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

The Number of Rational Points on Elliptic Curves $y^2 = x^3 + b^2$ Over Finite Fields

Betül Gezer, Hacer Özden, Ahmet Tekcan, Osman Bizim

***Abstract*—Let p be a prime number, $\mathbf{F}_p$ be a finite field and let Q_p denote the set of quadratic residues in $\mathbf{F}_p$. In the first section we give some notations and preliminaries from elliptic curves. In the second section, we consider some properties of rational points on elliptic curves $E_{p,b} : y^2 = x^3 + b^2$ over $\mathbf{F}_p$, where $b \in \mathbf{F}_p^*$. Recall that the order of $E_{p,b}$ over $\mathbf{F}_p$ is $p + 1$ if $p \equiv 5(mod\, 6)$. We generalize this result to any field $\mathbf{F}_p^n$ for an integer $n \geq 2$. Further we obtain some results concerning the sum $\sum_{[x]} E_{p,b}(\mathbf{F}_p)$ and $\sum_{[y]} E_{p,b}(\mathbf{F}_p)$, the sum of $x-$ and $y-$coordinates of all points (x, y) on $E_{p,b}$, and also the the sum $\sum_{(x,0)} E_{p,b}(\mathbf{F}_p)$, the sum of points $(x, 0)$ on $E_{p,b}$.

***Keywords*—elliptic curves over finite fields, rational points on elliptic curves.

I. Introduction

Mordell began his famous paper [8] 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 [4,6,7], for factoring large integers [5] and for primality proving [2,3]. The mathematical theory of elliptic curves was also crucial in the proof of Fermat's Last Theorem [13].

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 char$(\overline{\mathbf{F}}_q) \neq 2, 3$. An elliptic curve E over $\mathbf{F}_q$ is defined by an equation

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

where $a, b \in \mathbf{F}_q$ 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 $y^2 z = x^3 + axz^2 + bz^3$, 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. Let

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

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 $\#E(\mathbf{F}_q)$, is defined as the number of the rational points on E and is given by

$$\begin{aligned} \#E(\mathbf{F}_q) &= 1 + \sum\nolimits_{x \in \mathbf{F}_q} \left(1 + \frac{x^3 + ax + b}{\mathbf{F}_q}\right) \qquad (1) \\ &= q + 1 + \sum\nolimits_{x \in \mathbf{F}_q} \left(\frac{x^3 + ax + b}{\mathbf{F}_q}\right), \end{aligned}$$

where $(\frac{\cdot}{\mathbf{F}_q})$ denotes the Legendre symbol (for further details on rational points on elliptic curves see [9,10,12]).

Let p be a prime number and let $q = p^n$ for integer $n > 1$. Let

$$N = q + 1 - a. \qquad (2)$$

Then a is called the trace of Frobenius and satisfies the inequality

$$|a| \leq 2\sqrt{q} \qquad (3)$$

known as the Hasse interval [12, p.91]. Then there is an elliptic curve E defined over $\mathbf{F}_q$ such that $\#E(\mathbf{F}_q) = N$ if and only if a satisfies (3) and also satisfies one of the following (see [12, p.92]):

1) gcd$(a, p) = 1$
2) n is even and $a = \pm 2\sqrt{q}$
3) n is even, p is not equivalent to $1(mod\, 3)$ and $a = \pm\sqrt{q}$
4) n is odd, $p = 2, 3$ and $a = \pm p^{(n+1)/2}$
5) n is even, p is not equivalent to $1(mod\, 4)$ and $a = 0$
6) n is odd and $a = 0$

The formula (1) can be generalized to any field $\mathbf{F}_{q^n}$ for an integer $n \geq 2$. Let $\#E(\mathbf{F}_q) = q + 1 - a$ and let

$$X^2 - aX + q = (X - \alpha)(X - \beta). \qquad (4)$$

Then the order of E over $\mathbf{F}_{q^n}$ is

$$\#E(\mathbf{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n). \qquad (5)$$

II. The Number of Rational Points on Elliptic Curve $y^2 = x^3 + b^2$ Over $\mathbf{F}_p$.

In [11], the third author consider the elliptic curves $E : y^2 = x^3 - t^2 x$ over a finite field $\mathbf{F}_p$, where p is a prime number and $t \in \mathbf{F}_p^*$. He obtain some results concerning rational points on E.

In the present paper we consider the elliptic curves

$$E_{p,b} : y^2 = x^3 + b^2 \qquad (6)$$

over $\mathbf{F}_p$. Recall that if $p \equiv 5(mod\, 6)$, then $\#E(\mathbf{F}_p) = p + 1$. But when $p \equiv 1(mod\, 6)$, then there is no rule for $\#E(\mathbf{F}_p)$. Therefore we assume that $p \equiv 5(mod\ 6)$ throughout the paper.

