-1}{k}$ is a square. So the sum of $x-$coordinates of all points (x,y) on $C_{p,k}$ is $p(\frac{p-1}{2}) = \frac{p^2-p}{2}$. When $y = 0$, we have two points $(1,0)$ and $(p-1,0)$ on $C_{p,k}$, and the sum of $x-$coordinates of these two points is p. Hence the sum of $x-$coordinates of all points (x,y) on $C_{p,k}$ is

$$\frac{p^2-p}{2} + p = \frac{p^2+p}{2}.$$

Let $p \equiv 3\,(mod\,4)$ and $(\frac{k}{p}) = 1$. Then there are $\frac{p-3}{2}$ points x in L_p such that $\frac{x^2-1}{k}$ is a square. If x is a point such that $\frac{x^2-1}{k}$ is a square, then $-x = p - x$ is also a point such that $\frac{x^2-1}{k}$ is a square. Therefore, the total of $x-$coordinates of these points is p. There are $\frac{p-3}{2}$ points in L_p such that $\frac{x^2-1}{k}$ is a square. So the sum of $x-$coordinates of all points (x,y) on $C_{p,k}$ is $p(\frac{p-3}{2}) = \frac{p^2-3p}{2}$. When $y = 0$, we have two points $(1,0)$ and $(p-1,0)$ on $C_{p,k}$, and the sum of $x-$coordinates of these two points is p. Hence the sum of $x-$coordinates of all points (x,y) on $C_{p,k}$ is

$$\frac{p^2-3p}{2} + p = \frac{p^2-p}{2}.$$

Let $p \equiv 3\,(mod\,4)$ and $(\frac{k}{p}) = -1$. Then there are $\frac{p-3}{2}$ points x such that $\frac{x^2-1}{k}$ is a square. If x is a point such that $\frac{x^2-1}{k}$ is a square, then $-x = p - x$ is also a point such that $\frac{x^2-1}{k}$ is a square. Therefore, the total of $x-$coordinates of these points is p. So the sum of $x-$coordinates of all points (x,y) on $C_{p,k}$ is $p(\frac{p-3}{2}) = \frac{p^2-3p}{2}$. When $y = 0$, we have two points $(1,0)$

and $(p-1,0)$ on $C_{p,k}$, and the sum of $x-$coordinates of them is p. Hence the sum of $[x]$ of all (x,y)on $C_{p,k}$ is

$$\frac{p^2-3p}{2}+p=\frac{p^2-p}{2}$$

as we claimed. ■

Theorem 2.3: The sum of $[y]$ on $C_{p,k}$ is

$$\sum C^{[y]}_{p,k}(\mathbf{F}_p)=\begin{cases}\frac{p^2-3p}{2} & if(\frac{k}{p})=1\\ \\ \frac{p^2-p}{2} & if(\frac{k}{p})=-1.\end{cases}$$

Proof: Let $p\equiv 1\,(mod\,4)$ and $(\frac{k}{p})=1$. Then there are $\frac{p-5}{2}$ points x in L_p such that $\frac{x^2-1}{k}$ is a square. Let $\frac{x^2-1}{k}=t^2$ for some $t\in\mathbf{F}_p^*$. Then

$$y^2\equiv t^2\,(mod\,p)\Leftrightarrow y^2\equiv\pm t\,(mod\,p).$$

Therefore, when $\frac{x^2-1}{k}$ is a square, we have two points (x,t) and $(x,p-t)$. Therefore, the total of $y-$coordinates of these points is p. There are $\frac{p-5}{2}$ points in L_p such that $\frac{x^2-1}{k}$ is a square. So the sum of $y-$coordinates of all points (x,y) on $C_{p,k}$ is $p(\frac{p-5}{2})=\frac{p^2-5p}{2}$. When $x=0$, we have two points $(0,\pm\sqrt{\frac{-1}{k}})$ on $C_{p,k}$, and the sum of $y-$coordinates of these two points is p. So the sum of $y-$coordinates of all points (x,y) on $C_{p,k}$ is

$$\frac{p^2-5p}{2}+p=\frac{p^2-3p}{2}.$$

Let $p\equiv 1\,(mod\,4)$ and $(\frac{k}{p})=-1$. Then there are $\frac{p-1}{2}$ points x in L_p such that $\frac{x^2-1}{k}$ is a square. Let $\frac{x^2-1}{k}=t^2$ for some $t\in\mathbf{F}_p^*$. Then

$$y^2\equiv t^2\,(mod\,q)\Leftrightarrow y^2\equiv\pm t\,(mod\,p).$$

Therefore, when $\frac{x^2-1}{k}$ is a square, we have two points (x,t) and $(x,p-t)$. Therefore, the total of $y-$coordinates of these points is p. There are $\frac{p-1}{2}$ points in L_p such that $\frac{x^2-1}{k}$ is a square. So the sum of $y-$coordinates of all points (x,y) on $C_{p,k}$ is $p(\frac{p-1}{2})=\frac{p^2-p}{2}$. When $x=0$, we have no points on $C_{p,k}$. So the sum of $y-$coordinates of all points (x,y) on $C_{p,k}$ is

