# The Elliptic Curves $y^{2}=x^{3}-t^{2} x$ over $\mathbf{F}_{p}$ 

Ahmet Tekcan


#### Abstract

Let $p$ be a prime number, $\mathbf{F}_{p}$ be a finite field and $t \in$ $\mathbf{F}_{p}^{*}=\mathbf{F}_{p}-\{0\}$. In this paper we obtain some properties of elliptic curves $E_{p, t}: y^{2}=y^{2}=x^{3}-t^{2} x$ over $\mathbf{F}_{p}$. In the first section we give some notations and preliminaries from elliptic curves. In the second section we consider the rational points $(x, y)$ on $E_{p, t}$. We give a formula for the number of rational points on $E_{p, t}$ over $\mathbf{F}_{p}^{n}$ for an integer $n \geq 1$. We also give some formulas for the sum of $x$-and $y$-coordinates of the points $(x, y)$ on $E_{p, t}$. In the third section we consider the rank of $E_{t}: y^{2}=x^{3}-t^{2} x$ and its 2 -isogenous curve $\bar{E}_{t}$ over $\mathbf{Q}$. We proved that the rank of $E_{t}$ and $\bar{E}_{t}$ is 2 over $\mathbf{Q}$. In the last section we obtain some formulas for the sums $\sum_{t \in \mathbf{F}_{p}^{*}} a_{p, t}^{n}$ for an integer $n \geq 1$, where $a_{p, t}$ denote the trace of Frobenius.


Keywords-elliptic curves over finite fields, rational points on elliptic curves, rank, trace of Frobenius.

## I. Introduction

Mordell began his famous paper [13] 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 [6,11,12], for factoring large integers [9], and for primality proving [1,5].The mathematical theory of elliptic curves was also crucial in the proof of Fermat's Last Theorem [19].

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

$$
E_{q, a, b}: y^{2}=x^{3}+a x+b
$$

where $a, b \in \mathbf{F}_{q}$ and $4 a^{3}+27 b^{2} \neq 0$. We can view an elliptic curve $E_{q, a, b}$ as a curve in projective plane $\mathbf{P}^{2}$, with a homogeneous equation $y^{2} z=x^{3}+a x z^{2}+b z^{3}$, and one point at infinity, namely $(0,1,0)$. This point $\infty$ is the point where all vertical lines meet. We denote this point by $O$. Let

$$
\begin{aligned}
E_{q, a, b}\left(\mathbf{F}_{q}\right)= & \left\{(x, y) \in \mathbf{F}_{q} \times \mathbf{F}_{q}: y^{2}=x^{3}+a x+b\right\} \\
& \cup\{O\}
\end{aligned}
$$

denote the set of rational points $(x, y)$ on $E_{q, a, b}$. Then it is a subgroup of $E_{q, a, b}$. The order of $E_{q, a, b}\left(\mathbf{F}_{q}\right)$, denoted by $\# E_{q, a, b}\left(\mathbf{F}_{q}\right)$, is defined as the number of the rational points on $E_{q, a, b}$ (for further details see $[15,17,18]$ ), and is given by

$$
\begin{align*}
\# E_{q, a, b}\left(\mathbf{F}_{q}\right) & =1+\sum_{x \in \mathbf{F}_{q}}\left(1+\frac{x^{3}+a x+b}{\mathbf{F}_{q}}\right)  \tag{1}\\
& =q+1+\sum_{x \in \mathbf{F}_{q}}\left(\frac{x^{3}+a x+b}{\mathbf{F}_{q}}\right)
\end{align*}
$$

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.
where $\left(\dot{\overline{\mathbf{F}_{q}}}\right)$ denotes the Legendre symbol.

$$
\begin{equation*}
\# E_{q, a, b}\left(\mathbf{F}_{q}\right)=q+1-a_{q, a, b} \tag{2}
\end{equation*}
$$

Then $a_{q, a, b}$ is called the trace of Frobenius and satisfies the inequality

$$
\left|a_{q, a, b}\right| \leq 2 \sqrt{q}
$$

known as the Hasse interval [18, p.91]. The formula (1) can be generalized to any field $\mathbf{F}_{q^{n}}$ for an integer $n \geq 2$ [18, p.97]. Let $\# E_{q, a, b}\left(\mathbf{F}_{q}\right)=q+1-a_{q, a, b}$ and let

$$
\begin{equation*}
X^{2}-a_{q, a, b} X+q=(X-\alpha)(X-\beta) \tag{3}
\end{equation*}
$$

Then the order of $E_{q, a, b}$ over $\mathbf{F}_{q^{n}}$ is

$$
\begin{equation*}
\# E_{q, a, b}\left(\mathbf{F}_{q^{n}}\right)=q^{n}+1-\left(\alpha^{n}+\beta^{n}\right) \tag{4}
\end{equation*}
$$

## II. Rational Points on Elliptic Curves

$$
E_{p, t}: y^{2}=x^{3}-t^{2} x \text { OVER } \mathbf{F}_{p}
$$

In [16], we consider the elliptic curves $E_{p, \lambda}: y^{2}=x(x-1)$ $(x-\lambda)$ over $\mathbf{F}_{p}$ for $\lambda \neq 0,1$, where $p$ is a prime number and $\mathbf{F}_{p}$ is a finite field. We consider the rational points on $E_{p, \lambda}$ and also its rank over $\mathbf{Q}$. In the present paper we consider the elliptic curves

$$
\begin{equation*}
E_{p, t}: y^{2}=x^{3}-t^{2} x \tag{5}
\end{equation*}
$$

over $\mathbf{F}_{p}$ for an integer $t \in \mathbf{F}_{p}^{*}$. This elliptic curve was studied by Lemmermeyer and Mollin [8] in the sense of its TateShafarevich group. Here we only consider its rational points, rank and trace of Forbenius.