Betül Gezer, Hacer Özden, Ahmet Tekcan and Osman Bizim are with the Uludag University, Department of Mathematics, Faculty of Science, Bursa-TURKEY, emails: betulgezer@uludag.edu.tr, hozden@uludag.edu.tr, tekcan@uludag.edu.tr, obizim@uludag.edu.tr

First we give the following theorem.

Theorem 2.1: Let $p \equiv 5(mod\, 6)$ be a prime. If $(p-1,3) = 1$, then the congruence

$$x^3 \equiv b(mod\, p)$$

has a solution for each $b \in \mathbf{F}_p$, that is every $b \in \mathbf{F}_p$ is a cubic residue.

Proof: Let $p \equiv 5(mod\, 6)$. Then $p = 5 + 6q$ for some $q \in \mathbf{Z}$. Then

$$(p-1,3) = (6q+4,3) = 1.$$

Hence we have either $p = 3$ or $p \equiv 2(mod\, 3)$. So if $p = 3$, then

$$0^3 \equiv 0(mod\, 3),\ 1^3 \equiv 1(mod\, 3),\ 2^3 \equiv 2(mod\, 3)$$

in $\mathbf{F}_3$. Therefore every $b \in \mathbf{F}_3$ is a cubic residue.

If $p \equiv 2(mod\, 3)$, then $p = 2 + 3q$ for $q \in \mathbf{Z}$. Therefore the norm of p is

$$|p| = p\overline{p} = (2+3q)(2+3q) = 9q^2 + 12q + 4$$

and hence

$$\frac{|p|-1}{3} = 3q^2 + 4q + 1.$$

So we have

$$b^{\frac{|p|-1}{3}} = b^{3q^2+4q+1}.$$

Hence $b^{p-1} \equiv 1(mod\, p)$ by Fermat's Little Theorem. So

$$b^{p-1} \equiv b^{3q+2-1} \equiv b^{3q+1} \equiv 1(mod\, p).$$

Consequently

$$b^{\frac{|p|-1}{3}} \equiv (b^{3q+1})^{q+1} \equiv 1^{q+1} \equiv 1(mod\, p).$$

Now let $1 \le b \le p-1$ and let $0 \le q \le p-2$. Let g be a primitive root modulo p such that $g^q \equiv b(mod\, p)$. Hence there are integers u and v such that

$$3u + (p-1)v = 1 \tag{7}$$

since $(3, p-1) = 1$. If we take $x = uq$ and $y = vq$, then (7) becomes

$$3x + (p-1)y = q.$$

Therefore we get

$$\begin{aligned} b &\equiv g^q(mod\, p) \\ &\equiv g^{sx+(p-1)y}(mod\, p) \\ &\equiv (g^x)^3(g^{p-1})^y(mod\, p) \\ &\equiv (g^x)^3(mod\, p) \end{aligned}$$

since $g^{p-1} \equiv 1(mod\, p)$, that is, b is a cubic residue modulo p. Further $0^3 \equiv 0(mod\, p)$. Therefore all elements of $\mathbf{F}_p$ are cubic residues. ■

We know that the order of $E_{p,b} : y^2 = x^3 + b^2$ over $\mathbf{F}_p$ is $\#E_{p,b}(\mathbf{F}_p) = p+1$. Now we generalize this result to $\mathbf{F}_{p^n}$ for a positive integer $n \ge 2$.

Theorem 2.2: Let $E_{p,b} : y^2 = x^3 + b^2$ be an elliptic curve over $\mathbf{F}_p$. Then

$$\#E_{p,b}(\mathbf{F}_{p^n}) = \begin{cases} (p^{\frac{n}{2}}-1)^2 & if \quad n \equiv 0(mod\, 4) \\ p^n + 1 & if \quad n \equiv 1,3(mod\, 4) \\ (p^{\frac{n}{2}}+1)^2 & if \quad n \equiv 2(mod\, 4). \end{cases}$$

Proof: Let $E_{p,b} : y^2 = x^3 + b^2$. Then the order of $E_{p,b}$ over $\mathbf{F}_p$ is $\#E_{p,b}(\mathbf{F}_p) = p+1$. Therefore $a = 0$ by (2). Then

$$\begin{aligned} X^2 + p &= (X - i\sqrt{p})(X + i\sqrt{p}) \\ &= (X-\alpha)(X-\beta) \end{aligned}$$

for $\alpha = i\sqrt{p}$ and $\beta = -i\sqrt{p}$.

