

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

Ahmet Tekcan

Abstract—Let $p \geq 5$ be a prime number and let \mathbf{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 \mathbf{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, \mathbf{F}_q be a finite field and let $\overline{\mathbf{F}}_q$ denote the algebraic closure of \mathbf{F}_q with $\text{char}(\overline{\mathbf{F}}_q) \neq 2, 3$. An elliptic curve E over \mathbf{F}_q is defined by an equation

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

where $a, b \in \mathbf{F}_q$ 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 \mathbf{P}^2 , with a homogeneous equation

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

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

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

denote the set of rational points (x, y) on E . Then it is a subgroup of E . The order of $E(\mathbf{F}_q)$, denoted by $N_q = \#E(\mathbf{F}_q)$, is defined as the number of the rational points on E and is given by

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

where $\left(\frac{\cdot}{\mathbf{F}_q}\right)$ denotes the Legendre symbol (for further details on elliptic curves see [10], [11], [16]).

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.

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

$$E_a : y^2 = x(x - a)^2 \tag{1}$$

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

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

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

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

$$N_p(f) = p + S_p(f), \tag{2}$$

where

$$S_p(f) = \sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right). \tag{3}$$

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

$$\sum_{x=0}^{p-1} \left(\frac{f(x)}{\mathbf{F}_p} \right) = -\left(\frac{r - s}{\mathbf{F}_p} \right). \tag{4}$$

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

$$\begin{aligned} \#E_a(\mathbf{F}_p) &= p + 1 + \sum_{x=0}^{p-1} \left(\frac{x(x - a)^2}{p} \right) \\ &= p + 1 - \left(\frac{a}{p} \right) \end{aligned} \tag{5}$$

by (3) and (4). Therefore if $\left(\frac{a}{p}\right) = 1$, then $\#E_a(\mathbf{F}_p) = p$ and if $\left(\frac{a}{p}\right) = -1$, then $\#E_a(\mathbf{F}_p) = p + 2$. Therefore the order of E_a over \mathbf{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 \mathbf{F}_p be a finite field. Then

$$\left(\frac{1}{p}\right) = 1 \text{ for every primes } p \geq 5$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7(8) \\ -1 & \text{if } p \equiv 3, 5(8) \end{cases}$$

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 11(12) \\ -1 & \text{if } p \equiv 5, 7(12) \end{cases}$$

$$\left(\frac{4}{p}\right) = 1 \text{ for every primes } p \geq 5$$

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 9(10) \\ -1 & \text{if } p \equiv 3, 7(10) \end{cases}$$

$$\left(\frac{6}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 5, 19, 23(24) \\ -1 & \text{if } p \equiv 7, 11, 13, 17(24) \end{cases}$$

$$\left(\frac{7}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 3, 9, 19, 25, 27(28) \\ -1 & \text{if } p \equiv 5, 11, 13, 15, 17, 23(28) \end{cases}$$

$$\left(\frac{8}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7, 17, 23(24) \\ -1 & \text{if } p \equiv 5, 11, 13, 19(24) \end{cases}$$

$$\left(\frac{9}{p}\right) = 1 \text{ for every primes } p \geq 11$$

$$\left(\frac{10}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 3, 9, 13, 27, 31, 37, 39(40) \\ -1 & \text{if } p \equiv 7, 11, 17, 19, 21, 23, 29, 33, 37(40). \end{cases}$$

Theorem 2.2: Let \mathbf{F}_p be a finite field. Then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1(4) \\ -1 & \text{if } p \equiv 3(4) \end{cases}$$

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 3(8) \\ -1 & \text{if } p \equiv 5, 7(8) \end{cases}$$

