THE ELLIPTIC CURVES $y^2 = x(x-1)(x-\lambda)$

AHMET TEKCAN

ABSTRACT. Let p be a prime number and let $\mathbb{F}_p$ be a finite field. In the first section, we give some preliminaries from elliptic curves over finite fields. In the second section we consider the rational points on the elliptic curves $E_{p,\lambda} : y^2 = x(x-1)(x-\lambda)$ over $\mathbb{F}_p$ for primes $p \equiv 3 \pmod 4$, where $\lambda \neq 0, 1$. We proved that the order of $E_{p,\lambda}$ over $\mathbb{F}_p$ is $p+1$ if $\lambda = 2$, $\frac{p+1}{2}$ or $p-1$. Later we generalize this result to $\mathbb{F}_{p^n}$ for any integer $n \geq 2$. Also we obtain some results concerning the sum of x-and y-coordinates of all rational points (x, y) on $E_{p,\lambda}$ over $\mathbb{F}_p$. In the third section, we consider the rank of $E_\lambda : y^2 = x(x-1)(x-\lambda)$ over $\mathbb{Q}$.

AMS Subject Classification 2000: 11G05, 11G07, 11G20, 14H52.
Keywords: Elliptic curves over finite fields, rational points on elliptic curves, rank of elliptic curves.
Date: 13 February 2007.

1. INTRODUCTION.

Mordell began his famous paper [10] 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 [4,8,9], for factoring large integers [7], 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, $\mathbb{F}_q$ be a finite field and let $\overline{\mathbb{F}}_q$ denote the algebraic closure of $\mathbb{F}_q$ with char($\overline{\mathbb{F}}_q$)$\neq 2, 3$. An elliptic curve E over $\mathbb{F}_q$ is defined by an equation

$$E : y^2 = x^3 + ax^2 + bx, \tag{1.1}$$

where $a, b \in \mathbb{F}_q$ and $b^2(a^2 - 4b) \neq 0$. The discriminant of E is defined by $\Delta = 16b^2(a^2 - 4b)$. The condition that $\Delta \neq 0$ is equivalent to the curve being smooth. We can view an elliptic curve E as a curve in projective plane $\mathbb{P}^2$, with a homogeneous equation $y^2z = x^3 + ax^2z^2 + bxz^3$, 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. Then the set of rational points (x,y) on E

$$(1.2) \qquad E(\mathbb{F}_q) = \{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q : y^2 = x^3 + ax^2 + bx\} \cup \{O\}$$

is a subgroup of E. The order of $E(\mathbb{F}_q)$, denoted by $\#E(\mathbb{F}_q) = N$, is defined as the number of the points on E and is given by the following formula:

$$(1.3) \qquad \#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + ax^2 + bx}{\mathbb{F}_q} \right),$$

where $(\frac{\cdot}{\mathbb{F}_q})$ denotes the Legendre symbol (for the arithmetic of elliptic curves and rational points on them see [13,14,15,16]).

Let p be a prime number and let $q = p^n$ for integer $n > 1$. Let $N = q+1-a$ (the integer a is called the trace of Frobenius). Then there is an elliptic curve E defined over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = N$ if and only if $|a| \leq 2\sqrt{q}$, know the Hasse interval, and a satisfies one of the following (see [16, 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 $1 (\text{mod}\, 3)$ 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 $1 (\text{mod}\, 4)$ and $a = 0$
(6) n is odd and $a = 0$

Let $P \in E(\mathbb{F}_q)$. Then the order of P is the smallest positive integer m such that $mP = O$. A fundamental result from group theory is that the order of a point always divides the order of the group $E(\mathbb{F}_q)$. An elliptic curve E over $\mathbb{F}_q$ is called supersingular if there are no points of order q, even with coordinates in an algebraically closed field. For prime $p \geq 5$, E is supersingular if and only if $a = 0$, in which case $\#E(\mathbb{F}_p) = p + 1$.