Let $Q_{p}$ denote the set of quadratic residues. Let $Q_{p}^{4,+}$ denote the set of 4th power of elements of $\mathbf{F}_{p}^{*}$ and let $Q_{p}^{4,-}=\mathbf{F}_{p}^{*}-$ $Q_{p}^{4,+}$. Set $Q_{p}^{4}=Q_{p}^{4,+} \cup Q_{p}^{4,-}$. Then $\# Q_{p}^{4,+}=\# Q_{p}^{4,-}=\frac{p-1}{4}$ and $\# Q_{p}^{4}=\frac{p-1}{2}$. Recall that the order of $E_{p, t}: y^{2}=x^{3}-t^{2} x$ over $\mathbf{F}_{p}$ is given in [18, p.105] by

1. If $p \equiv 3(\bmod 4)$, then $\# E_{p, t}\left(\mathbf{F}_{p}\right)=p+1$.
2. If $p \equiv 1(\bmod 4)$, write $p=a^{2}+b^{2}$, where $a$ and $b$ are integers with $b$ is even and $a+b \equiv 1(\bmod 4)$, then

$$
\# E_{p, t}\left(\mathbf{F}_{p}\right)=\left\{\begin{array}{cl}
p+1-2 a & \text { if } k \in Q_{p}^{4,+} \\
p+1+2 a & \text { if } k \in Q_{p}^{4,-} \\
p+1 \pm 2 b & \text { if } k \notin Q_{p}
\end{array}\right.
$$

First we generalize this result to any field $\mathbf{F}_{p^{n}}$ for an integer $n \geq 2$.

Theorem 2.1: Let $E_{p, t}: y^{2}=x^{3}-t^{2} x$ be an elliptic curve over $\mathbf{F}_{p}$.

1) If $p \equiv 3(\bmod 4)$, then

$$
\# E_{p, t}\left(\mathbf{F}_{p^{n}}\right)= \begin{cases}\left(p^{\frac{n}{2}}-1\right)^{2} & \text { if } n \equiv 0(\bmod 4) \\ p^{n}+1 & \text { if } n \equiv 1,3(\bmod 4) \\ \left(p^{\frac{n}{2}}+1\right)^{2} & \text { if } n \equiv 2(\bmod 4)\end{cases}
$$

2) If $p \equiv 1(\bmod 4)$, then $\# E_{p, t}\left(\mathbf{F}_{p^{n}}\right)=p^{n}+1-$

$$
\begin{cases}(a+i b)^{n}+(a-i b)^{n} & \text { if } t^{2} \in Q_{p}^{4,+} \\ (-a+i b)^{n}+(-a-i b)^{n} & \text { if } t^{2} \in Q_{p}^{4,-}\end{cases}
$$

Proof: 1 . Let $p \equiv 3(\bmod 4)$. Then $\# E_{p, t}\left(\mathbf{F}_{p}\right)=p+1$. Hence $a_{p, t}=0$ by (2). Let

$$
X^{2}+p=(X-\alpha)(X-\beta)
$$

for $\alpha=i \sqrt{p}$ and $\beta=-i \sqrt{p}$ by (3).
Let $n \equiv 0(\bmod 4)$, i.e. $n=4 m$ for an integer $m \geq 1$. Then we get

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

Therefore $\# E_{p, t}\left(\mathbf{F}_{p^{n}}\right)=p^{n}+1-\left(\alpha^{n}+\beta^{n}\right)=p^{n}+1-2 p^{\frac{n}{2}}=$ $\left(p^{\frac{n}{2}}-1\right)^{2}$ by (4).

Let $n \equiv 1(\bmod 4)$, say $n=1+4 m$. Then we get

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

Therefore $\# E_{p, t}\left(\mathbf{F}_{p^{n}}\right)=p^{n}+1-\left(\alpha^{n}+\beta^{n}\right)=p^{n}+1$.
Let $n \equiv 2(\bmod 4)$, say $n=2+4 m$. Then we get

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

Therefore $\# E_{p, t}\left(\mathbf{F}_{p^{n}}\right)=p^{n}+1-\left(\alpha^{n}+\beta^{n}\right)=p^{n}+1+2 p^{\frac{n}{2}}=$ $\left(p^{\frac{n}{2}}+1\right)^{2}$.

Finally, let $n \equiv 3(\bmod 4)$, say $n=3+4 m$. Then we get

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

Therefore $\# E_{p, t}\left(\mathbf{F}_{p^{n}}\right)=p^{n}+1-\left(\alpha^{n}+\beta^{n}\right)=p^{n}+1$.
2. Let $p \equiv 1(\bmod 4)$, and let $t^{2} \in Q_{p}^{4,+}$. Then $\# E_{p, t}\left(\mathbf{F}_{p}\right)=$ $p+1-2 a$ and hence $a_{p, t}=2 a$ by (2). Let

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

Then $2 a=\alpha+\beta$ and $p=\alpha \beta$. Hence we get

$$
\begin{aligned}
2 a=\alpha+\frac{p}{\alpha} & \Leftrightarrow \alpha^{2}-2 a \alpha+p=0 \\
& \Leftrightarrow \alpha_{1,2}=\frac{2 a \pm \sqrt{4 a^{2}-4 p}}{2} \\
& \Leftrightarrow \alpha_{1,2}=a \pm i b .
\end{aligned}
$$

Therefore

$$
\alpha_{1}=a+i b \Rightarrow \beta_{1}=\frac{p}{\alpha_{1}}=a-i b
$$

or

$$
\alpha_{2}=a-i b \Rightarrow \beta_{2}=\frac{p}{\alpha_{2}}=a+i b .
$$

Consequently in both cases, the order of $E_{p, t}$ over $\mathbf{F}_{p^{n}}$ is

$$
\begin{aligned}
\# E_{p, t}\left(\mathbf{F}_{p^{n}}\right) & =p^{n}+1-\left(\alpha^{n}+\beta^{n}\right) \\
& =p^{n}+1-\left[(a+i b)^{n}+(a-i b)^{n}\right] .
\end{aligned}
$$

Let $t^{2} \in Q_{p}^{4,-}$. Then $\# E_{p, t}\left(\mathbf{F}_{p}\right)=p+1+2 a$ and hence $a_{p, t}=-2 a$ by (2). Let

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

Then $-2 a=\alpha+\beta$ and $p=\alpha \beta$. Hence we get

$$
\begin{aligned}
-2 a=\alpha+\frac{p}{\alpha} & \Leftrightarrow \alpha^{2}+2 a \alpha+p=0 \\
& \Leftrightarrow \alpha_{1,2}=\frac{-2 a \pm \sqrt{4 a^{2}-4 p}}{2} \\
& \Leftrightarrow \alpha_{1,2}=-a \pm i b .
\end{aligned}
$$

Therefore

$$
\alpha_{1}=-a+i b \Rightarrow \beta_{1}=\frac{p}{\alpha_{1}}=-a-i b
$$

or

$$
\alpha_{2}=-a-i b \Rightarrow \beta_{2}=\frac{p}{\alpha_{2}}=-a+i b
$$

Consequently the order of $E_{p, t}$ over $\mathbf{F}_{p^{n}}$ is

$$
\begin{aligned}
\# E_{p, t}\left(\mathbf{F}_{p^{n}}\right) & =p^{n}+1-\left(\alpha^{n}+\beta^{n}\right) \\
& =p^{n}+1-\left[(-a+i b)^{n}+(-a-i b)^{n}\right] .
\end{aligned}
$$