Let $n \equiv 0(mod\, 4)$, say $n = 4k$ for an integer $k \ge 1$. Then

$$\begin{aligned} \alpha^n + \beta^n &= (i\sqrt{p})^{4k} + (-i\sqrt{p})^{4k} \\ &= i^{4k}(\sqrt{p})^{4k} + (-i)^{4k}(\sqrt{p})^{4k} \\ &= p^{2k} + p^{2k} \\ &= 2p^{2k} \\ &= 2p^{\frac{n}{2}}. \end{aligned}$$

So

$$\begin{aligned} \#E_{p,b}(\mathbf{F}_{p^n}) &= p^n + 1 - (\alpha^n + \beta^n) \\ &= p^n + 1 - 2p^{\frac{n}{2}} \\ &= (p^{\frac{n}{2}} - 1)^2 \end{aligned}$$

by (5).

Let $n \equiv 1(mod\, 4)$, say $n = 1 + 4k$. Then

$$\begin{aligned} \alpha^n + \beta^n &= (i\sqrt{p})^{4k+1} + (-i\sqrt{p})^{4k+1} \\ &= i^{4k+1}(\sqrt{p})^{4k+1} + (-i)^{4k+1}(\sqrt{p})^{4k+1} \\ &= i(\sqrt{p})^{4k+1} - i(\sqrt{p})^{4k+1} \\ &= 0 \end{aligned}$$

So $\#E_{p,b}(\mathbf{F}_{p^n}) = p^n + 1$.

Let $n \equiv 2(mod\, 4)$, say $n = 2 + 4k$. Then

$$\begin{aligned} \alpha^n + \beta^n &= (i\sqrt{p})^{4k+2} + (-i\sqrt{p})^{4k+2} \\ &= i^{4k+2}(\sqrt{p})^{4k+2} + (-i)^{4k+2}(\sqrt{p})^{4k+2} \\ &= -p^{2k+1} - p^{2k+1} \\ &= -2p^{2k+1} \\ &= -2p^{\frac{n}{2}}. \end{aligned}$$

So $\#E_{p,b}(\mathbf{F}_{p^n}) = p^n + 1 + 2p^{\frac{n}{2}} = (p^{\frac{n}{2}} + 1)^2$.

Finally, let $n \equiv 3(mod\, 4)$, say $n = 3 + 4k$. Then

$$\begin{aligned} \alpha^n + \beta^n &= (i\sqrt{p})^{4k+3} + (-i\sqrt{p})^{4k+3} \\ &= i^{4k+3}(\sqrt{p})^{4k+3} + (-i)^{4k+3}(\sqrt{p})^{4k+3} \\ &= -i(\sqrt{p})^{4k+3} + i(\sqrt{p})^{4k+3} \\ &= 0 \end{aligned}$$

So $\#E_{p,b}(\mathbf{F}_{p^n}) = p^n + 1$. ■

Example 2.1: Let $E_{11,2} : y^2 = x^3 + 4$ be an elliptic curve over $\mathbf{F}_{11}$. Then the order of $E_{11,2}$ over $\mathbf{F}_{11^n}$ is

$$\#E_{11,2}(\mathbf{F}_{11^n}) = \begin{cases} 214329600 & for \quad n = 8 \\ 2357947692 & for \quad n = 9 \\ 285311670612 & for \quad n = 11 \\ 25937746704 & for \quad n = 10. \end{cases}$$

Let $[x]$ and $[y]$ denote the $x-$coordinates and $y-$coordinates of the points (x, y) on $E_{p,b}$, respectively. Then we have the following results.

Theorem 2.3: The sum of $[x]$ on $E_{p,b}$ is

$$\sum_{[x]} E_{p,b}(\mathbf{F}_p) = \sum_{[x]} \left(1 + \left(\frac{x^3 + b^2}{\mathbf{F}_p}\right)\right).x$$

Proof: We know that

$$\left(\frac{x^3 + b^2}{\mathbf{F}_p}\right) = \begin{cases} 0 & if \quad x^3 + b^2 = 0 \\ 1 & if \quad x^3 + b^2 \in Q_p \\ -1 & if \quad x^3 + b^2 \notin Q_p. \end{cases}$$

Let $\left(\frac{x^3+b^2}{\mathbf{F}_p}\right) = 0$. Then $x^3 + b^2 = 0$. Hence the cubic equation $x^3 + b^2 = 0$ has only one solution $x = \sqrt[3]{-b^2}$. Therefore

$$y^2 \equiv 0(mod\, p) \Leftrightarrow y \equiv 0(mod\, p).$$

So for such a point x, we have a point $(x, 0)$ on $E_{p,b}$. Therefore we get $(x + 0).x = x$ is added to the sum.