The formula defined in (1.3) can be generalized to $\mathbb{F}_{q^n}$ for some integer $n \geq 2$. Let $\#E(\mathbb{F}_q) = q + 1 - a$ and let

$$(1.4) \qquad X^2 - aX + q = (X - \alpha)(X - \beta).$$

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

$$(1.5) \qquad \#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$

2. Rational Points on $y^2 = x(x-1)(x-\lambda)$ Over $\mathbb{F}_p$.

It is known that every elliptic curve E over $\mathbb{F}_q$ is isomorphic to an elliptic curve in Legendre form $E_\lambda : y^2 = x(x-1)(x-\lambda)$ for some $\lambda \in \overline{\mathbb{F}}_q$ with $\lambda \neq 0, 1$. Let p be a odd prime and let $\mathbb{F}_p$ be a finite field, and let $\lambda \in \overline{\mathbb{F}}_p$ with $\lambda \neq 0, 1$. In this section we consider the number of rational points on elliptic curve

$$E_{p,\lambda} : y^2 = x(x-1)(x-\lambda) \tag{2.1}$$

over $\mathbb{F}_p$. When $p \equiv 1 (\mathrm{mod}\, 4)$, there is no rule. Therefore we only consider the case $p \equiv 3 (\mathrm{mod}\, 4)$.

Theorem 2.1. *If $\lambda = 2, \frac{p+1}{2}$ or $p-1$, then the order of $E_{p,\lambda}$ over $\mathbb{F}_p$ is $p+1$, that is, $E_{p,\lambda}$ is supersingular.*

Proof. Let $\lambda = 2, \frac{p+1}{2}$ or $p-1$ and let $x \in \mathbb{F}_p$ be any point. Now consider the cubic equation

$$x(x-1)(x-\lambda) = 0.$$

This equation has three solutions $x = 0, x = 1$ and $x = \lambda$. Therefore we have $y^2 \equiv 0 (\mathrm{mod}\, p) \Leftrightarrow y \equiv 0 (\mathrm{mod}\, p)$, that is, there are three points $(0,0), (1,0)$ and $(\lambda, 0)$ on $E_{p,\lambda}$. Therefore for these values of x, we have

$$\left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_q}\right) = 0.$$

Set $\mathbb{F}_p^0 = \{0, 1, \lambda\}$. Then $x(x-1)(x-\lambda)$ is zero for $x \in \mathbb{F}_p^0$. So we get

$$\sum_{x \in \mathbb{F}_p^0} \left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right) = 0. \tag{2.2}$$

For the other values of x, i.e. $x \in \mathbb{F}_p - \mathbb{F}_p^0$, we have both x and $-x$. Each of these values gives two points, the one makes $x(x-1)(x-\lambda)$ a square, i.e.

$$\left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right) = 1.$$

So there are two values of y since $y^2 = x(x-1)(x-\lambda)$ is a square. There are $\frac{p-3}{2}$ (since $\#(\mathbb{F}_p - \mathbb{F}_p^0) = \frac{p-3}{2}$) points x in $\mathbb{F}_p - \mathbb{F}_p^0$ such that $x(x-1)(x-\lambda)$ is a square. Let $\mathbb{F}_p^+$ denote the set of the points x in $\mathbb{F}_p$ such that $x(x-1)(x-\lambda)$ is a square. Then we get

$$\sum_{x \in \mathbb{F}_p^+} \left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right) = \frac{p-3}{2}. \tag{2.3}$$

The other value gives no points since

$$\left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right) = -1.$$

So there are no values of y since $y^2 = x(x-1)(x-\lambda)$ is not a square. There are $\frac{p-3}{2}$ points x such that $x(x-1)(x-\lambda)$ is not a square. Let $\mathbb{F}_p^-$ denote the set of the points x in $\mathbb{F}_p$ such that $x(x-1)(x-\lambda)$ is not a square. Then we get

$$\sum_{x\in\mathbb{F}_p^-}\left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right) = -\frac{p-3}{2}. \tag{2.4}$$