This completes the proof.
In the following table some values of $p, a$ and $b$ is given.

| $p$ | $a$ | $b$ | $p$ | $a$ | $b$ |
| :---: | :---: | :---: | :---: | :---: | :---: |
| 5 | 1 | 2 | 229 | 15 | 2 |
| 13 | 3 | 2 | 233 | 13 | 8 |
| 17 | 1 | 4 | 241 | 15 | 4 |
| 29 | 5 | 2 | 257 | 1 | 16 |
| 37 | 1 | 6 | 269 | 13 | 10 |
| 41 | 5 | 4 | 277 | 9 | 14 |
| 53 | 7 | 2 | 281 | 5 | 16 |
| 61 | 5 | 6 | 293 | 17 | 2 |
| 73 | 3 | 8 | 313 | 13 | 12 |
| 89 | 5 | 8 | 317 | 11 | 14 |
| 97 | 9 | 4 | 337 | 9 | 16 |
| 101 | 1 | 10 | 349 | 5 | 18 |
| 109 | 3 | 10 | 353 | 17 | 8 |
| 113 | 7 | 8 | 373 | 7 | 18 |
| 137 | 11 | 4 | 389 | 17 | 10 |
| 149 | 7 | 10 | 397 | 19 | 6 |
| 157 | 11 | 6 | 401 | 1 | 20 |
| 173 | 13 | 2 | 409 | 3 | 20 |
| 181 | 9 | 10 | 421 | 15 | 14 |
| 193 | 7 | 12 | 433 | 17 | 12 |
| 197 | 1 | 14 | 449 | 7 | 20 |

In the following examples the orders of $E_{p, t}: y^{2}=x^{3}-t^{2} x$ over $\mathbf{F}_{p^{n}}$ are given for $2 \leq n \leq 15$.

Example 2.1: Let $p=23$ and $t=2$. Then the order of $E_{23,2}: y^{2}=x^{3}-4 x$ over $\mathbf{F}_{23^{n}}$ is

| $n$ | $\mathbf{F}_{23^{n}}$ |
| :---: | :--- |
| 2 | 576 |
| 3 | 12168 |
| 4 | 278784 |
| 5 | 6436344 |
| 6 | 148060224 |
| 7 | 3404825448 |
| 8 | 78310425600 |
| 9 | 1801152661464 |
| 10 | 41426524086336 |
| 11 | 952809757913928 |
| 12 | 21914624135948544 |
| 13 | 504036361936467384 |
| 14 | 11592836331348400704 |
| 15 | 266635235464391245608 |

Example 2.2: Let $p=13$. Then $a=3$ and $b=2$. Let $t=4$. Then $t^{2} \equiv 3(\bmod 13)$. So $t^{2} \in Q_{13}^{4,+}=\{1,3,9\}$. Then the order of $E_{13,4}: y^{2}=x^{3}-3 x$ over $\mathbf{F}_{13^{n}}$ is

| $n$ | $\mathbf{F}_{13^{n}}$ |
| :---: | :--- |
| 2 | 160 |
| 3 | 2216 |
| 4 | 28800 |
| 5 | 372488 |
| 6 | 4830880 |
| 7 | 62757416 |
| 8 | 815731200 |
| 9 | 10604386564 |
| 10 | 137857808810 |
| 11 | 1792157762000 |
| 12 | 23298078210000 |
| 13 | 302875099300000 |
| 14 | 3937376432000000 |
| 15 | 51185893380000000 |

Similarly let $p=13$ and $t=11$. Then $t^{2} \equiv 4(\bmod 13)$. So $t^{2} \in Q_{13}^{4,-}$. Therefore the order of $E_{13,11}: y^{2}=x^{3}-4 x$ over $\mathbf{F}_{13^{n}}$ is

| $n$ | $\mathbf{F}_{13^{n}}$ |
| :---: | :--- |
| 2 | 160 |
| 3 | 2180 |
| 4 | 28800 |
| 5 | 370100 |
| 6 | 4830880 |
| 7 | 62739620 |
| 8 | 815731200 |
| 9 | 106041612184 |
| 10 | 137857808810 |
| 11 | 1792163026000 |
| 12 | 23298078210000 |
| 13 | 302875113900000 |
| 14 | 3937376432000000 |
| 15 | 51185892640000000 |

Now we consider some properties of rational points on elliptic curve $E_{p, t}$.

Theorem 2.2: Let $[x]$ denote the $x$-coordinates of $(x, y)$ on $E_{p, t}$. Then sum of $[x]$ on $E_{p, t}$ is

$$
\sum_{[x]} E_{p, t}\left(\mathbf{F}_{p}\right)=\sum\left(1+\left(\frac{x^{3}-t^{2} x}{\mathbf{F}_{p}}\right)\right) \cdot x
$$

for all primes $p$
Proof: We know that
$\left(\frac{x^{3}-t^{2} x}{\mathbf{F}_{p}}\right)= \begin{cases}0 & \text { if } x^{3}-t^{2} x \text { is zero } \\ 1 & \text { if } x^{3}-t^{2} x \text { is a square } \\ -1 & \text { if } x^{3}-t^{2} x \text { is not a square } .\end{cases}$
Let $\left(\frac{x^{3}-t^{2} x}{\mathbf{F}_{p}}\right)=0$. Then $x^{3}-t^{2} x=0$, and hence this equation has three solutions $x=0, x=t$ and $x=-t$. Then $y^{2} \equiv 0(\bmod p) \Leftrightarrow y \equiv 0(\bmod p)$. So for such a point $x$, we have a point $(x, 0)$ on $E_{p, t}$. Therefore we get $(x+0) \cdot x=x$ is added to the sum.

Let $\left(\frac{x^{3}-t^{2} x}{\mathbf{F}_{p}}\right)=1$. Then $x^{3}-t^{2} x$ is a square in $\mathbf{F}_{p}$. Let $x^{3}-$ $t^{2} x=k^{2}$ for any $k \in \mathbf{F}_{p}^{*}$. Then $y^{2} \equiv k^{2}(\bmod p) \Leftrightarrow y= \pm k$, that is, for any point $(x, k)$ on $E_{p, t}$, the point $(x,-k)$ is also on $E_{p, t}$. Therefore for each point $x$ we have $(1+1) \cdot x=2 x$ is added to the sum.

