RATIONAL POINTS ON ELLIPTIC CURVES

\[ y^2 = x^3 + a^3 \text{ IN } \mathbb{F}_p \text{ WHERE } p \equiv 1 \pmod{6} \text{ IS PRIME}^* \]

Musa Demirci, Gökhan Soydan, Ismail Naci Cangül

Abstract

In this work, we consider the rational points on elliptic curves over finite fields \( \mathbb{F}_p \). We give results concerning the number of points on the elliptic curve \( y^2 \equiv x^3 + a^3 \pmod{p} \) where \( p \) is a prime congruent to 1 modulo 6. Also some results are given on the sum of abscissae of these points. We give the number of solutions to \( y^2 \equiv x^3 + a^3 \pmod{p} \), also given in [1], p.174, this time by means of the quadratic residue character, in a different way, by using the cubic residue character. Using the Weil conjecture, one can generalize the results concerning the number of points in \( \mathbb{F}_p \) to \( \mathbb{F}_p^r \).

1 Introduction

Let \( F \) be a field of characteristic not equal to 2 or 3. An elliptic curve \( E \) defined over \( F \) is given by an equation

\[ y^2 = x^3 + Ax + B \in \mathbb{F}[x] \] (1)

where \( A, B \in \mathbb{F} \) so that \( 4A^3 + 27B^2 \neq 0 \) in \( \mathbb{F} \). The set of all solutions \((x, y)\in \mathbb{F} \times \mathbb{F} \) to this equation together with a point \( \mathcal{O} \), called the point at infinity, is denoted by \( E(\mathbb{F}) \), and called the set of \( \mathbb{F} \)-rational points on \( E \). The value \( \Delta(E) = -16(4A^3 + 27B^2) \) is called the discriminant of the elliptic curve \( E \). For a more detailed information about elliptic curves in general, see [3].

The \( E(\mathbb{F}) \) forms an additive abelian group having identity \( \mathcal{O} \). Here by definition, \(-P = (x, -y)\) for a point \( P = (x, y) \) on \( E \).

It has always been interesting to look for the number of points over a given field \( \mathbb{F} \). In [5], three algorithms to find the number of points on an elliptic curve over a finite field are given.

*This work was supported by the research fund of Uludag University project no: F-2003/63

AMS 2000 Subject Classification Number : 11G20, 14H25, 14K15, 14G99

Keywords: Elliptic curves over finite fields, rational points
2 The Group $E(F_p)$ of Points Modulo $p, p \equiv 1 \pmod{6}$

It is interesting to solve polynomial congruences modulo $p$. Clearly, it is much easier to find solutions in $F_p$ for small $p$, than to find them in $Q$. Because, in $F_p$, there is always a finite number of solutions.

Let $\alpha \in F_p$ and let $p$ be as stated earlier, then the number of solutions to $x^3 = \alpha$ is given by $1 + \chi_3(\alpha) + \chi_3^2(\alpha)$ for a cubic character $\chi_3$ (so $\chi_3 : F_p^* \to \{1, \omega, \omega^2\}$ where $\omega$ is a non-trivial cubic root of unity). Likewise, let $\chi(a) = (a \mid p)$ denote the Legendre symbol which is equal to $+1$ if $a$ is a quadratic residue modulo $p$; $-1$ if not; and $0$ if $p|a$. The number of solutions to $x^2 = \alpha$ is then $1 + \chi(\alpha)$.

In this work, we consider the elliptic curve (1) in modulo $p$, for $A = 0$ and $B = a^3$, and denote it by $E_a$. We try to obtain results concerning the number of points on $E_a$ over $F_p$, and also their orders.

Let us denote the set of $F_p$-rational points on $E_a$ by $E_a(F_p)$, and let $N_{p,a}$ be the cardinality of the set $E_a(F_p)$. It is known that the number of solutions of $y^2 = u (\pmod{p})$ is $1 + \chi(u)$, and so the number of solutions to $y^2 \equiv x^3 + a^3 (\pmod{p})$, counting the point at infinity, is

$$N_{p,a} = 1 + \sum_{x \in F_p} (1 + \chi(x^3 + a^3)) = p + 1 + \sum_{x \in F_p} \chi(x^3 + a^3).$$

It can easily be seen that an elliptic curve

$$y^2 = x^3 + a^3$$

(2)

can have at most $2p + 1$ points in $\mathbb{Z}_p$; i.e. the point at infinity along with $2p$ pairs $(x, y)$ with $x, y \in F_p$, satisfying the equation (2). This is because, for each $x \in F_p$, there are at most two possible values of $y \in F_p$, satisfying (2).

