Werk

Titel: Q(T)-rank of elliptic curves and certain limit coming from the local points.

Autor: Nagao, Koh-ichi

Jahr: 1997

PURL: https://resolver.sub.uni-goettingen.de/purl?365956996_0092|log5

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

manuscripta math. 92, 13 - 32 (1997)

manuscripta mathematica
© Springer-Verlag 1997

$\mathbb{Q}(T)$-rank of elliptic curves and certain limit coming from the local points

Koh-ichi Nagao

Shiga Polytechnic College, 1414 Furukawa cho Oh-mihachiman city Shiga 523 Japan

Received December 15, 1995;
in revised form August 18, 1996

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$. For a prime number p, denote by $N_p(E)$ the number of rational points on the non-singular part of the curve over $\mathbb{F}_p$ obtained from E by the reduction modulo p. Put

$$a_p(E) = p + 1 - N_p(E).$$

Then for a positive integer N, in the previous paper [7], we defined a real number $s(N, E)$ by

$$s(N, E) = -\frac{1}{N} \sum_{p:primes \leq N} a_p(E) \cdot \log p.$$

We used this number $s(N, E)$ as a sort of measure of rank of E and found some elliptic curves of rank ≥ 21. Experimentally, we know, it is a number approximate to the rank of E for a sufficiently large N. However it does not seem that the number $s(N, E)$ has a limit as $N \to \infty$. For certain kind of elliptic curves $\mathcal{E}$ defined over the rational function field $\mathbf{Q}(T)$ of a variable T, we may define a number $S(N, \mathcal{E})$ similar to $s(N, E)$ as follows.

Let $\mathcal{E}$ be an elliptic curve defined by a Weierstrass equation with $\mathbb{Z}[T]$-coefficients. For an integer t, denote by E_t the curve defined over $\mathbb{Z}$ obtain from $\mathcal{E}$ by the specialization: $T \to t$. Let p be a prime. Then we can obtained the curve $E_{t,p}$ defined over $\mathbb{F}_p$ by reducing the coefficients of the equation of E_t modulo p. We denote by $E_t(\mathbb{F}_p)$ the set of $\mathbb{F}_p$-rational points on $E_{t,p}$ including the point at the infinity. For $\mathcal{E}$, a prime p, and a positive integer N, we define

Correspondence to: nagao@shiga-pc.ac.jp

$$a_p(E_t) = p + 1 - \#E_t(\mathbb{F}_p),$$

$$A_p(\mathcal{E}) = \frac{1}{p}\sum_{t=0}^{p-1} a_p(E_t),$$

$$S(N,\mathcal{E}) = -\frac{1}{N}\sum_{p:prime \le N} A_p(\mathcal{E}) \cdot \log p.$$

In the case $\mathcal{E}$ is rational over $\mathbb{Q}$, it is noted that $A_p(\mathcal{E}) = a_p(\mathcal{E})$ except a finite number of primes p and that $S(N,\mathcal{E})$ is equal to $s(N,\mathcal{E})$ up to a constant for sufficiently large N. Henceforth assume that $\mathcal{E}$ is not defined over $\mathbb{Q}$. Then we have following two questions:
(1) Does $S(N,\mathcal{E})$ converge as $N \to \infty$?
(2) If $S(N,\mathcal{E})$ converges, does it converges to $\mathbb{Q}(T)$-rank of $\mathcal{E}$?
By various data of computational experiments, we may conjecture that these questions should be solved affirmatively. In general, for a given elliptic curve $\mathcal{E}$, it seems rather difficult to determine $A_p(\mathcal{E})$ and $\mathbb{Q}(T)$-rank of $\mathcal{E}$. The purpose of this paper is to show that our conjecture holds true for some families of elliptic curves $\mathcal{E}$ over $\mathbb{Q}(T)$. Only for them we can compute $A_p(\mathcal{E})$ and $\mathbb{Q}(T)$-rank of $\mathcal{E}$ at present. Our main results are given in the following Theorems 1 and 2.

Theorem 1. *The sequence $S(N,\mathcal{E}_i)$ converges to $\mathbb{Q}(T)$-rank of $\mathcal{E}_i$, as $N \to \infty$, for the elliptic curves $\mathcal{E}_i$ over $\mathbb{Q}(T)$ of the following types $(T_1) \sim (T_5)$,*
(T_i) $\mathcal{E}_i : Y^2 = f(X) + T^i$,
where $i = 1$ or 2 and $f(X) \in \mathbb{Z}[X]$ is a monic cubic polynomial without double roots,
(T_3) $\mathcal{E}_3 : Y^2 = X^3 - 3T^4X - T^2(1+T^8)$,
(T_4) $\mathcal{E}_4 : Y^2 = X^3 - k^2(T^3 - T)^2X$,
where k is a non-zero integer,
(T_5) $\mathcal{E}_5 : Y^2 = X^3 - k^2(T^4 + 1)^2X$,
where k is a non-zero integer.