Finally, let $\left(\frac{x^{3}-t^{2} x}{\mathbf{F}_{p}}\right)=-1$. Then $x^{3}-t^{2} x$ is not a square in $\mathbf{F}_{p}$. Therefore the equation $y^{2} \equiv x^{3}-t^{2} x(\bmod p)$ has no solution. Therefore for each point $x$, we have $(1+(-1)) \cdot x=0$ as we claimed.

Theorem 2.3: Let $[y]$ denote the $y$-coordinates of $(x, y)$ on $E_{p, t}$.

1) If $p \equiv 3(\bmod 4)$, then the sum of $[y]$ on $E_{p, t}$ is

$$
\sum_{[y]} E_{p, t}\left(\mathbf{F}_{p}\right)=\frac{p^{2}-3 p}{2}
$$

2) If $p \equiv 1(\bmod 4)$, then the sum of $[y]$ on $E_{p, t}$ is

$$
\sum_{[y]} E_{p, t}\left(\mathbf{F}_{p}\right)= \begin{cases}\frac{p^{2}-(2 a+3) p}{2} & \text { if } t^{2} \in Q_{p}^{4,+} \\ \frac{p^{2}+(2 a-3) p}{2} & \text { if } t^{2} \in Q_{p}^{4,-}\end{cases}
$$

Proof: 1 . Let $p \equiv 3(\bmod 4)$. Note that the cubic equation $x^{3}-t^{2} x=0$ has three solutions $x=0, x=t$ and $x=-t$. For the other values of $x$, we have both $x$ and $-x$. One of these gives two points. The one makes $x^{3}-t^{2} x$ a square. So there are two values of $y$ since $y^{2}=x^{3}-t^{2} x$ is square. Let $x^{3}-t^{2} x=k^{2}$ for any $k \in \mathbf{F}_{p}^{*}$. Then we have $y^{2}=k^{2}$ if and only if $y=k$ and $y=-k=p-k$. So the sum of these values of $y$ is $k+(p-k)=p$. We know that there are $\frac{p-3}{2}$ points $x$ such that $y^{2}=x^{3}-t^{2} x$ is a square. Therefore the sum of $y$-coordinates of all points $(x, y)$ is

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

2. Let $p \equiv 3(\bmod 4)$. If $t^{2} \in Q_{p}^{4,+}$, then $E_{p, t}\left(\mathbf{F}_{p}\right)=p+1-$ $2 a$. We know that the cubic equation $x^{3}-t^{2} x=0$ has three solutions $x=0, x=t$ and $x=-t$, that is, there are three points $(0,0),(t, 0),(-t, 0)$ on $E_{p, t}$. The sum of $y$-coordinates of these points is 0 . Further we have to disregard the point $\infty$. Then there are $(p+1-2 a)-4=p-2 a-3$ points $(x, y)$ on

ISSN: 2517-9934
Vol:1, No:1, 2007
$E_{p, t}$ such that $y \neq 0$. Half of these points make $x^{3}-t^{2} x$ a square, that is, there are $\frac{p-2 a-3}{2}$ points $x$ such that $x^{3}-t^{2} x$ is a square. Let $x^{3}-t^{2} x=\stackrel{2}{k^{2}}$ for any $k \in \mathbf{F}_{p}^{*}$. Then we have $y^{2}=k^{2}$ if and only if $y=k$ and $y=-k=p-k$. So the sum of these values of $y$ is $k+(p-k)=p$. Hence the sum of $y$-coordinates of all points $(x, y)$ on $E_{p, t}$ is

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

If $t^{2} \in Q_{p}^{4,-}$, then $E_{p, t}\left(\mathbf{F}_{p}\right)=p+1+2 a$. The cubic equation $x^{3}-t^{2} x=0$ has three solutions $x=0, x=t$ and $x=-t$, that is, there are three points $(0,0),(t, 0),(-t, 0)$ on $E_{p, t}$ and the sum of $y$-coordinates of these points is 0 . Further we have to disregard the point $\infty$. Then there are $(p+1+2 a)-4=p+2 a-3$ points $(x, y)$ on $E_{p, t}$ such that $y \neq 0$. Half of these points make $x^{3}-t^{2} x$ a square, that is, there are $\frac{p+2 a-3}{2}$ points $x$ such that $x^{3}-t^{2} x$ is a square. Let $x^{3}-t^{2} x=k^{2}$ for any $k \in \mathbf{F}_{p}^{*}$. Then we have $y^{2}=k^{2}$ if and only if $y=k$ and $y=-k=p-k$. So the sum of these values of $y$ is $k+(p-k)=p$. Hence the sum of $y$-coordinates of all points $(x, y)$ on $E_{p, t}$ is

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

Theorem 2.4: Let $\mathbf{E}_{p, t}=\left\{E_{p, t}: t \in \mathbf{F}_{p}^{*}\right\}$ denote the set of all elliptic curves $E_{p, t}$ over $\mathbf{F}_{p}$. Then

$$
\sum_{t \in \mathbf{F}_{p}^{*}} \# \mathbf{E}_{p, t}\left(\mathbf{F}_{p}\right)=\frac{p^{2}-1}{2}
$$

for all primes $p$.
Proof: Note that there are $\frac{p-1}{2}$ elliptic curves $E_{p, t}$ in $\mathbf{E}_{p, t}$ over $\mathbf{F}_{p}$. We know that the order of $E_{p, t}$ over $\mathbf{F}_{p}$ is $p+1$ when $p \equiv 3(\bmod 4)$. Therefore the total number of the points $(x, y)$ on all elliptic curves $E_{p, t}$ in $\mathbf{E}_{p, t}$ over $\mathbf{F}_{p}$ is

