The Number of Rational Points on Singular Curves $y^2 = x(x - a)^2$ over Finite Fields $\mathbb{F}_p$

Ahmet Tekcan

Abstract—Let $p \geq 5$ be a prime number and let $\mathbb{F}_p$ be a finite field. In this work, we determine the number of rational points on singular curves $E_a : y^2 = x(x - a)^2$ over $\mathbb{F}_p$ for some specific values of $a$.

Keywords—Singular curve, elliptic curve, rational points.

I. INTRODUCTION

Mordell began his famous paper [9] 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 [4], [7], [8], for factoring large integers [6] and for primality proving [1], [3]. The mathematical theory of elliptic curves was also crucial in the proof of Fermat’s Last Theorem [17].

Let $q$ be a positive integer, $\mathbb{F}_q$ be a finite field and let $\mathbb{F}_q$ denote the algebraic closure of $\mathbb{F}_q$ with $\text{char}(\mathbb{F}_q) \neq 2, 3$. An elliptic curve $E$ over $\mathbb{F}_q$ is defined by an equation

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

where $a, b \in \mathbb{F}_q$ and $b^2(a^2 - 4b) \neq 0$. The discriminant of $E$ is

$$\Delta = 16b^2(a^2 - 4b).$$

If $\Delta = 0$, then $E$ is not an elliptic curve is a singular curve. We can view an elliptic curve $E$ as a curve in projective plane $\mathbb{P}^2$, with a homogenous equation

$$y^2z = x^3 + ax^2z + bxz^3,$$

and one point at infinity, namely $(0, 1, 0)$. This point is the point where all vertical lines meet. We denote this point by $O$. Let $E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : y^2 = x^3 + ax^2 + bx\} \cup \{O\}$ denote the set of rational points $(x, y)$ on $E$. Then it is a subgroup of $E$. The order of $E(\mathbb{F}_q)$, denoted by $N_q = \#E(\mathbb{F}_q)$, is defined as the number of the rational points on $E$ and is given by

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left( \frac{x^3 + ax^2 + bx}{\mathbb{F}_q} \right),$$

where $\left( \frac{x^3 + ax^2 + bx}{\mathbb{F}_q} \right)$ denotes the Legendre symbol (for further details on elliptic curves see [10], [11], [16]).

II. THE NUMBER OF RATIONAL POINTS ON SINGULAR CURVES $y^2 = x(x - a)^2$ OVER $\mathbb{F}_p$.

In [2], [12], [14], we considered some specific elliptic curves (including the number of rational points on them) over finite fields. In this section we will determine the number of rational points on singular curves

$$E_a : y^2 = x(x - a)^2$$

over finite fields $\mathbb{F}_p$ for primes $p \geq 5$. Let

$$E_a(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = x(x - a)^2\} \cup O.$$

Before we consider our problem we give some notations which we need later.

Lemma 2.1: [5] Let $p$ be an odd prime and let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree $\geq 1$. Then the number $N_p(f)$ of solutions $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ of the congruence $y^2 \equiv f(x) (mod p)$ is

$$N_p(f) = p + S_p(f),$$

where

$$S_p(f) = \sum_{x=0}^{p-1} \left( \frac{f(x)}{p} \right).$$

Also it is showed in [16] that for the polynomial $f(x) = (x - r)^2(x - s)$ of degree 3 for some $r, s \in \mathbb{F}_p$,

$$\sum_{x=0}^{p-1} \left( \frac{f(x)}{\mathbb{F}_p} \right) = -(r - s).$$

Note that the $f(x) = x(x - a)^2$ is a polynomial of degree 3. So by considering the point 0, we can rewrite the formula (2) as

$$\#E_a(\mathbb{F}_p) = p + 1 + \sum_{x=0}^{p-1} \left( \frac{x(x - a)^2}{p} \right)$$

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

by (3) and (4). Therefore if $\left( \frac{a}{p} \right) = 1$, then $\#E_a(\mathbb{F}_p) = p$ and if $\left( \frac{a}{p} \right) = -1$, then $\#E_a(\mathbb{F}_p) = p + 2$. Therefore the order of $E_a$ over $\mathbb{F}_p$ depends on whether $a$ is a quadratic residue or not.

Now we can give the following two theorems which I proved them in [13] and [15], respectively.