Further, if we assume the Sato-Tate conjecture(cf. §2.2), then we have;

Theorem 2. *Let $f(X) = X^3 + aX^2 + bX + c$ be a cubic polynomial of $\mathbb{Z}[X]$ such that $Y^2 = f(X)$ is an elliptic curve of non-CM type. Let $\mathcal{E}_6$ be the elliptic curve defined by*

$$\mathcal{E}_6 : Y^2 = X^3 + a \cdot f(T)X^2 + b \cdot f(T)^2X + c \cdot f(T)^3.$$

Then under the Sato-Tate conjecture, we have

$$\lim_{N\to\infty} S(N,\mathcal{E}_6) = \mathbb{Q}(T)\text{-rank of } \mathcal{E}_6.$$

In §3, we shall prove these theorems. In §2, we shall give some auxiliary lemmas to compute the limit of $S(N,\mathcal{E}_i)$ $(N \to \infty)$ and $\mathbb{Q}(T)$-rank of $\mathcal{E}_i$.

2. Auxiliary lemmas

2.1. Density of prime numbers

For positive integers N, a and b, put

$$M_0(N) = \{p : \text{primes} \mid p \leq N\},$$

and

$$M(a, b, N) = \{p : \text{primes} \mid p \leq N,\ p \equiv a \bmod b\}.$$

Further put $\pi(N) = \#M_0(N)$.

Lemma 2.1. *Let $\{c_p\}_p$ be a bounded sequence of non-negative numbers indexed by prime numbers p. If one of the sequences of numbers*

$$\{\frac{1}{\pi(N)} \sum_{p \in M_0(N)} c_p\}_N,$$

$$\{\frac{1}{N} \sum_{p \in M_0(N)} c_p \cdot \log p\}_N$$

converges, then both of them converge to a common limit.

Proof. Let M be a constant such that $|c_p| < M$ for all primes p. Put

$$\begin{aligned} U_N &= \sum_{p \in M_0(N)} c_p \cdot \log p, \\ V_N &= \sum_{p \in M_0(N)} c_p. \end{aligned}$$

Then we see easily $U_N < V_N \cdot \log N$. For any δ satisfying $0 < \delta < 1$, we have

$$\begin{aligned} U_N &\geq \sum_{N^\delta < p < N} c_p \cdot \log p \\ &\geq \delta \cdot \log N \cdot \sum_{N^\delta < p < N} c_p \\ &= \delta \cdot \log N \cdot \sum_{p < N} c_p - \delta \cdot \log N \cdot \sum_{p < N^\delta} c_p \\ &\geq \delta \cdot \log N \cdot \sum_{p < N} c_p - K \cdot N^\delta \cdot \log N \\ &= \delta \cdot \log N \cdot V_N - K \cdot N^\delta \cdot \log N. \end{aligned}$$

By the prime density theorem, we know that $\pi(N) \sim N/\log(N)$. Thus we have

$$\overline{\lim_{N \to \infty}}\ U_N/N \leq \underline{\lim_{N \to \infty}}\ V_N \cdot \log N/N = \underline{\lim_{N \to \infty}}\ V_N/\pi(N),$$

$$\underline{\lim_{N \to \infty}}\ U_N/N \geq \overline{\lim_{N \to \infty}}\ \delta \cdot V_N \cdot \log N/N = \overline{\lim_{N \to \infty}}\ \delta \cdot V_N/\pi(N).$$

Therefore we have our assertions. □

From this we have immediately:

Lemma 2.2.

$$\lim_{N\to\infty}\frac{1}{N}\sum_{p\in M_0(N)}\log p = 1.$$

Proof. By definition, we have

$$\lim_{N\to\infty}\frac{1}{\pi(N)}\sum_{p\in M_0(N)} 1 = 1.$$

Therefore by Lemma 2.1, we have our assertion. □
Let K be an algebraic number field of finite degree. For a prime number p, put

$$c_p(K) = \#\{\wp\text{:prime ideal in } K \mid N(\wp) = p\},$$

where $N(\wp)$ means the absolute norm of $\wp$. Then we have:

Lemma 2.3.

$$\lim_{N\to\infty}\frac{1}{N}\sum_{p\in M_0(N)} c_p(K)\cdot\log p = 1.$$

Proof. In [3, Formula 47], we know

$$\sum_{N(\wp)=p\le N} 1 = \int_2^N \frac{du}{\log u} + O(N\cdot e^{-c\sqrt{\log N}}).$$

So we have easily

$$\lim_{N\to\infty}\frac{1}{\pi(N)}\sum_{N(\wp)=p\le N} 1 = 1.$$

Hence by Lemma 2.1, we obtain the desired result. □

Applying Lemma 2.3 to the fields $K = \mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-1},\sqrt{-2})$, we have at once,

Lemma 2.4.

$$\lim_{N\to\infty}\frac{1}{N}\sum_{p\in M(1,4,N)}\log p = \frac{1}{2},$$

$$\lim_{N\to\infty}\frac{1}{N}\sum_{p\in M(3,4,N)}\log p = \frac{1}{2},$$

$$\lim_{N\to\infty}\frac{1}{N}\sum_{p\in M(1,8,N)}\log p = \frac{1}{4},$$

$$\lim_{N\to\infty}\frac{1}{N}\sum_{p\in M(5,8,N)}\log p = \frac{1}{4}.$$

Further we have the following lemmas.