But not all elements of $F_p$ have a square root. In fact, only half of the elements in $F_p^* = F_p \setminus \{0\}$ have square roots. Therefore the expected number of points on $E(F_p)$ is about $p + 1$.

It is known, as a more precise formula, that the number of solutions to (2) is

$$p + 1 + \sum \chi(x^3 + a^3).$$

The following theorem of Hasse quantifies this result:

**Theorem 1 (Hasse, 1922)** An elliptic curve (2) has

$$p + 1 + \delta$$

solutions $(x, y)$ modulo $p$, where $|\delta| < 2\sqrt{p}$.

Equivalently, the number of solutions is bounded above by the number $(\sqrt{p} + 1)^2$. 

2
From now on, we will only consider the case where \( p \) is a prime congruent to 1 modulo 6. We begin by some calculations regarding the number of points on (2). First we have

**Theorem 2** Let \( p \equiv 1 \pmod{6} \) be a prime. The number of points \( (x, y) \) on the curve \( y^2 = x^3 + a^3 \) modulo \( p \) is given by

\[
4 + \sum_{x \in \mathbb{F}_p} \rho(x)
\]

where

\[
\rho(x) = \begin{cases} 
2 & \text{if } \chi(x^3 + a^3) = 1 \\
0 & \text{if } \chi(x^3 + a^3) \neq 1
\end{cases}
\]

Also the sum of such \( y \) is \( p \).

**Proof.** For \( x = 0, 1, 2, \ldots, p-1 \pmod{p} \), find the values \( y^2 = x^3 + a^3 \pmod{p} \). Let \( Q_p \) denote the set of quadratic residues modulo \( p \). When \( y^2 \in Q_p \), then there are two values of \( y \in U_p \), the set of units in \( \mathbb{F}_p \); which are \( x_0 \) and \( p - x_0 \). When \( y = 0 \), there are three more points which are \( x = a \), \( x = wa \) and \( x = w^2a \) where \( w^2 + w + 1 = 0 \). (Here \( w \in \mathbb{F}_p \) since \( p \equiv 1 \pmod{6} \)). Finally considering the point at infinity, the result follows. \( \blacksquare \)

We now consider the points on (2) lying on the \( y \)-axis.

**Theorem 3** Let \( p \equiv 1 \pmod{6} \) be prime. For \( x \equiv 0 \pmod{p} \), there are two points on the curve \( y^2 \equiv x^3 + a^3 \pmod{p} \), when \( a \in Q_p \), while when \( a \notin Q_p \), there is no point with \( x \equiv 0 \pmod{p} \).

**Proof.** For \( x \equiv 0 \pmod{p} \), we have \( y^2 \equiv a^3 \pmod{p} \). First consider \( y^2 \equiv a^3 \pmod{p} \). This congruence has a solution if and only if \( \left( \frac{a^3}{p} \right) = \left( \frac{a}{p} \right) = 1 \); i.e. if and only if \( a \) is a quadratic residue modulo \( p \). \( \blacksquare \)

Let us now denote by \( K_p \), the set of cubic residues modulo \( p \). We can now restate the result given just before Hasse’s theorem in terms of cubic residues modulo \( p \), instead of quadratic residues.

**Theorem 4** Let \( p \equiv 1 \pmod{6} \) be prime. Let \( t = y^2 - a^3 \). Then the number of points on the curve \( y^2 \equiv x^3 + a^3 \pmod{p} \) is given by the sum

\[
1 + \sum f(t)
\]

where

\[
f(t) = \begin{cases} 
0 & \text{if } t \notin K_p, \\
1 & \text{if } p | t, \\
3 & \text{if } t \in K_p^*,
\end{cases}
\]

and the sum is taken over all \( y \in \mathbb{F}_p \).
Proof. Let $p|t$. Then the equation $x^3 \equiv t \pmod{p}$ becomes $x^3 \equiv 0 \pmod{p}$. Then the unique solution is $x \equiv 0 \pmod{p}$. Therefore $f(t) = 1$.

Let secondly $t \notin K_p$. Then $t$ is not a cubic residue and the congruence $x^3 \equiv t \pmod{p}$ has no solutions. If $t \in K_p^*$, then $x^3 \equiv t \pmod{p}$ has three solutions since $p \equiv 1 \pmod{6}$ and $(p-1, 3) = 3$.