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

Let $p \equiv 1(\bmod 4)$. If $t^{2} \in Q_{p}^{4,+}$, then the order of $E_{p, t}$ over $\mathbf{F}_{p}$ is $p+1-2 a$, and if $t^{2} \in Q^{4,-}$, then the order of $E_{p, t}$ over $\mathbf{F}_{p}$ is $p+1+2 a$. Further the order of $Q_{p}^{4,+}$ and $Q_{p}^{4,-}$ is $\frac{p-1}{4}$. Therefore the total number of the points $(x, y)$ on all elliptic curves $E_{p, t}$ in $\mathbf{E}_{p, t}$ over $\mathbf{F}_{p}$ is

$$
\begin{aligned}
& \frac{p-1}{4}(p+1-2 a)+\frac{p-1}{4}(p+1+2 a) \\
& =\frac{p-1}{4}(p+1-2 a+p+1+2 a) \\
& =\frac{p-1}{4}(2 p+2) \\
& =\frac{p^{2}-1}{2}
\end{aligned}
$$

as we claimed.
Theorem 2.5: The sum of $[y]$ in $\mathbf{E}_{p, t}\left(\mathbf{F}_{p}\right)$ is

$$
\sum_{t \in \mathbf{F}_{p}^{*}} \mathbf{E}_{p, t}\left(\mathbf{F}_{p}\right)=\frac{p^{3}-4 p^{2}+3 p}{4}
$$

for all primes $p$.
Proof: Let $p \equiv 3(\bmod 4)$. We know that the sum of $[y]$ is $\frac{p^{2}-3 p}{2}$. Further there are $\frac{p-1}{2}$ elliptic curves in $\mathbf{E}_{p, t}$. Therefore the sum of $[y]$ of all points $(x, y)$ on all elliptic curves $E_{p, t}$ in $\mathbf{E}_{p, t}\left(\mathbf{F}_{p}\right)$ is

$$
\left(\frac{p-1}{2}\right)\left(\frac{p^{2}-3 p}{2}\right)=\frac{p^{3}-4 p^{2}+3 p}{4}
$$

Let $p \equiv 1(\bmod 4)$. We know that there are $\frac{p-1}{4}$ elements in both $Q_{p}^{4,+}$ and $Q_{p}^{4,-}$. Further by Theorem 2.3, if $t^{2} \in Q_{p}^{4,+}$, then the the sum of $[y]$ of all points on elliptic curves $E_{p, t}$ is $\frac{p^{2}-(2 a+3) p}{2}$, and if $t^{2} \in Q_{p}^{4,-}$, then the the sum of $[y]$ of all points on elliptic curves $E_{p, t}$ is $\frac{p^{2}+(2 a-3) p}{2}$. Therefore the sum of $[y]$ of all points on elliptic curves $E_{p, t}$ is

$$
\begin{aligned}
& \left(\frac{p-1}{4}\right)\left[\frac{p^{2}-(2 a+3) p}{2}+\frac{p^{2}+(2 a-3) p}{2}\right] \\
& =\left(\frac{p-1}{4}\right)\left(\frac{2 p^{2}-6 p}{2}\right) \\
& =\frac{p^{3}-4 p^{2}+3 p}{4}
\end{aligned}
$$

## III. RANK of $E_{t}: y^{2}=x^{3}-t^{2} x$ Over $\mathbf{Q}$.

Let $E$ be an elliptic curve over $\mathbf{Q}$. By Mordell's theorem, we know that $E(\mathbf{Q})$ is a finitely generated abelian group, that is, $E(\mathbf{Q})=E(\mathbf{Q})_{\text {tors }} \times \mathbf{Z}^{r}$. Further by Mazur's theorem,

$$
E(Q)_{t o r s} \cong \mathbf{Z} / n \mathbf{Z} \text { for } 1 \leq n \leq 10 \text { or } n=12
$$

or

$$
E(Q)_{t o r s} \cong \mathbf{Z} / 2 \mathbf{Z} \times \mathbf{Z} / 2 n \mathbf{Z} \text { for } 1 \leq n \leq 4
$$

On the other hand, it is not known that what values of rank $r$ are possible for elliptic curves over $\mathbf{Q}$. The main idea is that a rank can be arbitrary large. The current record is an example of elliptic curve with rank $\geq 28$, found by Elkies [3] in 2006. The previous record one with rank $\geq 24$, found by Martin and McMillen [10] in 2000. The highest rank of an elliptic curve which is known exactly (not only a lower bound for rank) is equal to 18, and it was found by Elkies [3] in 2006. It improves previous records due to Kretschmer [7](rank = 10), Schneiders-Zimmer [14](rank $=11$ ), Fermigier [4](rank $=14)$, Dujella [2](rank $=15$ ) and Elkies [3](rank $=17$ ).

Recall that the 2 -isogenous curve of an elliptic curve

$$
E_{a, b}: y^{2}=x^{3}+a x^{2}+b x
$$

is given by

$$
\begin{equation*}
\bar{E}_{a, b}: y^{2}=x^{3}+\bar{a} x^{2}+\bar{b} x \tag{6}
\end{equation*}
$$

where $\bar{a}=-2 a$ and $\bar{b}=a^{2}-4 b$. Then there exists a $2-$ isogeny $\phi$ from $E_{a, b}$ to $\bar{E}_{a, b}$ given by

$$
\phi: E_{a, b} \rightarrow \bar{E}_{a, b}, \quad \phi(x, y)=\left(\frac{y^{2}}{x^{2}}, \frac{y\left(b-x^{2}\right)}{x^{2}}\right)
$$

ISSN: 2517-9934
Vol:1, No:1, 2007

Conversely, there exists a dual isogeny $\psi$ from $\bar{E}_{a, b}$ to $E_{a, b}$ given by

$$
\psi: \bar{E}_{a, b} \rightarrow E_{a, b}, \quad \psi(x, y)=\left(\frac{y^{2}}{4 x^{2}}, \frac{y\left(a^{2}-4 b-x^{2}\right)}{8 x^{2}}\right) .
$$

Let

$$
\begin{equation*}
2^{r}=\frac{\# \alpha\left(E_{a, b}(\mathbf{Q})\right) \# \bar{\alpha}\left(\bar{E}_{a, b}(\mathbf{Q})\right)}{4} \tag{7}
\end{equation*}
$$

where $\alpha$ is a homomorphism

$$
\alpha: E_{a, b}(\mathbf{Q}) \rightarrow \mathbf{Q}^{*} / \mathbf{Q}^{* 2}
$$

such that

$$
\begin{aligned}
& 0 \rightarrow 1\left(\bmod \mathbf{Q}^{* 2}\right) \\
& (0,0) \rightarrow b\left(\bmod \mathbf{Q}^{* 2}\right) \\
& (x, y) \rightarrow x\left(\bmod \mathbf{Q}^{* 2}\right),
\end{aligned}
$$

where $\mathbf{Q}^{*}$ is the multiplicative group of rational units, and $\mathbf{Q}^{* 2}$ is the subgroup consisting of perfect squares. So $\mathbf{Q}^{*} / \mathbf{Q}^{* 2}$ is like the non-zero rational numbers, with two elements identified if their quotient is the square of a rational number. We shall call $\alpha$ the Weil map (in fact it is actually a group homomorphism). We found the Weil map from the group of rational points on $E_{a, b}$ to the group $\mathbf{Q}^{*} / \mathbf{Q}^{* 2}$ by studying the rational points on torsors

$$
\begin{equation*}
T^{(\psi)}\left(b_{1}\right): N^{2}=b_{1} M^{4}+a M^{2} e^{2}+b_{2} e^{4} \tag{8}
\end{equation*}
$$

where $b_{1}$ runs through the square free divisors of $b=b_{1} b_{2}$. Then $\alpha\left(E_{a, b}(\mathbf{Q})\right)$ consists of $b\left(\bmod \mathbf{Q}^{* 2}\right)$, together with those $b_{1}\left(\bmod \mathbf{Q}^{* 2}\right)$ such that (8) has a solution $(N, M, e)$.