Applying (2.2), (2.3) and (2.4), we get

$$\begin{aligned}\sum_{x\in\mathbb{F}_p}\left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right) &= \sum_{x\in\mathbb{F}_p^0\cup\mathbb{F}_p^+\cup\mathbb{F}_p^-}\left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right)\\ &= 0+\frac{p-3}{2}-\frac{p-3}{2}\\ &= 0.\end{aligned}$$

Therefore the order of $E_{p,\lambda}$ over $\mathbb{F}_p$ is $p+1$ since

$$\#E_{p,\lambda}(\mathbb{F}_p) = p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right) = p+1$$

by (1.3). □

Example 2.1. *Let $p = 11$. Then we have the following table for elliptic curves $E_{11,\lambda}: y^2 = x(x-1)(x-\lambda)$ over $\mathbb{F}_{11}$:*

λ	$E_{11,\lambda}$	$\#E_{11,\lambda}(\mathbb{F}_{11})$
2	$y^2 = x^3 - 3x^2 + 2x$	12
3	$y^2 = x^3 - 4x^2 + 3x$	16
4	$y^2 = x^3 - 5x^2 + 4x$	16
5	$y^2 = x^3 - 6x^2 + 5x$	8
6	$y^2 = x^3 - 7x^2 + 6x$	12
7	$y^2 = x^3 - 8x^2 + 7x$	16
8	$y^2 = x^3 - 9x^2 + 8x$	8
9	$y^2 = x^3 - 10x^2 + 9x$	8
10	$y^2 = x^3 - 11x^2 + 10x$	12

It is clear that $E_{11,2}, E_{11,6}$ and $E_{11,10}$ are supersingular elliptic curves since their orders are 12.

From now on we assume that $\lambda = 2, \frac{p+1}{2}$ or $p-1$ throughout the paper. Now we generalize Theorem 2.1 to $\mathbb{F}_{p^n}$ for integer $n \geq 2$.

Theorem 2.2. *The order of $E_{p,\lambda}$ over $\mathbb{F}_{p^n}$ is*

$$\#E_{p,\lambda}(\mathbb{F}_{p^n}) = \begin{cases} (p^{\frac{n}{2}}-1)^2 & \text{if } n \equiv 0 \pmod 4) \\ p^n+1 & \text{if } n \equiv 1,3 \pmod 4) \\ (p^{\frac{n}{2}}+1)^2 & \text{if } n \equiv 2 \pmod 4). \end{cases}$$

Proof. We know that $E_{p,\lambda}$ is supersingular, that is $\#E_{p,\lambda}(\mathbb{F}_p) = p+1$. Therefore $a = 0$. Then by (1.4), we get

$$X^2 + p = (X - i\sqrt{p})(X + i\sqrt{p}).$$

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

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

Therefore by (1.5), we get

$$\#E_{p,\lambda}(\mathbb{F}_{p^n}) = p^n + 1 - (\alpha^n + \beta^n) = p^n + 1 - 2p^{\frac{n}{2}} = (p^{\frac{n}{2}} - 1)^2.$$

Similarly, it can be shown that $\#E_{p,\lambda}(\mathbb{F}_{p^n}) = p^n + 1$ if $n \equiv 1, 3 (\bmod 4)$ and $\#E_{p,\lambda}(\mathbb{F}_{p^n}) = (p^{\frac{n}{2}} + 1)^2$ if $n \equiv 2 (\bmod 4)$. □

Example 2.2. *Let $p = 19$ and $\lambda = 20$. Then the order of $E_{19,10} : y^2 = x^3 - 11x^2 + 10x$ over $\mathbb{F}_{19^n}$ is*

$$\#E_{19,10}(\mathbb{F}_{19^n}) = \begin{cases} 16983302400 & \text{for } n = 8 \\ 322687697780 & \text{for } n = 9 \\ 116490258898220 & \text{for } n = 11 \\ 6131071210000 & \text{for } n = 10. \end{cases}$$

Let $[x]$ and $[y]$ denote the $x-$and $y-$coordinates of all points (x, y) on $E_{p,\lambda} : y^2 = x(x-1)(x-\lambda)$, respectively. Then we can give the following results concerning the sum of $[x]$ and $[y]$.