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.
Theorem 2.1: Let \( F_p \) be a finite field. Then
\[
\begin{align*}
\frac{1}{p} &= 1 & \text{for every primes } p \geq 5 \\
\frac{2}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,7(8) \\ -1 & \text{if } p \equiv 3,5(8) \end{cases} \\
\frac{3}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,11(12) \\ -1 & \text{if } p \equiv 5,7(12) \end{cases} \\
\frac{4}{p} &= 1 \text{ for every primes } p \geq 5 \\
\frac{5}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,9(10) \\ -1 & \text{if } p \equiv 3,7(10) \end{cases} \\
\frac{6}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,5,19,23(24) \\ -1 & \text{if } p \equiv 7,11,13,17(24) \end{cases} \\
\frac{7}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,3,9,19,25,27(28) \\ -1 & \text{if } p \equiv 5,11,13,15,17,23(28) \end{cases} \\
\frac{8}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,7,17,23(24) \\ -1 & \text{if } p \equiv 5,11,13,19(24) \end{cases} \\
\frac{9}{p} &= 1 \text{ for every primes } p \geq 11 \\
\frac{10}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,3,9,13,27,31,37,39(40) \\ -1 & \text{if } p \equiv 7,11,17,19,21,23,29,33,37,39(40) \end{cases}
\end{align*}
\]

Theorem 2.2: Let \( F_p \) be a finite field. Then
\[
\begin{align*}
\frac{-1}{p} &= \begin{cases} 1 & \text{if } p \equiv 1(4) \\ -1 & \text{if } p \equiv 3(4) \end{cases} \\
\frac{-2}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,3(8) \\ -1 & \text{if } p \equiv 5,7(8) \end{cases} \\
\frac{-3}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,7(12) \\ -1 & \text{if } p \equiv 5,11(12) \end{cases} \\
\frac{-4}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,5(12) \\ -1 & \text{if } p \equiv 7,11(12) \end{cases} \\
\frac{-5}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,3,7,9(20) \\ -1 & \text{if } p \equiv 11,13,17,19(20) \end{cases} \\
\frac{-6}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,5,7,11,25,29,31,35(48) \\ -1 & \text{if } p \equiv 13,17,19,23,37,41,43,47(48) \end{cases} \\
\frac{-7}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,9,11,15,23,25(28) \\ -1 & \text{if } p \equiv 3,5,13,17,19,27(28) \end{cases} \\
\frac{-8}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,11,17,19,25,35,41,43(48) \\ -1 & \text{if } p \equiv 5,7,13,23,29,31,37,47(48) \end{cases} \\
\frac{-9}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,5,13,17(24) \\ -1 & \text{if } p \equiv 7,11,19,23(24) \end{cases} \\
\frac{-10}{p} &= \begin{cases} 1 & \text{if } p \equiv 1,7,9,11,13,19,23,37(40) \\ -1 & \text{if } p \equiv 3,17,21,27,29,31,33,39(40) \end{cases}
\end{align*}
\]

Now we can consider our main problem.

Theorem 2.3: Let \( E_a \) be the singular curve defined in (1). Then
\[
\begin{align*}
\#E_1(F_p) &= p \text{ for every primes } p \geq 5 \\
\#E_2(F_p) &= \begin{cases} p & \text{if } p \equiv 1,7(8) \\ p+2 & \text{if } p \equiv 3,5(8) \end{cases} \\
\#E_3(F_p) &= \begin{cases} p & \text{if } p \equiv 1,11(12) \\ p+2 & \text{if } p \equiv 5,7(12) \end{cases} \\
\#E_4(F_p) &= p \text{ for every primes } p \geq 5 \\
\#E_5(F_p) &= \begin{cases} p & \text{if } p \equiv 1,9(10) \\ p+2 & \text{if } p \equiv 3,7(10) \end{cases} \\
\#E_6(F_p) &= \begin{cases} p & \text{if } p \equiv 1,5,19,23(24) \\ p+2 & \text{if } p \equiv 7,11,13,17(24) \end{cases} \\
\#E_7(F_p) &= \begin{cases} p & \text{if } p \equiv 1,3,9,19,25,27(28) \\ p+2 & \text{if } p \equiv 5,11,13,15,17,23(28) \end{cases} \\
\#E_8(F_p) &= \begin{cases} p & \text{if } p \equiv 1,7,17,23(24) \\ p+2 & \text{if } p \equiv 5,11,13,19(24) \end{cases} \\
\#E_9(F_p) &= p \text{ for every primes } p \geq 11 \\
\#E_{10}(F_p) &= \begin{cases} p & \text{if } p \equiv 1,3,9,13,27,31,37,39(40) \\ p+2 & \text{if } p \equiv 7,11,17,19,21,23,29,33,37,39(40) \end{cases}
\end{align*}
\]
Proof: Applying Theorems 2.1 and 2.2 the result is clear.

Now we consider the sum of $x$- and $y$-coordinates of all rational points $(x, y)$ on $E_a$ over $F_p$. Let $|x|$ and $|y|$ denote the $x$- and $y$-coordinates of the points $(x, y)$ on $E_a$, respectively. Then we have the following results.