$$\frac{p^2-p}{2}.$$

Let $p\equiv 3\,(mod\,4)$ and $(\frac{k}{p})=1$. Then there are $\frac{p-3}{2}$ points x in L_p such that $\frac{x^2-1}{k}$ is a square. Let $\frac{x^2-1}{k}=t^2$ for some $t\in\mathbf{F}_p^*$. Then

$$y^2\equiv t^2\,(mod\,q)\Leftrightarrow y^2\equiv\pm t\,(mod\,p).$$

Therefore, when $\frac{x^2-1}{k}$ is a square, we have two points (x,t) and $(x,p-t)$. Therefore, the total of $y-$coordinates of these points is p. There are $\frac{p-3}{2}$ points in L_p such that $\frac{x^2-1}{k}$ is a square. So the sum of $y-$coordinates of all points (x,y) on $C_{p,k}$ is $p(\frac{p-3}{2})=\frac{p^2-3p}{2}$. When $x=0$, we have no points on $C_{p,k}$. So the sum of $y-$coordinates of all points (x,y) on $C_{p,k}$ is

$$\frac{p^2-3p}{2}.$$

Let $p\equiv 3\,(mod\,4)$ and $(\frac{k}{p})=-1$. Then there are $\frac{p-3}{2}$ points x in L_p such that $\frac{x^2-1}{k}$ is a square. Let $\frac{x^2-1}{k}=t^2$ for some $t\in\mathbf{F}_p^*$. Then

$$y^2\equiv t^2\,(mod\,q)\Leftrightarrow y^2\equiv\pm t\,(mod\,p).$$

Therefore, when $\frac{x^2-1}{k}$ is a square, we have two points (x,t) and $(x,p-t)$. Therefore, the total of $y-$coordinates of these points is p. There are $\frac{p-3}{2}$ points in L_p such that $\frac{x^2-1}{k}$ is a square. So the sum of $y-$coordinates of all points (x,y) on $C_{p,k}$ is $p(\frac{p-3}{2})=\frac{p^2-3p}{2}$. When $x=0$, we have two points $(0,\pm\sqrt{\frac{-1}{k}})$ on $C_{p,k}$, and the sum of $y-$coordinates of these two points is p. So the sum of $y-$coordinates of all points (x,y) on $C_{p,k}$ is

$$\frac{p^2-3p}{2}+p=\frac{p^2-p}{2}$$

as we predicted. ■

Theorem 2.4: Let $\mathbf{C}_{p,k}$ denote the set of the family of all conics $C_{p,k}$ over $\mathbf{F}_p$. Then

$$\sum\#\mathbf{C}_{p,k}(\mathbf{F}_p)=p^2-p.$$

Proof: We know from Theorem 2.1 that the order of $C_{p,k}$ over $\mathbf{F}_p$ is $p-1$ if $(\frac{k}{p})=1$ and is $p+1$ if $(\frac{k}{p})=-1$. On the other hand there are $p-1$ conics $C_{p,k}$ since $k\in\mathbf{F}_p^*$, and half of them of order $p-1$ and half of them of order $p+1$ since the order of Q_p is $\frac{p-1}{2}$. Therefore the total number of rational points on all conics in $\mathbf{C}_{p,k}$ is

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

■

REFERENCES

[1] A.O.L. Atkin and F. Moralin. *Elliptic Curves and Primality Proving.* Math. Comp. **61**(203)(1993), 29–68.
[2] S. Goldwasser and J. Kilian. *Almost all Primes Can be Quickly Certified, In Proc. 18th STOC (Berkeley, May 28-30, 1986).* ACM, New York, (1986), 316–329.
[3] N. Koblitz. *Elliptic Curve Cryptosystems.* Math. Comp. **48**(177)(1987), 203–209.
[4] H.W.Jr. Lenstra. *Factoring Integers with Elliptic Curves.* Annals of Maths. **126**(3)(1987), 649–673.
[5] V.S. Miller. *Use of Elliptic Curves in Cryptography, in Advances in Cryptology–CRYPTO'85*. Lect. Notes in Comp. Sci. **218**, Springer-Verlag, Berlin (1986), 417–426.
[6] R.A. Mollin. *An Introduction to Cryptography.* Chapman&Hall/CRC, 2001.
[7] L.J. Mordell. *On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degrees.* Proc. Cambridge Philos. Soc. **21**(1922), 179–192.
[8] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1986.
[9] J.H. Silverman and J. Tate. *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics, Springer, 1992.
[10] L.C. Washington. *Elliptic Curves, Number Theory and Cryptography.* Chapman & Hall/CRC, Boca London, New York, Washington DC, 2003.
[11] A. Wiles. *Modular Elliptic Curves and Fermat's Last Theorem.* Annals of Maths. **141**(3)(1995), 443–551.