Theorem 2.3. *The sum of $x-$coordinates on $E_{p,\lambda}$ is*

$$\sum_{[x]} E_{p,\lambda}(\mathbb{F}_p) = \sum_{[x]} \left(1 + \left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right)\right).x$$

Proof. Recall that

$$1+\left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right)=\begin{cases}1 & \text{if } x(x-1)(x-\lambda) \text{ is zero in } \mathbb{F}_p\\ 2 & \text{if } x(x-1)(x-\lambda) \text{ is a square in } \mathbb{F}_p\\ 0 & \text{if } x(x-1)(x-\lambda) \text{ is not a square in } \mathbb{F}_p.\end{cases}$$

Let $\left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right)=0$. Then $x(x-1)(x-\lambda)$ is zero in $\mathbb{F}_p$. Hence the equation $x(x-1)(x-\lambda)=0$ has three solutions $x=0,1,\lambda$. Therefore $y^2\equiv 0(\bmod p)\Leftrightarrow y\equiv 0(\bmod p)$. So for such a point $x\in\mathbb{F}_p^0$, we have a point $(x,0)$ on $E_{p,\lambda}$. Therefore we get $(x+0).x=x$ is added to the sum.

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

Finally, let $\left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right)=-1$. Then $x(x-1)(x-\lambda)$ is not a square in $\mathbb{F}_p$. Therefore the equation $y^2\equiv x(x-1)(x-\lambda)(\bmod p)$ has no solution. Hence for each point (x,y) we have $(1+(-1)).x=0$. This completes the proof. □

Theorem 2.4. *The sum of $y-$coordinates on $E_{p,\lambda}$ is*

$$\sum_{[y]}E_{p,\lambda}(\mathbb{F}_p)=\frac{p^2-3p}{2}.$$

Proof. We proved in Theorem 2.1 that the cubic equation $x(x-1)(x-\lambda)=0$ has three solutions $x=0, x=1$ and $x=\lambda$. We also proved that for the other values of x, i.e. $x\in\mathbb{F}_p-\mathbb{F}_p^0$, we have both x and $-x$. One of these gives two points. The one makes $x(x-1)(x-\lambda)$ a square, i.e. $\left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right)=1$. So there are two values of y since $y^2=x(x-1)(x-\lambda)$ is a square. Let $x\in\mathbb{F}_p^+$, then $x(x-1)(x-\lambda)=t^2$ for any $t\in\mathbb{F}_p^*$. Then we have $y^2\equiv t^2(\bmod p)\Leftrightarrow y\equiv\pm t(\bmod p)$, that is $y=t$ and $y=-t=p-t$. The sum of these values of y is $t+(p-t)=p$. We know that there are $\frac{p-3}{2}$ points $x\in\mathbb{F}_p^+$ such that $y^2=x(x-1)(x-\lambda)$ is a square. Therefore, the sum of $y-$coordinates of all points (x,y) on $E_{p,\lambda}$ is $p\frac{p-3}{2}$. Hence we conclude that the sum of $[y]$ on $E_{p,\lambda}$ is $\frac{p^2-3p}{2}$. □