Let $\left(\frac{x^3+b^2}{\mathbf{F}_p}\right) = 1$. Then $x^3 + b^2$ is a square in $\mathbf{F}_p$. Let $x^3 + b^2 = t^2$ for any $t \in \mathbf{F}_p^*$. Then

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

that is, for any point (x, t) on $E_{p,b}$, the point $(x, -t)$ is also on $E_{p,b}$. Therefore for each point (x, y), we have $(1+1).x = 2x$ is added to the sum.

Let $\left(\frac{x^3+b^2}{\mathbf{F}_p}\right) = -1$. Then x^3+b^2 is not a square in $\mathbf{F}_p$. Then the equation $y^2 \equiv x^3 + b^2(mod\, p)$ has no solution. Therefore for each point (x, y) we have $(1 + (-1)).x = 0$. ■

Theorem 2.4: The sum of $[y]$ on $E_{p,b}$ is

$$\sum_{[y]} E_{p,b}(\mathbf{F}_p) = \frac{p^2 - p}{2}.$$

Proof: Let $E_{p,b} : y^2 = x^3 + b^2$ be an elliptic curve over $\mathbf{F}_p$. The cubic equation $x^3+b^2 = 0$ has a solution $x = \sqrt[3]{-b^2}$. For the other values of x, we have both x and $-x$. One of these gives two points. The one makes $x^3 + b^2$ is a square, i.e. $\left(\frac{x^3+b^2}{\mathbf{F}_p}\right) = 1$. There are $\frac{p-1}{2}$ points x in $\mathbf{F}_p$ such that $x^3 + b^2$ is a square. Let $x^3 + b^2 = t^2$ for any $t \in \mathbf{F}_p^*$. Then we have

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

Hence $y = t$ and $y = p - t$. So the sum of these values of y is $t + (p - t) = p$. We know that there are $\frac{p-1}{2}$ points x in $\mathbf{F}_p$ such that $y^2 = x^3 + b^2$ is a square. Therefore, the sum of ordinates of all points (x, y) is $p\frac{p-1}{2}$, that is

$$\sum_{[y]} E_{p,b}(\mathbf{F}_p) = \frac{p^2 - p}{2}.$$

■

Theorem 2.5: Let $\mathbf{E}_{p,b}$ denote the set of the family of all elliptic curves over $\mathbf{F}_p$. Then

$$\sum_{b \in \mathbf{F}_p^*} \#\mathbf{E}_{p,b}(\mathbf{F}_p) = \frac{p^2 - 1}{2}.$$

Proof: Note that there are $\frac{p-1}{2}$ elliptic curves $E_{p,b} : y^2 = x^3 + b^2$ over $\mathbf{F}_p$, and also the order of $E_{p,b}$ over $\mathbf{F}_p$ is $p+1$, i.e. $\#E_{p,b}(\mathbf{F}_p) = p + 1$. Therefore the total number of the points (x, y) on all elliptic curves $E_{p,b}$ in $\mathbf{E}_{p,b}$ over $\mathbf{F}_p$ is

$$\sum_{b \in \mathbf{F}_p^*} \#\mathbf{E}_{p,b}(\mathbf{F}_p) = (p + 1)\frac{p - 1}{2} = \frac{p^2 - 1}{2}.$$

■

We can give the following two theorems for the rational points $(x, 0)$ on $E_{p,b}$.

Theorem 2.6: Let $E_{p,b} : y^2 = x^3 + b^2$ be an elliptic curve over $\mathbf{F}_p$, and let $(x, 0)$ be a point on $E_{p,b}$. Then

$$x \in Q_p \Leftrightarrow p \equiv 1(mod\, 4)$$

and

$$x \notin Q_p \Leftrightarrow p \equiv 3(mod\, 4).$$

Proof: Let $(x, 0)$ be a point on $E_{p,b}$ and let $x \in Q_p$. Then $x^3 \equiv -b^2(mod\, 4)$ since $0 \equiv x^3 + b^2(mod\, 4)$, and $x^3 = x^2.x \in Q_p$. Note that $-b^2 \in Q_p$ if and only if $-1 \in Q_p$, and hence $p \equiv 1(mod\, 4)$.

Conversely, let $p \equiv 1(mod\, 4)$, and let $(x, 0)$ be a point on $E_{p,b}$. Then $x^3 \equiv -b^2(mod\, 4)$. Since $-1 \in Q_p$ and $b^2 \in Q_p$, we have $x^3 \in Q_p$ and hence $x \in Q_p$.