Similarly, $\bar{\alpha}$ is an Weil map, which is from the group of rational points on $\bar{E}_{a, b}$ to the group $\mathbf{Q}^{*} / \mathbf{Q}^{* 2}$ by studying the rational points on torsors

$$
\begin{equation*}
T^{(\phi)}\left(\bar{b}_{1}\right): N^{2}=\bar{b}_{1} M^{4}+\bar{a} M^{2} e^{2}+\bar{b}_{2} e^{4} \tag{9}
\end{equation*}
$$

where $\bar{b}_{1}$ runs through the square free divisors of $\bar{b}=\bar{b}_{1} \bar{b}_{2}$. Then $\bar{\alpha}\left(\bar{E}_{a, b}(\mathbf{Q})\right)$ consists of $\bar{b}\left(\bmod \mathbf{Q}^{* 2}\right)$, together with those $\bar{b}_{1}\left(\bmod \mathbf{Q}^{* 2}\right)$ such that (9) has a solution $(N, M, e)$.

Note that the 2 -isogenous curve of our curve $E_{t}: y^{2}=$ $x^{3}-t^{2} x$ is

$$
\begin{equation*}
\bar{E}_{t}: y^{2}=x^{3}+4 t^{2} x \tag{10}
\end{equation*}
$$

if $t$ is odd, or

$$
\begin{equation*}
\bar{E}_{t}: y^{2}=x^{3}+\frac{t^{2}}{4} x \tag{11}
\end{equation*}
$$

if $t$ is even by (6). Now we can consider the rank of $E_{t}$ and $\bar{E}_{t}$ over $\mathbf{Q}$.

Theorem 3.1: The rank of $E_{t}$ and $\bar{E}_{t}$ over $\mathbf{Q}$ is 2.
Proof: Elliptic curves with a rational point of order 2 like our curves $E_{t}: y^{2}=x^{3}-t^{2} x$ come attached with a 2-isogeny $\phi: E_{t} \rightarrow \bar{E}_{t}$ (depending of choice of point if $E_{t}$ has three rational points of order 2) as we mentioned above.

Now consider the our elliptic curve $E_{t}: y^{2}=x^{3}-t^{2} x$. Then there are four possibilities for $b_{1}=-t^{2}$ which are $\pm 1$ and $\pm t$.

If $b_{1}=1$, then the equation

$$
N^{2}=M^{4}-t^{2} e^{4}
$$

has a solution $(N, M, e)=\left(t^{2}, t, 0\right)$. If $b_{1}=-1$, then the equation

$$
N^{2}=-M^{4}+t^{2} e^{4}
$$

has a solution $(N, M, e)=(t, 0,-1)$. If $b_{1}=t$, then the equation

$$
N^{2}=t M^{4}-t e^{4}
$$

has a solution $(N, M, e)=\left(0, t^{2}, t^{2}\right)$ and if $b_{1}=-t$, then the equation

$$
N^{2}=-t M^{4}+t e^{4}
$$

has a solution $(N, M, e)=\left(0, t^{2},-t^{2}\right)$. So

$$
\begin{align*}
\alpha\left(E_{t}(\mathbf{Q})\right)= & \left\{ \pm 1, \pm t\left(\bmod \mathbf{Q}^{* 2}\right)\right\} \text { and }  \tag{12}\\
& \# \alpha\left(E_{t}(\mathbf{Q})\right)=4
\end{align*}
$$

by (8).
Now we consider the 2 -isogeny of $E_{t}$. If $t$ is odd, then the 2-isogenous curve of $E_{t}$ is $\bar{E}_{t}: y^{2}=x^{3}+4 t^{2} x$ by (10). Then there are four possibilities for $\bar{b}_{1}=4 t^{2}$ which are $\pm 1$ and $\pm 2 t$.

If $\bar{b}_{1}=1$, then the equation

$$
N^{2}=M^{4}+4 t^{2} e^{4}
$$

has a solution $(N, M, e)=(2 t, 0,1)$. If $\bar{b}_{1}=-1$, then the equation

$$
N^{2}=-M^{4}-4 t^{2} e^{4}
$$

has no solution $(N, M, e)$ since its right-hand side is strictly negative. If $\bar{b}_{1}=2 t$, then the equation

$$
N^{2}=2 t M^{4}+2 t e^{4}
$$

has no solution $(N, M, e)$ and if $\bar{b}_{1}=-2 t$, then the equation

$$
N^{2}=-2 t M^{4}-2 t e^{4}
$$

has no solution $(N, M, e)$ since its right-hand side is strictly negative. Hence
by (9).
If $t$ is even, then the 2-isogenous curve of $E_{t}$ is $\bar{E}_{t}: y^{2}=$ $x^{3}+\frac{t^{2}}{4} x$ by (11). Let $t=2 k$ for integers $k \geq 1$. Then $\bar{E}_{t}$ becomes an elliptic curve has the form $\bar{E}_{t}: y^{2}=x^{3}+k^{2} x$. Then there are four possibilities for $\bar{b}_{1}=k^{2}$ which are $\pm 1$ and $\pm k$.
If $\bar{b}_{1}=1$, then the equation

$$
N^{2}=M^{4}+k^{2} e^{4}
$$

has a solution $(N, M, e)=(k, 0,1)$. If $\bar{b}_{1}=-1$, then the equation

$$
N^{2}=-M^{4}-k^{2} e^{4}
$$

has no solution $(N, M, e)$ since its right-hand side is strictly negative. If $\bar{b}_{1}=k$, then the equation

$$
N^{2}=k M^{4}+k e^{4}
$$

has no solution and if $\bar{b}_{1}=-k$, then the equation

$$
N^{2}=-k M^{4}-k e^{4}
$$

has no solution since its right-hand side is strictly negative. Hence

$$
\bar{\alpha}\left(\bar{E}_{t}(\mathbf{Q})\right)=\left\{1\left(\bmod \mathbf{Q}^{* 2}\right)\right\} \text { and } \# \bar{\alpha}\left(\bar{E}_{t}(\mathbf{Q})\right)=1
$$

by (9). So in both cases, i.e. whether $t$ is even or odd, we have

$$
\begin{align*}
\bar{\alpha}\left(\bar{E}_{t}(\mathbf{Q})\right) & =\left\{1\left(\bmod \mathbf{Q}^{* 2}\right)\right\} \text { and }  \tag{13}\\
& \# \bar{\alpha}\left(\bar{E}_{t}(\mathbf{Q})\right)=1 .
\end{align*}
$$