Theorem 2.5. *Let $\mathbb{E}_{p,\lambda}$ denote the set of the family of all supersingular elliptic curves over $\mathbb{F}_p$, i.e. $\mathbb{E}_{p,\lambda}=\{E_{p,\lambda}:\lambda=2,\frac{p-1}{2},p-1\}$. Then*

$$\sum_{\lambda}\#\mathbb{E}_{p,\lambda}=3p+3.$$

Proof. We know that there are three supersingular elliptic curves $E_{p,\lambda} : y^2 = x(x-1)(x-\lambda)$ over $\mathbb{F}_p$. We also proved in Theorem 2.1 that the order of $E_{p,\lambda}$ over $\mathbb{F}_p$ is $p+1$, i.e. $\#E_{p,\lambda}(\mathbb{F}_p) = p+1$. Therefore the total number of the points (x,y) on all elliptic curves $E_{p,\lambda}$ in $\mathbb{E}_{p,\lambda}$ over $\mathbb{F}_p$ is $\mathbb{N}_{p,\lambda} = 3(p+1)$. □

3. Rank of $E_\lambda : y^2 = x(x-1)(x-\lambda)$ Over $\mathbb{Q}$.

Ranks of elliptic curves have an important role on the theory of elliptic curves and are studied by many authors (see [2,5,6,11,12]). Recall that the quadratic twist of an elliptic curve $E : y^2 = x^3 + ax^2 + bx$ is $E^{(d)} : dy^2 = x^3 + ax^2 + bx$. In this section we consider the rank of elliptic curve $E : y^2 = x(x-1)(x-\lambda)$ over $\mathbb{Q}$ for $\lambda \in \mathbb{Q} - \{0,1\}$. First we give the following Lemmas from [12].

Lemma 3.1. *Suppose that E is an elliptic curve over a field $\mathbb{F}$, that $K_1, K_2, \cdots, K_n$ are distinct separable extensions of $\mathbb{F}$ of degree at most 2, and that for $i = 1, 2, \cdots, n$, there are points $P_i \in E(K_i)$ of infinite order. Suppose also that if $K_i \neq \mathbb{F}$, then $\sigma(P_i) = -P_i$, where σ is the non-trivial element of $Gal(K_i/\mathbb{F})$. Let K denote the compositum $K_1K_2\cdots K_n$. Then $\{P_1, P_2, \cdots, P_n\}$ is an independent set in $E(K)$.*

Now let $k(z) \in \mathbb{Z}[z]$. We say that $k(z)$ is square free if $k(z)$ is not divisible by the square of any non-constant polynomial in $\mathbb{Z}[z]$. Let $g(z) \in \mathbb{Q}[z]$. A square free part of $g(z)$ is a square free $k(z) \in \mathbb{Z}[z]$ such that $g(z) = k(z)j^2(z)$ for some $j(z) \in \mathbb{Q}[z]$. Let $\mathbb{Q}^*$ denote the multiplicative group of rational units, and let $\mathbb{Q}^{*2}$ denote the subgroup consisting of perfect squares. Then we can give the following Lemma.

Lemma 3.2. *Suppose $f(x) \in \mathbb{Q}[x]$ is a separable cubic, and let E is the elliptic curve $E : y^2 = f(x)$. Let $h_1(z) = z$, suppose we have non-constant $h_2(z), h_3(z), \cdots, h_r(z) \in \mathbb{Q}[z]$, let $k_i(z)$ be a square free part of $\frac{f(h_i(z))}{f(z)}$, and suppose that $k_1(z), k_2(z), \cdots, k_r(z)$ are distinct modulo $\mathbb{Q}^{*2}$. Then the rank of $E^{(f(z))}\left(\mathbb{Q}\left(z, \sqrt{k_2(z)}, \cdots, \sqrt{k_r(z)}\right)\right)$ is at least r and if C is the curve defined by the equations $s_i^2 = k_i(z)$ for $i = 1, 2, \cdots, r$, then for all but at most finitely many rational points $(\tau, \sigma_1, \sigma_2, \cdots, \sigma_r) \in C(\mathbb{Q})$, the rank of $E^{(f(\tau))}(\mathbb{Q})$ is at least r.*