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7(12) \\ -1 & \text{if } p \equiv 5, 11(12) \end{cases}$$

$$\left(\frac{-4}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 5(12) \\ -1 & \text{if } p \equiv 7, 11(12) \end{cases}$$

$$\left(\frac{-5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 3, 7, 9(20) \\ -1 & \text{if } p \equiv 11, 13, 17, 19(20) \end{cases}$$

$$\left(\frac{-6}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 5, 7, 11, 25, 29, 31, 35(48) \\ -1 & \text{if } p \equiv 13, 17, 19, 23, 37, 41, 43, 47(48) \end{cases}$$

$$\left(\frac{-7}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 9, 11, 15, 23, 25(28) \\ -1 & \text{if } p \equiv 3, 5, 13, 17, 19, 27(28) \end{cases}$$

$$\left(\frac{-8}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 11, 17, 19, 25, 35, 41, 43(48) \\ -1 & \text{if } p \equiv 5, 7, 13, 23, 29, 31, 37, 47(48) \end{cases}$$

$$\left(\frac{-9}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 5, 13, 17(24) \\ -1 & \text{if } p \equiv 7, 11, 19, 23(24) \end{cases}$$

$$\left(\frac{-10}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7, 9, 11, 13, 19, 23, 37(40) \\ -1 & \text{if } p \equiv 3, 17, 21, 27, 29, 31, 33, 39(40). \end{cases}$$

Now we can consider our main problem.

Theorem 2.3: Let E_a be the singular curve defined in (1). Then

$$\#E_1(\mathbf{F}_p) = p \text{ for every primes } p \geq 5$$

$$\#E_2(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 7(8) \\ p+2 & \text{if } p \equiv 3, 5(8) \end{cases}$$

$$\#E_3(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 11(12) \\ p+2 & \text{if } p \equiv 5, 7(12) \end{cases}$$

$$\#E_4(\mathbf{F}_p) = p \text{ for every primes } p \geq 5$$

$$\#E_5(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 9(10) \\ p+2 & \text{if } p \equiv 3, 7(10) \end{cases}$$

$$\#E_6(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 5, 19, 23(24) \\ p+2 & \text{if } p \equiv 7, 11, 13, 17(24) \end{cases}$$

$$\#E_7(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 3, 9, 19, 25, 27(28) \\ p+2 & \text{if } p \equiv 5, 11, 13, 15, 17, 23(28) \end{cases}$$

$$\#E_8(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 7, 17, 23(24) \\ p+2 & \text{if } p \equiv 5, 11, 13, 19(24) \end{cases}$$

$$\#E_9(\mathbf{F}_p) = p \text{ for every primes } p \geq 11$$

$$\#E_{10}(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 3, 9, 13, 27, 31, 37, 39(40) \\ p+2 & \text{if } p \equiv 7, 11, 17, 19, 21, 23, 29, 33, 37(40) \end{cases}$$

$$\#E_{-1}(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1(4) \\ p+2 & \text{if } p \equiv 3(4) \end{cases}$$

$$\#E_{-2}(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 3(8) \\ p+2 & \text{if } p \equiv 5, 7(8) \end{cases}$$

$$\#E_{-3}(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 7(12) \\ p+2 & \text{if } p \equiv 5, 11(12) \end{cases}$$

$$\#E_{-4}(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 5(12) \\ p+2 & \text{if } p \equiv 7, 11(12) \end{cases}$$

$$\#E_{-5}(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 3, 7, 9(20) \\ p+2 & \text{if } p \equiv 11, 13, 17, 19(20) \end{cases}$$

$$\#E_{-6}(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 5, 7, 11, 25, 29, 31, 35(48) \\ p+2 & \text{if } p \equiv 13, 17, 19, 23, 37, 41, 43, 47(48) \end{cases}$$

$$\#E_{-7}(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 9, 11, 15, 23, 25(28) \\ p+2 & \text{if } p \equiv 3, 5, 13, 17, 19, 27(28) \end{cases}$$

$$\#E_{-8}(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 11, 17, 19, 25, 35, 41, 43(48) \\ p+2 & \text{if } p \equiv 5, 7, 13, 23, 29, 31, 37, 47(48) \end{cases}$$

$$\#E_{-9}(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 5, 13, 17(24) \\ p+2 & \text{if } p \equiv 7, 11, 19, 23(24) \end{cases}$$

$$\#E_{-10}(\mathbf{F}_p) = \begin{cases} p & \text{if } p \equiv 1, 7, 9, 11, 13, 19, 23, 37(40) \\ p+2 & \text{if } p \equiv 3, 17, 21, 27, 29, 31, 33, 39(40). \end{cases}$$

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 the results.