The second assertion can be proved as in the same way that the first assertion was proved. ■

Theorem 2.7: Let $E_{p,b} : y^2 = x^3 + b^2$ be an elliptic curve over $\mathbf{F}_p$, and let $(x, 0)$ be a point on $E_{p,b}$.

1) If $p \equiv 1(mod\, 4)$, then

$$\begin{aligned} \sum_{(x,0)} E_{p,b} &= \sum_{t \in Q_p} t \\ &= \frac{p(p - 1)(p + 1)}{24} \end{aligned}$$

2) If $p \equiv 3(mod\, 4)$, then

$$\begin{aligned} \sum_{(x,0)} E_{p,b} &= \sum_{t \notin Q_p} t \\ &= \frac{p(p - 1)(11 - p)}{24}. \end{aligned}$$

Proof: 1) Let $p \equiv 1(mod\, 4)$. Then we proved in Theorem 2.6 that there exits only one point $x \in Q_p$ such that $(x, 0)$ is a point on $E_{p,b}$. We know that there are $\frac{p-1}{2}$ elements in Q_p. Therefore there are $\frac{p-1}{2}$ points $(x, 0)$ on $E_{p,b}$. Consequently the sum of $x-$coordinates of all points $(x, 0)$ on $E_{p,b}$ is equal to the sum of all elements in Q_p, that is

$$\sum_{(x,0)} E_{p,b} = \sum_{t \in Q_p} t. \tag{8}$$

Let $U_p = \{1, 2, \cdots, p - 1\}$ be the set of units in $\mathbf{F}_p$. Then then taking squares of elements in U_p, we would obtain

$$Q_p = \{1, 4, 9, \cdots, (\frac{p - 1}{2})^2\}.$$

Then the sum of all elements in Q_p is

$$1 + 4 + 9 + \cdots + \frac{p^2 - 2p + 1}{4} = \frac{p(p - 1)(p + 1)}{24}. \tag{9}$$

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

(8) and (9) yield that

$$\begin{aligned}\sum\nolimits_{(x,0)} E_{p,b} &= \sum\nolimits_{t\in Q_p} t\\ &= \frac{p(p-1)(p+1)}{24}.\end{aligned}$$

2) Let $p \equiv 3(mod\,4)$. Then there exits a point $x \notin Q_p$ such that $(x,0)$ is a point on $E_{p,b}$. We know that there are $\frac{p-1}{2}$ elements in $U_p - Q_p$. Therefore there are $\frac{p-1}{2}$ points $(x,0)$ on $E_{p,b}$. Consequently the sum of $x-$coordinates of all points $(x,0)$ on $E_{p,b}$ is equal to the sum of all elements in $U_p - Q_p$, that is

$$\sum\nolimits_{(x,0)} E_{p,b} = \sum\nolimits_{t\in U_p-Q_p} t. \tag{10}$$

We proved as above that the sum of all elements in Q_p is

$$\frac{p(p-1)(p+1)}{24}.$$

Therefore the sum of all elements in $U_p - Q_p$ is

$$\frac{p(p-1)}{2} - \frac{p(p-1)(p+1)}{24} = \frac{p(p-1)(11-p)}{24}. \tag{11}$$

Applying (10) and (11) we conclude that

$$\begin{aligned}\sum\nolimits_{(x,0)} E_{p,b} &= \sum\nolimits_{t\notin Q_p} t\\ &= \frac{p(p-1)(11-p)}{24}.\end{aligned}$$

■

Theorem 2.8: Let $b \in Q_p$ be a fixed number. Then the order of $E_{p,b}$ over $\mathbf{F}_p$ is

$$\#E_{p,b}(\mathbf{F}_p) = \frac{p-3}{2}$$

for $x \in Q_p$.

Proof: Let $b \in Q_p$ be fixed and let $x \in Q_p$. Recall that the order of an elliptic curve E over a finite field $\mathbf{F}_p$ is given in (1) as

$$\begin{aligned}\#E(\mathbf{F}_p) &= \sum\nolimits_{x\in Q_p}\left(1+\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\right) \qquad (12)\\ &= \sum\nolimits_{x\in Q_p}1+\sum\nolimits_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\sum\nolimits_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right).\end{aligned}$$

Note that the set of b^2x^3's and the set of x^3' s are same when $p \equiv 2(mod\,3)$, that is,

$$\sum\nolimits_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right) = \sum\nolimits_{x\in Q_p}\left(\frac{b^2x^3+b^2}{\mathbf{F}_p}\right).$$

Therefore we can rewrite (12) as

$$\begin{aligned}\#E(\mathbf{F}_p) &= \sum\nolimits_{x\in Q_p}\left(1+\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\right) \qquad (13)\\ &= \sum\nolimits_{x\in Q_p}1+\sum\nolimits_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\sum\nolimits_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\sum\nolimits_{x\in Q_p}\left(\frac{b^2x^3+b^2}{\mathbf{F}_p}\right).\end{aligned}$$