In Lemma 3.2, h_i is a linear fractional transformation that permutes the roots of f. Hence $k_i(z)$ is linear. Further $k_1(z) = 1$ and if $h_i(z) = \frac{\alpha z+\beta}{z+\delta}$ with $\alpha, \beta, \delta \in \mathbb{Q}$, then $k_i(z) = f(\alpha)(z+\delta)$ and

$$\frac{f(h_i(z))}{f(z)} = \frac{k_i(z)}{(z+\delta)^4}.$$

Let $E : y^2 = x(x-1)(x-\lambda)$ be an elliptic curve over $\mathbb{Q}$ and let

$$\begin{aligned}
h_1(z) &= z \\
h_2(z) &= \frac{z-\lambda}{(2-\lambda)z-1} \\
h_3(z) &= \frac{\lambda^2(z-1)}{(\lambda^2-\lambda+1)z-\lambda} \\
h_4(z) &= \frac{\lambda z}{(\lambda+1)z-\lambda} \\
h_5(z) &= \frac{\lambda^2(z-1)}{z(2\lambda-1)-\lambda^2} \\
h_6(z) &= \frac{\lambda(2-\lambda)}{(\lambda^2-\lambda+1)z-\lambda^2}
\end{aligned} \tag{3.1}$$

be the linear fractional transformations in $\mathbb{Q}[z]$ that permutes the set $\{0, 1, \lambda\}$. Then the square parts of h_i in $\mathbb{Q}[z]$ are

$$\begin{aligned}
k_1(z) &= 1 \\
k_2(z) &= (1-\lambda)\left[(\lambda-2)z+1\right] \\
k_3(z) &= \lambda(1-\lambda)\left[(\lambda^2-\lambda+1)z-\lambda\right] \\
k_4(z) &= \lambda\left[(\lambda+1)z-\lambda\right] \\
k_5(z) &= \lambda(\lambda-1)\left[(1-2\lambda)z+\lambda^2\right] \\
k_6(z) &= \lambda(1-\lambda)\left[(\lambda^2-\lambda+1)z-\lambda^2\right].
\end{aligned} \tag{3.2}$$

Theorem 3.1. *Let $t \in \mathbb{Q} - \{0, \pm 1\}$, and let $k = t^2$. Let*

$$f_k(x) = x(x-1)\left(x - \frac{1-k}{k+2}\right) \tag{3.3}$$

and let $E_k : y^2 = f_k(x)$. Set $w_k(u) = \frac{2(1-k)W_k(u)}{3[(k+1)u^2+1-k^3]^2}$ for $W_k(u) = (k+1)^2u^4 + 2k(2k^2+3k+1)u^3 + 2(3k^4+3k^3+k^2+k+1)u^2 + 2k(k^3-1)(2k+1)u + k^6 - 2k^3 + 1$. Let $\widetilde{E}_k : v^2 = (k+1)^2u^4 + 4k(2k^2+3k+1)u^3 + 2(7k^4+7k^3+2k^2+k+1)u^2 + 4(2k^5+k^4-2k^2-k)u + (k^3-1)^2$. Then E_k and $\widetilde{E}_k$ are elliptic curves over $\mathbb{Q}$, rank$(\widetilde{E}_k(\mathbb{Q})) \geq 1$, for all but possibly finitely many $(u, v) \in \widetilde{E}_k(\mathbb{Q})$, the quadratic twist of E_k by $(f_k \circ w_k)(u)$ has rank at least 4 over $\mathbb{Q}$ and there are infinitely many non-isomorphic quadratic twists of E_k of rank at least 4 over $\mathbb{Q}$.