Theorem 2.4: The sum of $[x]$ on E_a is

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

Proof: Let $U_p = \{1, 2, \dots, p-1\}$ be the set of units in \mathbf{F}_p . Then then taking squares of elements in U_p , we would obtain the set of quadratic residues $Q_p = \{1^2, 2^2, \dots, (\frac{p-1}{2})^2\}$. Then the sum of all elements in Q_p hence

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

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 $H = Q_p - \{a\}$. Then

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

We know that every element x of H makes $x(x - a)^2$ is 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

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

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

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

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

$$\sum_{[y]} E_a(\mathbf{F}_p) = \begin{cases} \frac{p^2 - 3p}{2} & \text{if } \left(\frac{a}{p}\right) = 1 \\ \frac{p^2 - p}{2} & \text{if } \left(\frac{a}{p}\right) = -1. \end{cases}$$

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

$$y^2 \equiv t^2 \pmod{p} \Leftrightarrow y \equiv \pm t \pmod{p}.$$

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

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

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

$$y^2 \equiv t^2 \pmod{p} \Leftrightarrow y \equiv \pm t \pmod{p}.$$

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

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

REFERENCES

- [1] A.O.L. Atkin and F. Moralin. *Elliptic Curves and Primality Proving*. Math. Comp. **61** (1993), 29–68.
- [2] B. Gezer, H. Özden, A. Tekcan and O. Bizim. *The Number of Rational Points on Elliptic Curves $y^2 = x^3 + b^2$ over Finite Fields*. International Journal of Computational and Mathematics Sciences **1**(3)(2007), 178–184.
- [3] 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.
- [4] N. Koblitz. *A Course in Number Theory and Cryptography*. Springer-Verlag, 1994.
- [5] F. Lemmermeyer. *Reciprocity Laws. From Euler to Eisenstein*. Springer-Verlag Heidelberg, 2000.
- [6] H.W.Jr. Lenstra. *Factoring Integers with Elliptic Curves*. Annals of Maths. **126**(3) (1987), 649–673.
- [7] 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.
- [8] R.A. Mollin. *An Introduction to Cryptography*. Chapman&Hall/CRC, 2001.
- [9] L.J. Mordell. *On the Rational Solutions of the Indeterminate Eqnarrays of the Third and Fourth Degrees*. Proc. Cambridge Philos. Soc. **21**(1922), 179–192.
- [10] R. Schoof. *Counting Points on Elliptic Curves Over Finite Fields*. Journal de Theorie des Nombres de Bordeaux **7**(1995), 219–254.
- [11] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.
- [12] A. Tekcan. *Elliptic Curves $y^2 = x^3 - t^2x$ over \mathbf{F}_p* . Int. Jour. of Comp. and Math. Sci. **1**(3) (2007), 165-171.
- [13] A. Tekcan. *The Cubic Congruence $x^2 + ax^2 + bx + c \equiv 0 \pmod{p}$ and Binary Quadratic Forms $F(x, y) = ax^2 + bxy + cy^2$* . Ars Combinatoria **85**(2007), 257-269.

- [14] A. Tekcan. *The Elliptic Curves $y^2 = x(x-1)(x-\lambda)$* . Accepted for publication to *Ars Combinatoria*.
- [15] A. Tekcan. *The Cubic Congruence $x^3 + ax^2 + bx + c \equiv 0 \pmod{p}$ and Binary Quadratic Forms $F(x, y) = ax^2 + bxy + cy^2$ II*. To appear in *Bulletin of Malaysian Math. Soc.*
- [16] L.C. Washington. *Elliptic Curves, Number Theory and Cryptography*. Chapman&Hall /CRC, Boca London, New York, Washington DC, 2003.
- [17] A. Wiles. *Modular Elliptic Curves and Fermat's Last Theorem*. *Annals of Maths.* **141**(3) (1995), 443–551.