The last sum over $x \in Q_p$ can be rearranged as

$$\begin{aligned}\sum\nolimits_{x\in Q_p}\left(\frac{b^2x^3+b^2}{\mathbf{F}_p}\right) &= \sum\nolimits_{x\in Q_p}\left(\frac{b^2(x^3+1)}{\mathbf{F}_p}\right)\\ &= \left(\frac{b^2}{\mathbf{F}_p}\right)\sum\nolimits_{x\in Q_p}\left(\frac{x^3+1}{\mathbf{F}_p}\right).\end{aligned}$$

Therefore we can rewrite (13) as

$$\begin{aligned}\#E(\mathbf{F}_p) &= \sum\nolimits_{x\in Q_p}\left(1+\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\right) \qquad (14)\\ &= \sum\nolimits_{x\in Q_p}1+\sum\nolimits_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\sum\nolimits_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\sum\nolimits_{x\in Q_p}\left(\frac{b^2x^3+b^2}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\sum\nolimits_{x\in Q_p}\left(\frac{b^2(x^3+1)}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\left(\frac{b^2}{\mathbf{F}_p}\right)\sum\nolimits_{x\in Q_p}\left(\frac{x^3+1}{\mathbf{F}_p}\right).\end{aligned}$$

Note that $b^2 \in Q_p$, that is, $\left(\frac{b^2}{\mathbf{F}_p}\right) = 1$. Therefore (14) becomes

$$\begin{aligned}\#E(\mathbf{F}_p) &= \sum\nolimits_{x\in Q_p}\left(1+\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\right) \qquad (15)\\ &= \sum\nolimits_{x\in Q_p}1+\sum\nolimits_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\sum\nolimits_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\sum\nolimits_{x\in Q_p}\left(\frac{b^2x^3+b^2}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\sum\nolimits_{x\in Q_p}\left(\frac{b^2(x^3+1)}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\left(\frac{b^2}{\mathbf{F}_p}\right)\sum\nolimits_{x\in Q_p}\left(\frac{x^3+1}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\sum\nolimits_{x\in Q_p}\left(\frac{x^3+1}{\mathbf{F}_p}\right).\end{aligned}$$

Note that x takes $\frac{p-1}{2}$ values between 1 and $p-1$ since $x \in Q_p$. So we can rewrite (15) as

$$\begin{aligned}\#E(\mathbf{F}_p) &= \sum\nolimits_{x\in Q_p}\left(1+\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\right) \qquad (16)\\ &= \sum\nolimits_{x\in Q_p}1+\sum\nolimits_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\sum\nolimits_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\sum\nolimits_{x\in Q_p}\left(\frac{b^2x^3+b^2}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\sum\nolimits_{x\in Q_p}\left(\frac{b^2(x^3+1)}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\left(\frac{b^2}{\mathbf{F}_p}\right)\sum\nolimits_{x\in Q_p}\left(\frac{x^3+1}{\mathbf{F}_p}\right)\\ &= \frac{p-1}{2}+\sum\nolimits_{x\in Q_p}\left(\frac{x^3+1}{\mathbf{F}_p}\right)\end{aligned}$$

$$= \frac{p-1}{2} + \sum\nolimits_{1 \le x \le p-1} \left(\frac{x^3+1}{\mathbf{F}_p} \right).$$

On the other hand, $\left(\frac{(p-1)^3+1}{\mathbf{F}_p}\right) = 0$ for $x = p-1$. Hence (16) becomes

$$\begin{aligned}
\#E(\mathbf{F}_p) &= \sum\nolimits_{x \in Q_p} \left(1 + \left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\right) \qquad (17)\\
&= \sum\nolimits_{x \in Q_p} 1 + \sum\nolimits_{x \in Q_p} \left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{x \in Q_p} \left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{x \in Q_p} \left(\frac{b^2x^3+b^2}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{x \in Q_p} \left(\frac{b^2(x^3+1)}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \left(\frac{b^2}{\mathbf{F}_p}\right) \sum\nolimits_{x \in Q_p} \left(\frac{x^3+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{x \in Q_p} \left(\frac{x^3+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{1 \le x \le p-1} \left(\frac{x^3+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{1 \le x \le p-2} \left(\frac{x^3+1}{\mathbf{F}_p}\right).
\end{aligned}$$