Proof. Let $\mu = \frac{2\lambda}{\lambda+1}$. Then by (3.2) we get

$$(3.4) \qquad \begin{aligned} \frac{k_3(\mu)}{k_2(\mu)} &= \frac{\lambda(1-\lambda)\left[(\lambda^2-\lambda+1).\frac{2\lambda}{\lambda+1}-\lambda\right]}{(1-\lambda)\left[(\lambda-2).\frac{2\lambda}{\lambda+1}+1\right]} \\ &= \frac{\lambda(1-\lambda)\left[\frac{2\lambda^3-2\lambda^2+2\lambda-\lambda^2-\lambda}{\lambda+1}\right]}{(1-\lambda)\left[\frac{2\lambda^2-4\lambda+\lambda+1}{\lambda+1}\right]} \\ &= \frac{\lambda(2\lambda^3-3\lambda^2+\lambda)}{2\lambda^2-3\lambda+1} \\ &= \frac{\lambda\left[\lambda(2\lambda^2-3\lambda+1)\right]}{2\lambda^2-3\lambda+1} \\ &= \lambda^2 \end{aligned}$$

and also

$$(3.5) \qquad \begin{aligned} k_2(\mu) &= (1-\lambda)\left[(\lambda-2).\frac{2\lambda}{\lambda+1}+1\right] \\ &= \frac{(\lambda-1)^2(-2\lambda+1)}{\lambda+1}. \end{aligned}$$

Let $\frac{-2\lambda+1}{\lambda+1} = t^2$. Then $\frac{-2\lambda+1}{\lambda+1} = t^2 \Leftrightarrow \lambda = \frac{1-t^2}{2+t^2}$ which is in (3.3). So if $\lambda = \frac{1-t^2}{2+t^2}$, then $k_2(\mu)$ and $k_3(\mu)$ are both squares. Therefore $(\mu, (\lambda-1)t, \lambda(\lambda-1)t) \in \widetilde{E}_{t^2}$ and $\mathbb{Q}\left(z, \sqrt{k_2(z)}, \sqrt{k_3(z)}\right) \in \mathbb{Q}(u)$ since k_2 and k_3 are both squares. Note that the curve $\widetilde{E}_k$ is the curve $v^2 = k_4(w_k(u))$ and also $(0, k^3-1) \in \widetilde{E}_k(\mathbb{Q})$. So $\mathbb{Q}(\widetilde{E}_k) = \mathbb{Q}\left(u, \sqrt{k_4(w_k(u))}\right) = \mathbb{Q}\left(z, \sqrt{k_2(z)}, \sqrt{k_3(z)}, \sqrt{k_4(z)}\right)$ by Lemma 3.2 and hence the rank of $E_k^{(f_k \circ w_k)(u)}(\mathbb{Q}(\widetilde{E}_k))$ is at least 4. Also the rank of $E_k^{(f_k \circ w_k)(u)}(\mathbb{Q})$ is at least 4 for all but infinitely many $(u,v) \in \widetilde{E}_k(\mathbb{Q})$. Let $f_k \circ h_i(z) = f_k(z)k_i(z)j_i^2(z)$, where $j_i(z) \in \mathbb{Q}[z]$ for $i = 1,2,3,4$. Since $k_i(z)$ is square free parts of $h_i(z)$, the points on $E_k^{(f_k \circ w_k)(u)}(\mathbb{Q}(u,v))$ are

$$\begin{aligned} &(w_k(u), 1), \\ &\left(h_1 \circ w_k(u), \left(\frac{-(k+1)u^2+k^3-1}{t\left[(k+1)u^2+2(k^2-1)u+k^3-1\right]}\right)^3\right), \\ &\left(h_2 \circ w_k(u), \left(\frac{-(k+1)u^2+k^3-1}{t\left[(k+1)u^2+2(k^2+k+1)u+k^3-1\right]}\right)^3\right), \\ &\left(h_3 \circ w_k(u), \left(\frac{-(k+1)u^2+k^3-1}{v}\right)^3\right). \end{aligned}$$

Note that these four points are independent points in $E_k^{(f_k \circ w_k)(u)}(\mathbb{Q}(\widetilde{E}_k))$ by Lemma 3.1.