Applying (12) and (13), we get

$$
\begin{aligned}
2^{r} & =\frac{\# \alpha\left(E_{t}(\mathbf{Q})\right) \cdot \# \bar{\alpha}\left(\bar{E}_{t}(\mathbf{Q})\right)}{4} \\
& =\frac{4.1}{4} \\
& =4 \\
& \Leftrightarrow r=2 .
\end{aligned}
$$

Consequently, the rank of $E_{t}(\mathbf{Q})$ and $\bar{E}_{t}(\mathbf{Q})$ over $\mathbf{Q}$ is 2 by (7) as we claimed.

## IV. Trace of Frobenius of Elliptic Curves

$$
E_{p, t}: y^{2}=x^{3}-t^{2} x
$$

Let $a_{p, t}$ denote the trace of Frobenius of elliptic curve $E_{p, t}$ : $y^{2}=x^{3}-t^{2} x$. Then by (2), we get $\# E_{p, t}\left(\mathbf{F}_{p}\right)=p+1-a_{p, t}$. In this section we will obtain some relations on the sums

$$
\sum_{t \in \mathbf{F}_{p}^{*}} a_{p, t}^{n}
$$

for an integer $n \geq 1$.
Theorem 4.1: Let $a_{p, t}$ denote the trace of Frobenius of elliptic curve $E_{p, t}$.

1) If $p \equiv 3(\bmod 4)$, then

$$
\sum_{t \in \mathbf{F}_{p}^{*}} a_{p, t}^{n}=0
$$

for all integers $n \geq 1$.
2) Let $p \equiv 1(\bmod 4)$, write $p=a^{2}+b^{2}$.
i. If $a+b \equiv 1(\bmod 4)$, then

$$
\sum_{t^{2} \in Q^{4,+}} a_{p, t}^{n}=2^{n-2} a^{n}(p-1)
$$

and

$$
\sum_{t^{2} \in Q^{4,-}} a_{p, t}^{n}=(-1)^{n} 2^{n-2} a^{n}(p-1) .
$$

ii. If $a+b \equiv 3(\bmod 4)$, then

$$
\sum_{t^{2} \in Q^{4,+}} a_{p, t}^{n}=(-1)^{n} 2^{n-2} a^{n}(p-1)
$$

and

$$
\sum_{t^{2} \in Q^{4,-}} a_{p, t}^{n}=2^{n-2} a^{n}(p-1) .
$$

for all integers $n \geq 1$.

Proof: 1. Let $p \equiv 3(\bmod 4)$. Then $E_{p, t}(\mathbf{F})=p+1$. So $a_{p, t}=0$ by (2). Consequently all powers of sums of $a_{p, t}=0$ is 0 , that is

$$
\sum_{t \in \mathbf{F}_{p}^{*}} a_{p, t}^{n}=0
$$

for all integers $n \geq 1$.
2. Let $p \equiv 1(\bmod 4)$ and let $a+b \equiv 1(\bmod 4)$. If $t^{2} \in Q_{p}^{4,+}$ then $a_{p, t}=2 a$ and hence the sum of $a_{p, t}^{n}$ over $t^{2} \in Q_{p}^{4,+}$ is

$$
\begin{aligned}
\sum_{t^{2} \in Q^{4,+}} a_{p, t}^{n} & =\# Q_{p}^{4,+} \cdot \sum_{t^{2} \in Q^{4,+}} a_{p, t}^{n} \\
& =\# Q_{p}^{4,+} \cdot(2 a)^{n} \\
& =\frac{p-1}{4} \cdot 2^{n} a^{n} \\
& =2^{n-2}(p-1) a^{n} .
\end{aligned}
$$

If $t^{2} \in Q_{p}^{4,-}$, then $a_{p, t}=-2 a$ and hence the sum of $a_{p, t}^{n}$ over $t^{2} \in Q_{p}^{4,-}$ is

$$
\begin{aligned}
\sum_{t^{2} \in Q^{4,-}} a_{p, t}^{n} & =\# Q_{p}^{4,-} \cdot \sum_{t^{2} \in Q^{4,-}} a_{p, t}^{n} \\
& =\# Q_{p}^{4,-} \cdot(-2 a)^{n} \\
& =\frac{p-1}{4} \cdot(-1)^{n} 2^{n} a^{n} \\
& =(-1)^{n} 2^{n-2}(p-1) a^{n} .
\end{aligned}
$$

Let $a+b \equiv 3(\bmod 4)$. If $t^{2} \in Q_{p}^{4,+}$, then $a_{p, t}=-2 a$ and hence the sum of $a_{p, t}^{n}$ over $t^{2} \in Q_{p}^{4,+}$ is

$$
\begin{aligned}
\sum_{t^{2} \in Q^{4,+}} a_{p, t}^{n} & =\# Q_{p}^{4,+} \cdot \sum_{t^{2} \in Q^{4,+}} a_{p, t}^{n} \\
& =\# Q_{p}^{4,+} \cdot(-2 a)^{n} \\
& =\frac{p-1}{4} \cdot(-1)^{n} 2^{n} a^{n} \\
& =(-1)^{n} 2^{n-2}(p-1) a^{n} .
\end{aligned}
$$

If $t^{2} \in Q_{p}^{4,-}$, then $a_{p, t}=2 a$ and hence the sum of $a_{p, t}^{n}$ over $t^{2} \in Q_{p}^{4,-}$ is

$$
\begin{aligned}
\sum_{t^{2} \in Q^{4,-}} a_{p, t}^{n} & =\# Q_{p}^{4,-} \cdot \sum_{t^{2} \in Q^{4,-}} a_{p, t}^{n} \\
& =\# Q_{p}^{4,-} \cdot(2 a)^{n} \\
& =\frac{p-1}{4} \cdot 2^{n} a^{n} \\
& =2^{n-2}(p-1) a^{n} .
\end{aligned}
$$