**Theorem 2.4:** The sum of $|x|$ on $E_a$ is

$$
\sum_{x \in E_a} |x| = \left\{ \begin{array}{ll} 
\frac{p^3 - p - 12a}{12} & i f \left( \frac{a}{p} \right) = 1 \\
\frac{p^3 - p + 12a}{12} & i f \left( \frac{a}{p} \right) = -1.
\end{array} \right.
$$

**Proof:** Let $U_p = \{1, 2, \cdots, p-1\}$ be the set of units in $F_p$. Then taking squares of elements in $U_p$, we would obtain the set of quadratic residues $Q_p = \{1^2, 2^2, \cdots, (\frac{p-1}{2})^2\}$. Then the sum of all elements in $Q_p$ is

$$
\sum_{x \in Q_p} x = \frac{p^3 - p}{24}.
$$

Now let $\left( \frac{a}{p} \right) = 1$. Then $a$ is a quadratic residue. But for this values of $a$, there is one rational point $(a, 0)$ on $E_a$. Let $H = Q_p \setminus \{a\}$. Then

$$
\sum_{x \in H} x = \left( \sum_{x \in Q_p} x \right) - a = \frac{p^3 - p}{24} - a = \frac{p^3 - p - 24a}{24}.
$$

We know that every element $x$ of $H$ makes $x(x-a)^2$ a square. Let $x(x-a)^2 \equiv t^2 \pmod{p}$. Then $y^2 \equiv t^2 \pmod{p}$. So there are two rational points $(x, t)$ and $(x, p-t)$ on $E_a$. The sum of $x$-coordinates of these two points is $2x$, that is, for every $x \in H$, the sum of $x$-coordinates of $(x, t)$ and $(x, p-t)$ is $2x$. So the sum of $x$-coordinates of all points on $E_a$ is

$$
2 \sum_{x \in H} x.
$$

Further we said above that the point $(a, 0)$ is also on $E_a$. Consequently

$$
\sum_{x \in E_a} |x| = 2 \left( \sum_{x \in H} x \right) + a = \frac{p^3 - p - 12a}{12}.
$$

Let $\left( \frac{a}{p} \right) = -1$. Then $a$ is not a quadratic residue. But every element $x$ of $Q_p$ makes $x(x-a)^2$ a square. So there are two rational points on $E_a$ and hence the sum of $x$-coordinates of these two points is $2x$. Further $(a, 0)$ is also a rational point on $E_a$. Consequently

$$
\sum_{x \in E_a} |x| = 2 \left( \sum_{x \in Q_p} x \right) + a = \frac{p^3 - p + 12a}{12}.
$$

**Theorem 2.5:** The sum of $|y|$ on $E_a$ is

$$
\sum_{y \in E_a} |y| = \left\{ \begin{array}{ll}
\frac{p^2 - 3p}{2} & i f \left( \frac{a}{p} \right) = 1 \\
\frac{p^2 + p}{2} & i f \left( \frac{a}{p} \right) = -1.
\end{array} \right.
$$

**Proof:** Let $\left( \frac{a}{p} \right) = 1$. Then $a$ is a quadratic residue but again for this value of $a$, there is one rational point $(a, 0)$ on $E_a$. Also every element $x$ of $Q_p$ makes $x(x-a)^2$ a square. Let $x(x-a)^2 \equiv t^2 \pmod{p}$. Then $y^2 \equiv t^2 \pmod{p}$. So there are two points $(x, t)$ and $(x, p-t)$ on $E_a$. The sum of $y$-coordinates of these two points is $p$. We know that there are $\frac{p^2 - 3}{2} - 1$ points $x$ such that $x(x-a)^2$ is a square. So the sum of $y$-coordinates of all points $(x, y)$ on $E_a$ is

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

Now let $\left( \frac{a}{p} \right) = -1$. Then $a$ is not a quadratic residue. But every element $x$ of $Q_p$ makes $x(x-a)^2$ a square. Let $x(x-a)^2 \equiv t^2 \pmod{p}$. Then $y^2 \equiv t^2 \pmod{p} \iff y \equiv \pm t \pmod{p}$.

So there are two points $(x, t)$ and $(x, p-t)$ on $E_a$. The sum of $y$-coordinates of these two points is $p$. We know that there are $\frac{p^2 + p}{2}$ points $x$ such that $x(x-a)^2$ is a square. So the sum of $y$-coordinates of all points $(x, y)$ on $E_a$ is

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

**REFERENCES**


[14] A. Tekcan. The Elliptic Curves $y^2 = x(x-1)(x-\lambda)$. Accepted for publication to Ars Combinatoria.