We know that all elements of $\mathbf{F}_p$ are cubic residues by Theorem 2.1. Consequently the set of consisting of the values of x^3 is the same with the set of values of x. So we can rewrite (17) as

$$\begin{aligned}
\#E(\mathbf{F}_p) &= \sum\nolimits_{x \in Q_p} \left(1 + \left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\right) \qquad (18)\\
&= \sum\nolimits_{x \in Q_p} 1 + \sum\nolimits_{x \in Q_p} \left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{x \in Q_p} \left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{x \in Q_p} \left(\frac{b^2x^3+b^2}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{x \in Q_p} \left(\frac{b^2(x^3+1)}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \left(\frac{b^2}{\mathbf{F}_p}\right) \sum\nolimits_{x \in Q_p} \left(\frac{x^3+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{x \in Q_p} \left(\frac{x^3+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{1 \le x \le p-1} \left(\frac{x^3+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{1 \le x \le p-2} \left(\frac{x^3+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{1 \le x \le p-2} \left(\frac{x+1}{\mathbf{F}_p}\right).
\end{aligned}$$

It is proved in [1, p.128] that, the number of consecutive pairs of quadratic residues in $\mathbf{F}_p$ is given by formula

$$\eta_p = \frac{(p-4-(-1)^{\frac{p-1}{2}})}{4}. \qquad (19)$$

Hence we have two cases:

Case 1: Let $p \equiv 1 (mod\, 4)$. Then by the Chinese remainder theorem we get $p \equiv 5(mod\, 12)$. So $(-1)^{\frac{p-1}{2}} = 1$. Therefore

$$\eta_p = \frac{p-5}{4} \qquad (20)$$

by (19). Further $-1 \in Q_p$ since $p \equiv 5(mod\, 12)$. So there are

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

values of x between 1 and $p-2$ lying in Q_p. Further $\frac{p-5}{4}$ values of $x+1$ are also in Q_p by (20). Consequently there are $\frac{p-5}{4}$ times $+1$ and $\frac{p-3}{2} - \frac{p-5}{4} = \frac{p-1}{4}$ times -1. So

$$\frac{p-5}{4} - \frac{p-1}{4} = -1.$$

Therefore

$$\sum\nolimits_{1 \le x \le p-2} \left(\frac{x+1}{\mathbf{F}_p}\right) = -1.$$

So (18) becomes

$$\begin{aligned}
\#E(\mathbf{F}_p) &= \sum\nolimits_{x \in Q_p} \left(1 + \left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\right)\\
&= \sum\nolimits_{x \in Q_p} 1 + \sum\nolimits_{x \in Q_p} \left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{x \in Q_p} \left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{x \in Q_p} \left(\frac{b^2x^3+b^2}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{x \in Q_p} \left(\frac{b^2(x^3+1)}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \left(\frac{b^2}{\mathbf{F}_p}\right) \sum\nolimits_{x \in Q_p} \left(\frac{x^3+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{x \in Q_p} \left(\frac{x^3+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{1 \le x \le p-1} \left(\frac{x^3+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{1 \le x \le p-2} \left(\frac{x^3+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} + \sum\nolimits_{1 \le x \le p-2} \left(\frac{x+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2} - 1\\
&= \frac{p-3}{2}.
\end{aligned}$$

Case 2: Let $p \equiv 3(mod\, 4)$. Then by the Chinese reminder theorem we get $p \equiv 11(mod\, 12)$. So $(-1)^{\frac{p-1}{2}} = 1$. Therefore

$$\eta_p = \frac{p-3}{4} \qquad (21)$$

by (19). Further $-1 \notin Q_p$ since $p \equiv 11(mod\, 12)$. So there are

$$\frac{p-1}{2} - 0 = \frac{p-1}{2}$$

values of x between 1 and $p-2$ lying in Q_p since $p-1 \notin Q_p$. Further $\frac{p-3}{4}$ values of $x+1$ are also in Q_p by (21).

Consequently, there are $\frac{p-3}{4}$ times $+1$ and $\frac{p-1}{2}-\frac{p-3}{4}=\frac{p+1}{4}$ times -1. So

$$\frac{p-3}{4}-\frac{p+1}{4}=-1.$$

Therefore

$$\sum_{1\leq x\leq p-2}\left(\frac{x+1}{\mathbf{F}_p}\right)=-1.$$

So (18) becomes

$$\begin{aligned}
\#E(\mathbf{F}_p) &= \sum_{x\in Q_p}\left(1+\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\right)\\
&= \sum_{x\in Q_p}1+\sum_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2}+\sum_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2}+\sum_{x\in Q_p}\left(\frac{b^2x^3+b^2}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2}+\sum_{x\in Q_p}\left(\frac{b^2(x^3+1)}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2}+\left(\frac{b^2}{\mathbf{F}_p}\right)\sum_{x\in Q_p}\left(\frac{x^3+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2}+\sum_{x\in Q_p}\left(\frac{x^3+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2}+\sum_{1\leq x\leq p-1}\left(\frac{x^3+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2}+\sum_{1\leq x\leq p-2}\left(\frac{x^3+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2}+\sum_{1\leq x\leq p-2}\left(\frac{x+1}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2}-1\\
&= \frac{p-3}{2}.
\end{aligned}$$

Hence in two cases we have

$$\#E(\mathbf{F}_p)=\frac{p-3}{2}.$$

■

Now we can give the following theorem for $x\in U_p-Q_p$ without giving its proof since it is similar.