Form above theorem we can give the following theorem
Theorem 4.2: If $p \equiv 1(\bmod 4)$, then

$$
\sum_{t \in \mathbf{F}_{p}^{*}} a_{p, t}^{n}=\left\{\begin{array}{cc}
0 & \text { if } n \text { is odd } \\
2^{n-1} a^{n}(p-1) & \text { if } n \text { is even }
\end{array}\right.
$$

for all integers $n \geq 1$.
Proof: Let $p \equiv 1(\bmod 4)$ and let $a+b \equiv 1(\bmod 4)$. Then we know that

$$
\sum_{t^{2} \in Q^{4,+}} a_{p, t}^{n}=2^{n-2} a^{n}(p-1)
$$

and

$$
\sum_{t^{2} \in Q^{4,-}} a_{p, t}^{n}=(-1)^{n} 2^{n-2} a^{n}(p-1)
$$

If $n$ is odd, then

$$
\begin{aligned}
\sum_{t \in \mathbf{F}_{p}^{*}} a_{p, t}^{n} & =\sum_{t^{2} \in Q^{4,+}} a_{p, t}^{n}+\sum_{t^{2} \in Q^{4,-}} a_{p, t}^{n} \\
& =2^{n-2} a^{n}(p-1)-2^{n-2} a^{n}(p-1) \\
& =0 .
\end{aligned}
$$

If $n$ is even, then

$$
\begin{aligned}
\sum_{t \in \mathbf{F}_{p}^{*}} a_{p, t}^{n} & =\sum_{t^{2} \in Q^{4,+}} a_{p, t}^{n}+\sum_{t^{2} \in Q^{4,-}} a_{p, t}^{n} \\
& =2^{n-2} a^{n}(p-1)+2^{n-2} a^{n}(p-1) \\
& =2\left(2^{n-2} a^{n}(p-1)\right) \\
& =2^{n-1} a^{n}(p-1) .
\end{aligned}
$$

Similarly let $a+b \equiv 3(\bmod 4)$. Then we know that

$$
\sum_{t^{2} \in Q^{4,+}} a_{p, t}^{n}=(-1)^{n} 2^{n-2} a^{n}(p-1)
$$

and

$$
\sum_{t^{2} \in Q^{4,-}} a_{p, t}^{n}=2^{n-2} a^{n}(p-1)
$$

If $n$ is odd, then

$$
\begin{aligned}
\sum_{t \in \mathbf{F}_{p}^{*}} a_{p, t}^{n} & =\sum_{t^{2} \in Q^{4,+}} a_{p, t}^{n}+\sum_{t^{2} \in Q^{4,-}} a_{p, t}^{n} \\
& =-2^{n-2} a^{n}(p-1)+2^{n-2} a^{n}(p-1) \\
& =0 .
\end{aligned}
$$

If $n$ is even, then

$$
\begin{aligned}
\sum_{t \in \mathbf{F}_{p}^{*}} a_{p, t}^{n} & =\sum_{t^{2} \in Q^{4,+}} a_{p, t}^{n}+\sum_{t^{2} \in Q^{4},-} a_{p, t}^{n} \\
& =2^{n-2} a^{n}(p-1)+2^{n-2} a^{n}(p-1) \\
& =2\left(2^{n-2} a^{n}(p-1)\right) \\
& =2^{n-1} a^{n}(p-1) .
\end{aligned}
$$

## References

[1] A.O.L. Atkin and F. Moralin. Eliptic Curves and Primality Proving Math. Comp. 61 (1993), 29-68.
[2] A. Dujella. An Example of Elliptic Curve over Q with Rank Equal to 15. Proc. Japan Acad. Ser. A Math. Sci. 78(2002), 109-111.
[3] N.D. Elkies. Some More Rank Records: $E(\mathbf{Q})=(\mathbf{Z} / 2 \mathbf{Z}) * \mathbf{Z}^{18}$ $(\mathbf{Z} / 4 \mathbf{Z}) * \mathbf{Z}^{12},(\mathbf{Z} / 8 \mathbf{Z}) * \mathbf{Z}^{6},(\mathbf{Z} / 2 \mathbf{Z}) *(\mathbf{Z} / 6 \mathbf{Z}) * \mathbf{Z}^{6}$. Number Theory Listserver, Jun 2006.
[4] S. Fermigier. Exemples de Courbes Elliptiques de Grand Rang sur $\mathbf{Q}(t)$ et sur Q Possedant des points d'ordre 2. C.R. Acad. Sci. Paris Ser. I 322(1996), 949-952.
[5] 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.
[6] N. Koblitz. A Course in Number Theory and Cryptography. SpringerVerlag, 1994.
[7] T.J. Kretschmer. Construction of Elliptic Curves with Large Rank. Math Comp. 46 (1986), 627-635.
[8] F. Lemmermeyer and R.A. Mollin. On the Tate-Shafarevich Groups of $y^{2}=x\left(x^{2}-k^{2}\right)$. Acta Math. Universitatis Comenianae LXXII(1) (2003), 73-80.
[9] H.W.Jr. Lenstra. Factoring Integers with Elliptic Curves. Annals of Maths. 126(3) (1987), 649-673
[10] R. Martin and W. McMillen. An Elliptic Curve Over Q with Rank at least 24. Number Theory Listserver, May 2000.
[11] V.S. Miller. Use of Elliptic Curves in Cryptography, in Advances in Cryptology-CRYPTO'85. Lect. Notes in Comp. Sci. 218, SpringerVerlag, Berlin (1986), 417-426
[12] R.A. Mollin. An Introduction to Cryptography. Chapman\&Hall/CRC, 2001.
[13] 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.
[14] U. Schneiders and H.G. Zimmer. The Rank of Elliptic Curves upon Quadratic Extensions, in: Computational Number Theory. (A. Petho, H.C. Williams, H.G. Zimmer, eds.), de Gruyter, Berlin, 1991.
[15] R. Schoof. Counting Points on Elliptic Curves Over Finite Fields. Journal de Theorie des Nombres de Bordeaux 7(1995), 219-254.
[16] A. Tekcan. The Elliptic Curves $y^{2}=x(x-1)(x-\lambda)$. Accepted by Ars Combinatoria
[17] J.H. Silverman. The Arithmetic of Elliptic Curves. Springer-Verlag, 1986.
18] L.C. Washington. Elliptic Curves, Number Theory and Cryptography Chapman\&Hall /CRC, Boca London, New York, Washington DC, 2003
[19] A. Wiles. Modular Elliptic Curves and Fermat's Last Theorem. Annals of Maths. 141(3) (1995), 443-551.