Let $\widetilde{E}_k^* : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ be an elliptic curve for $\alpha = -2(k^2-1)(k^2+k+1), \beta = -2(k^2-1)(3k^2+k-1)$ and $\gamma = -2(k^2+k+1)(3k^2+2k+1)$. Then $\widetilde{E}_k^*$ is a Weierstrass model for $\widetilde{E}_k$. Therefore there is a birational isomorphism ϑ from $\widetilde{E}_k$ to $\widetilde{E}_k^*$ given by

$$\vartheta : \widetilde{E}_k(\mathbb{Q}) \to \widetilde{E}_k^*(\mathbb{Q})$$

such that $\vartheta(0, k^3-1) = I$, identity element of $\widetilde{E}_k^*(\mathbb{Q})$ and $\vartheta(\widetilde{P}_k) = \widetilde{P}_k^*$, where $\widetilde{P}_k = ((t+1)(k+t+1), -(t+1)(k+t+1)(k+2)(tk-2k+1))$ and $\widetilde{P}_k^* = (2(k^3-1), 8tk(k+2)(k^3-1))$. It is easily seen that the denominator of the x-coordinates of $n\widetilde{P}_k^*$ has no non-zero rational roots for $n = 2,3,4,5,6,7,8,9$ and 12. Therefore $\widetilde{P}_k^*$ has infinite order for every $t \in \mathbb{Q} - \{0, \pm 1\}$.

Let $k \in \mathbb{Q} - \{0,1\}$ is the square of a rational number. Then $(f_k \circ w_k)(u)$ is always separable, so for each square $s \in \mathbb{Z}$, the hyperelliptic curve $(f_k \circ w_k)(u) = st^2$ has genus 5, and thus has only finitely many rational solutions (u, z), that is, for each such k and s differ by a rational square is finite. Therefore for each w, there are infinitely many non-isomorphic quadratic twists of E_k of rank at least 4 over $\mathbb{Q}$ since $\widetilde{E}_k(\mathbb{Q})$ is infinite. □

References

[1] A.O.L. Atkin and F. Moralin. *Eliptic Curves and Primality Proving.* Math. Comp. **61** (1993), 29–68.

[2] A. Brumer and K. Kramer. *The Rank of Elliptic Curves.* Duke Math. Journal **44**(1977), 715–743.

[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] T.J. Kretschmer. *Construction of Elliptic Curves with Large Rank.* Math. Comp. **46** (1986), 627–635.

[6] F. Lemmermeyer and R.A. Mollin. *On the Tate-Shafarevich Groups of $y^2 = x(x^2-k^2)$.* Acta Math. Universitatis Comenianae LXXII(1)(2003), 73–80.

[7] H.W.Jr. Lenstra. *Factoring Integers with Elliptic Curves.* Annals of Maths. **126**(3) (1987), 649–673.

[8] 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.

[9] R.A. Mollin. *An Introduction to Cryptography.* Chapman&Hall/CRC, 2001.

[10] L.J. Mordell. *On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degrees.* Proc. Cambridge Philos. Soc. **21**(1922), 179–192.

[11] K. Nagao. *Construction of High-Rank Elliptic Curves.* Kobe J. Math. **11**(1994), 211–219.

[12] K. Rubin and A. Silverberg. *Rank Frequencies for Quadratic Twists of Elliptic Curves.* Experimental Math. **10**(2001), 559–569.

[13] R. Schoof. *Counting Points on Elliptic Curves Over Finite Fields.* Journal de Theorie des Nombres de Bordeaux **7**(1995), 219–254.

[14] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.
[15] J.H. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics, Springer, 1992.
[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.

Uludag University, Faculty of Science, Department of Mathematics, Görükle, 16059, Bursa-TURKEY

E-mail address: tekcan@uludag.edu.tr

URL: http://matematik.uludag.edu.tr/AhmetTekcan.htm