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].

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

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

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

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

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

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

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

Now we can consider our main problem.

Theorem 2.2: Let $F_p$ be a finite field. Then
\[
\#E_1(F_p) = \begin{cases} 
p & \text{if } p \equiv 1, 7(8) \\
p + 2 & \text{if } p \equiv 3, 5(8) 
\end{cases}
\]
\[
\#E_2(F_p) = \begin{cases} 
p & \text{if } p \equiv 1, 7(8) \\
p + 2 & \text{if } p \equiv 3, 5(8) 
\end{cases}
\]
\[
\#E_3(F_p) = \begin{cases} 
p & \text{if } p \equiv 1, 11(12) \\
p + 2 & \text{if } p \equiv 5, 7(12) 
\end{cases}
\]
\[
\#E_4(F_p) = \begin{cases} 
p & \text{for every primes } p \geq 5 \\
p + 2 & \text{if } p \equiv 1, 9(10) \\
p + 2 & \text{if } p \equiv 3, 7(10) 
\end{cases}
\]
\[
\#E_5(F_p) = \begin{cases} 
p & \text{if } p \equiv 1, 9(10) \\
p + 2 & \text{if } p \equiv 3, 7(10) 
\end{cases}
\]
\[
\#E_6(F_p) = \begin{cases} 
p & \text{if } p \equiv 1, 5, 19, 23(24) \\
p + 2 & \text{if } p \equiv 7, 11, 13, 17(24) 
\end{cases}
\]
\[
\#E_7(F_p) = \begin{cases} 
p & \text{if } p \equiv 1, 3, 9, 19, 25, 27(28) \\
p + 2 & \text{if } p \equiv 5, 11, 13, 15, 17, 23(28) 
\end{cases}
\]
\[
\#E_8(F_p) = \begin{cases} 
p & \text{if } p \equiv 1, 7, 17, 23(24) \\
p + 2 & \text{if } p \equiv 5, 11, 13, 19(24) 
\end{cases}
\]
\[
\#E_9(F_p) = \begin{cases} 
p & \text{for every primes } p \geq 11 \\
p + 2 & \text{if } p \equiv 1, 3, 9, 13, 27, 31, 37, 39(40) \\
p + 2 & \text{if } p \equiv 7, 11, 17, 19, 21, 23, 29, 33, 37(40) 
\end{cases}
\]

Theorem 2.3: Let $E_a$ be the singular curve defined in (1). Then
\[
\#E_{10}(F_p) = \begin{cases} 
p & \text{if } p \equiv 1, 3, 9, 13, 27, 31, 37, 39(40) \\
p + 2 & \text{if } p \equiv 7, 11, 17, 19, 21, 23, 29, 33, 37(40) 
\end{cases}
\]
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

$$\sum_{[x]} E_a(F_p) = \begin{cases} \frac{p^3 - p - 12a}{12} & \text{if } (\frac{a}{p}) = 1 \\ \frac{p^3 - p + 12a}{12} & \text{if } (\frac{a}{p}) = -1. \end{cases}$$

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

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

Let $(\frac{a}{p}) = 1$. Then $a$ is a quadratic residue. For this values of $a$, there is one rational point $(a,0)$ on $E_a$. Let $H = Q_p - \{a\}$. 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 $x(x-a)^2 \equiv t^2 (mod p)$. Then $y^2 \equiv t^2 (mod p)$. So there are two rational points $(x,t)$ and $(x,p-t)$ on $E_a$. The sum of $y$-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

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

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

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

Let $(\frac{a}{p}) = -1$. 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

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

Theorem 2.5: The sum of $[y]$ on $E_a$ is

$$\sum_{[y]} E_a(F_p) = \begin{cases} \frac{p^2 - 3p}{2} & \text{if } (\frac{a}{p}) = 1 \\ \frac{p^2 + p}{2} & \text{if } (\frac{a}{p}) = -1. \end{cases}$$

Proof: Let $(\frac{a}{p}) = 1$. 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 $x(x-a)^2 \equiv t^2 (mod p)$. Then $y^2 \equiv t^2 (mod p)$. The result is clear.

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 $p^2 - 1 - \frac{p-3}{2}$ 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

$$\sum_{y \in E_a(F_p)} y = \frac{p(p-1)^2}{2}.$$ 

Now let $(\frac{a}{p}) = -1$. Then $a$ is not a quadratic residue. But every element $x$ of $Q_p$ makes $x(x-a)^2$ a square. Let $x(x-a)^2 \equiv t^2 (mod p)$. Then $y^2 \equiv t^2 (mod p)$. The result is clear.

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 $\frac{p^2 - 3p}{2}$ points $x$ in $Q_p$ such that $x(x-a)^2$ is a square. So the sum of $y$-coordinates of all points $(x,y)$ on $E_a$ is

$$\sum_{y \in E_a(F_p)} y = \frac{p(p-1)}{2}.$$ 

REFERENCES


International Scholarly and Scientific Research & Innovation 3(11) 2009 981
[14] A. Tekcan. The Elliptic Curves $y^2 = x(x - 1)(x - \lambda)$. Accepted for publication in Ars Combinatoria.