We can also give a result about the sum of abscissae of the rational points on the curve:

**Theorem 5** Let $p \equiv 1 \pmod{6}$ be prime. The sum of abscissae of the rational points on the curve $y^2 \equiv x^3 + a^3 \pmod{p}$ is

$$\sum_{x \in \mathbb{F}_p} (1 + \chi_p(x^3 + a^3)).x.$$ 

**Proof.** Since

$$\chi_p(t) = \begin{cases} +1 & \text{if } x^2 \equiv t \pmod{p} \text{ has a solution,} \\ 0 & \text{if } p|t, \\ -1 & \text{if } x^2 \equiv t \pmod{p} \text{ has no solutions,} \end{cases}$$

we know that $1 + \chi_p(t) = 0, 1$ or $2$. When $y \equiv 0 \pmod{p}$, $x^3 + a^3 \equiv 0 \pmod{p}$ and hence as $p|0$, $\chi_p(x^3 + a^3) = 0$. For each such point $(x, 0)$ on the curve, $(1+0).x = x$ is added to the sum.

Let $x^3 + a^3 = t$. If $(\frac{1}{p}) = +1$, then for each such point $(x, y)$ on the curve, the point $(x, -y)$ is also on the curve. Therefore for each such $t$, $(1+1).x = 2x$ is added to the sum.

Finally if $(\frac{1}{p}) = -1$, then the congruence $x^2 \equiv t \pmod{p}$ has no solutions, and such points $(x, y)$ contribute to the sum as much as $(1 + (-1)).x = 0$.

As we can see from the following result, the above sum is always congruent to 0 modulo $p$.

**Theorem 6** Let $p \equiv 1 \pmod{6}$ be prime. Then the sum of the integer solutions of $x^3 \equiv t \pmod{p}$ is congruent to 0 modulo $p$.

**Proof.** The solutions of the congruence $x^3 \equiv 1 \pmod{p}$ are $x \equiv 1, w$ and $w^2 \pmod{p}$, where $w = \frac{-1 + \sqrt{3}}{2}$ is the cubic root of unity. In general, the solutions of $x^3 \equiv t \pmod{p}$ are $x \equiv x_0, x_0 w$ and $x_0 w^2 \pmod{p}$, where $x_0$ is a solution. This is because $(x_0 w)^3 \equiv x_0^3 w^3 \equiv x_0^3 \equiv t \pmod{p}$ and similarly $(x_0 w^2)^3 \equiv x_0^3 w^6 \equiv x_0^3 (w^3)^2 \equiv x_0^3 \equiv t \pmod{p}$. Therefore the sum of these solutions is

$$x_0 + x_0 w + x_0 w^2 = x_0 + x_0 w + x_0(-1 - w) = 0$$

If there is no solution, the sum can be thought of as 0.
Theorem 7 Let \( p \equiv 1 \pmod{6} \) be prime. Let \( 0 \leq x \leq p - 1 \) be an integer. Then for any \( 1 \leq a \leq p - 1 \), the sum (which is an integer)

\[
j(p) = \sum_{x=0}^{p-1} (1 + \chi(x^3 + a^3))x
\]

is divisible by \( p \). In particular

\[
s(p) = \sum_{x=0}^{p-1} \chi(x^3 + a^3)x
\]

is divisible by \( p \).

**Proof.** For every value of \( y \), let \( y^2 - a^3 = t \). Then the sum of the solutions of the congruence \( x^3 \equiv t \pmod{p} \) is congruent to 0 by Theorem 6.

For all values of \( y \), this is valid and hence the sum of all these abscissae is congruent to 0.

The hypothesis \( p \equiv 1 \pmod{6} \) is essential in this Theorem 7, as the following counterexample shows: take \( a = 1, \ p = 11 \). Then the first sum is easily seen to be 56 and the second is easily seen to be 1 and clearly neither of them is divisible by 11.

We now look at the points on the curve having the same ordinate:

Theorem 8 Let \( p \equiv 1 \pmod{6} \) be prime. The sum of the abscissae of the points \( (x, y) \) on the curve \( y^2 \equiv x^3 + a^3 \pmod{p} \) having the same ordinate \( y \), is congruent to zero modulo \( p \).

**Proof.** Let \( y \) be given. Then the congruence

\[
x^3 \equiv y^2 - a^3 \pmod{p}
\]

becomes

\[
x^3 \equiv t \pmod{p}
\]

after a substitution \( t = y^2 - a^3 \). The result then follows by Theorem 6.

Finally we consider the total number of points on a family of curves \( y^2 \equiv x^3 + a^3 \pmod{p} \), for \( a \equiv 0, 1, \ldots, p - 1 \pmod{p} \) and \( p \equiv 1 \pmod{6} \) is prime. We find that when \( (a, p) = 1 \), there are \( p + 1 - 2k \) or \( p + 1 + 2k \) points on a curve \( y^2 \equiv x^3 + a^3 \pmod{p} \), for a suitable integer \( k \).