Theorem 2.9: Let $b\in Q_p$ be a fixed number. Then the order of $E_{p,b}$ over $\mathbf{F}_p$ is

$$\#E_{p,b}(\mathbf{F}_p)=\frac{p+3}{2}$$

for $x\in U_p-Q_p$.

Theorem 2.10: Let $p\equiv 5(mod\,6)$ and let $b\in U_p-Q_p$ be a fixed number. Then the order of $E_{p,b}$ over $\mathbf{F}_p$ is

$$\#E_{p,b}(\mathbf{F}_p)=\frac{p-1}{2}$$

for $x\in Q_p$.

Proof: Note that $b\in Q_p$ if and only if $-b\in Q_p$ when $p\equiv 5(mod\,12)$ and $b\in Q_p$ if and only if $-b\in U_p-Q_p$ when $p\equiv 11(mod\,12)$. By (1), we get

$$\begin{aligned}
\#E(\mathbf{F}_p) &= \sum_{x\in Q_p}\left(1+\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\right)\\
&= \frac{p-1}{2}+\sum_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right).
\end{aligned}$$

Case 1: Let $p\equiv 1(mod\,4)$. Then by the Chinese remainder theorem we get $p\equiv 5(mod\,12)$. Then the order Q_p is $\frac{p-1}{2}$ which is an even number. So we have

$$\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)=1$$

for exactly half of the values of $x\in Q_p$, and

$$\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)=-1$$

for exactly other half of the values of $x\in Q_p$. So

$$\sum_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)=0.$$

Therefore

$$\begin{aligned}
\#E(\mathbf{F}_p) &= \sum_{x\in Q_p}\left(1+\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\right)\\
&= \frac{p-1}{2}+\sum_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2}+0\\
&= \frac{p-1}{2}.
\end{aligned}$$

Case 2: Let $p\equiv 3(mod\,4)$. Then by the Chinese reminder theorem we get $p\equiv 11(mod\,12)$. Then $\frac{p-1}{2}$ is odd. It is easily seen that

$$\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)=0$$

for $x=-b$. Further

$$\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)=1$$

for exactly $\frac{p-3}{4}$ values of $x\in Q_p$, and

$$\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)=-1$$

for exactly $\frac{p-3}{4}$ values of $x\in Q_p$. So

$$\sum_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)=0.$$

Therefore

$$\begin{aligned}
\#E(\mathbf{F}_p) &= \sum_{x\in Q_p}\left(1+\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\right)\\
&= \frac{p-1}{2}+\sum_{x\in Q_p}\left(\frac{x^3+b^2}{\mathbf{F}_p}\right)\\
&= \frac{p-1}{2}+0\\
&= \frac{p-1}{2}.
\end{aligned}$$

■

REFERENCES

[1] G.E. Andrews. *Number Theory.* Dover Pub., 1971
[2] A.O.L. Atkin and F. Moralin. *Eliptic Curves and Primality Proving*. Math. Comp. **61** (1993), 29–68.
[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] H.W.Jr. Lenstra. *Factoring Integers with Elliptic Curves.* Annals of Maths. **126**(3) (1987), 649–673.
[6] 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.
[7] R.A. Mollin. *An Introduction to Cryptography.* Chapman&Hall/CRC, 2001.
[8] 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.
[9] R. Schoof. *Counting Points on Elliptic Curves Over Finite Fields.* Journal de Theorie des Nombres de Bordeaux **7**(1995), 219–254.
[10] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1986.
[11] A.Tekcan. *Elliptic Curves* $y^2 = x^3 - t^2x$ *over* $\mathbf{F}_p$. International Journal of Mathematics Sciences **1**(3)(2007), 165-171.
[12] L.C. Washington. *Elliptic Curves, Number Theory and Cryptography.* Chapman&Hall /CRC, Boca London, New York, Washington DC, 2003.
[13] A. Wiles. *Modular Elliptic Curves and Fermat's Last Theorem.* Annals of Maths. **141**(3) (1995), 443–551.