Theorem 9 Let \( p \equiv 1 \pmod{6} \) be prime and let \( 1 \leq a \leq p - 1 \). Let \( N_{p,a} = \#E(\mathbb{F}_p) \). Then

\[
\sum_{a=1}^{p-1} N_{p,a} = p^2 - 1.
\]
Proof. Since $1 \leq a \leq p - 1$, we have $(a, p) = 1$. Then the set of elements $a^3x^3$ modulo $p$ is the same as the set of $x^3$ modulo $p$. Then

$$\sum_{x \in \mathbb{F}_p} \chi(x^3 + a^3) = \sum_{x \in \mathbb{F}_p} \chi(a^3x^3 + a^3) = \chi(a^3) \sum_{x \in \mathbb{F}_p} \chi(x^3 + 1).$$

By the discussion at the beginning of section 2, we get

$$N_{p,a} - p - 1 = \chi(a^3)(N_{p,1} - p - 1).$$

Then by taking sum at both sides, we obtain

$$\sum_{a=1}^{p-1} (N_{p,a} - p - 1) = \sum_{a=1}^{p-1} \chi(a^3)(N_{p,1} - p - 1).$$

Then

$$\sum_{a=1}^{p-1} N_{p,a} - \sum_{a=1}^{p-1} (p + 1) = (N_{p,1} - p - 1) \sum_{a=1}^{p-1} \chi(a^3) = (N_{p,1} - p - 1) \sum_{a=1}^{p-1} \chi(a)$$

using $\chi(a^3) = \chi(a)$ as both sides are 1 or $-1$. Finally as there are as many residues as non residues, we know that

$$\sum_{a=1}^{p-1} \chi(a) = 0$$

and by means of it, we conclude

$$\sum_{a=1}^{p-1} N_{p,a} = p^2 - 1,$$

as required. □

Conclusion 10 All the results concerning the number of points on $\mathbb{F}_p$ obtained here for prime $p \equiv 1 \pmod{6}$ can be generalized to $\mathbb{F}_{p^r}$, for a natural number $r > 1$, using the following result:

Theorem 11 (Weil Conjecture) The Zeta-function is a rational function of $T$ having the form

$$Z(T; E/\mathbb{F}_q) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)}$$

where only the integer $a$ depends on the particular elliptic curve $E$. The value $a$ is related to $N = N_1$ as follows:

$$N = q + 1 - a.$$
In addition, the discriminant of the quadratic polynomial in the numerator is negative, and so the quadratic has two conjugate roots \( \frac{1}{\alpha} \) and \( \frac{1}{\beta} \) with absolute value \( \frac{1}{\sqrt{q}} \). Writing the numerator in the form \((1 - \alpha T)(1 - \beta T)\) and taking the derivatives of logarithms of both sides, one can obtain the number of \( F_{q^r} \)-points on \( E \), denoted by \( N_r \), as follows:

\[
N_r = q^r + 1 - \alpha^r - \beta^r, \quad r = 1, 2, ...
\]

**Example 12** Let us find the \( F_7 \)-points on the elliptic curve \( y^2 = x^3 + 4 \). There are \( N_1 = 12 \) \( F_7 \)-points on the elliptic curve:

\[(0, 1), (0, 6), (1, 3), (1, 4), (2, 3), (2, 4), (3, 0), (4, 3), (4, 4), (5, 0), (6, 0) \text{ and } \circ.\]

Now as \( r = 2 \), we have \( a = -4 \). Then from the quadratic equation

\[
1 + 4T + 7T^2 = 0,
\]

\( \alpha = -2 - \sqrt{3}i \) and \( \beta = -2 + \sqrt{3}i \) and finally \( N_2 = 48 \). Similarly \( N_3 = 324 \) can be calculated.

**References**

[1] Koblitz, N., *A Course in Number Theory and Cryptography*, Springer-Verlag, (1994), ISBN 3-540-94293-9.

[2] Mollin, R. A., *An Introduction to Cryptography*, Chapman&Hall/CRC, (2001), ISBN 1-58488-127-5.

[3] Silverman, J. H., *The Arithmetic of Elliptic Curves*, Springer-Verlag, (1986), ISBN 0-387-96203-4.

[4] Silverman, J. H., Tate, J., *Rational Points on Elliptic Curves*, Springer-Verlag, (1992), ISBN 0-387-97825-9.

[5] Schoof, R., *Counting points on elliptic curves over finite fields*, Journal de Théorie des Nombres de Bordeaux, 7 (1995), 219-254.

Musa Demirci, Gökhan Soydan, Ismail Naci Cangül
Department of Mathematics
Uludağ University
16059 Bursa, TURKEY
mdemirci@uludag.edu.tr, gsoydan@uludag.edu.tr, cangul@uludag.edu.tr