Lemma 2.5. *Let k be a non-zero integer. Then*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{p\in M(1,4,N)}(\frac{k}{p})\cdot\log p=\begin{cases}\frac{1}{2} & \text{if } k=\pm m^2 \text{ for some } m\in\mathbb{Z},\\ 0 & \text{otherwise.}\end{cases}$$

Proof. If $k=\pm m^2$ for some $m\in\mathbb{Z}$, then for a prime p such that $p\equiv 1 \bmod 4$, we have $(\frac{k}{p})=1$. Thus we have our assertion by Lemma 2.4. If neither k nor $-k$ is square, applying Lemma 2.3 to $K=\mathbb{Q}(\sqrt{-1},\sqrt{k})$, we see

$$\lim_{N\to\infty}\frac{1}{N}\sum_{p\in M(1,4,N),\ (\frac{k}{p})=1}\log p=\frac{1}{4}.$$

Therefore by Lemma 2.4, we see

$$\lim_{N\to\infty}\frac{1}{N}\sum_{p\in M(1,4,N),\ (\frac{k}{p})=-1}\log p=\frac{1}{4}.$$

This completes the proof. □

Lemma 2.6. *Let E be an elliptic curve with the complex multiplications $K=\mathbb{Q}(\sqrt{-D})$. Assume that $-D$ is the discriminants of K. Then, for a positive integer k, we have*

$$\begin{aligned}&\lim_{N\to\infty}\frac{1}{N}\sum_{p\in M_0(N)}\frac{\log p\cdot(\frac{k}{p})\cdot a_p(E)^2}{p}\\ &=\lim_{N\to\infty}\frac{1}{N}\sum_{p\in M_0(N),\ (\frac{-D}{p})=1}\frac{\log p\cdot(\frac{k}{p})\cdot a_p(E)^2}{p}\\ &=\begin{cases}1 & \text{if } k=m^2,-Dm^2 \text{ for some } m\in\mathbb{Z},\\ 0 & \text{otherwise.}\end{cases}\end{aligned}$$

Proof. For a prime number p such that $(\frac{-D}{p})=-1$, we have $a_p(E)=0$. Thus we have the first equation. We shall prove the second equation. Let p be a prime such that $(\frac{-D}{p})=1$ and E has good reduction at p. Let α_p and $\overline{\alpha}_p$ be the roots of the equation $X^2-a_p(E)X+p=0$. Put

$$b(p,2)=\alpha_p^2+\overline{\alpha}_p^2=a_p(E)^2-2p.$$

Then there exists a non-trivial grössen character λ of $\mathbb{Q}(\sqrt{-D})$ such that

$$\frac{(\frac{k}{p})\cdot b(p,2)}{p}=\lambda(\wp)+\lambda(\overline{\wp}).$$

By [3, Formula 46], we see

$$\sum_{N(\wp)=p\le N}\lambda(\wp)=O(N\cdot e^{-c\sqrt{\log N}}).$$

So we have easily

$$\lim_{N\to\infty}\frac{1}{\pi(N)}\sum_{(\frac{-D}{p})=1,p\leq N}\frac{(\frac{k}{p})\cdot b(p,2)}{p}=\lim_{N\to\infty}\frac{1}{\pi(N)}\sum_{N(\mathfrak{p})=p\leq N}\lambda(\mathfrak{p})=0.$$

Thus we have

$$\begin{aligned}0 &= \lim_{N\to\infty}\frac{1}{\pi(N)}\sum_{p\in M_0(N),\ (\frac{-D}{p})=1}\frac{(\frac{k}{p})\cdot b(p,2)}{p}\\ &= \lim_{N\to\infty}\frac{1}{\pi(N)}\sum_{p\in M_0(N),\ (\frac{-D}{p})=1}\frac{(\frac{k}{p})\cdot a_p(E)^2}{p}\\ &\qquad + \lim_{N\to\infty}\frac{1}{\pi(N)}\sum_{p\in M_0(N),\ (\frac{-D}{p})=1}-2\cdot(\frac{k}{p}).\end{aligned}$$

By the way, if $k=m^2,-Dm^2$ for some $m\in\mathbb{Z}$, then, since $(\frac{k}{p})=1$, we have

$$\lim_{N\to\infty}\frac{1}{\pi(N)}\sum_{p\in M_0(N),\ (\frac{-D}{p})=1}-2\cdot(\frac{k}{p})=-1.$$

If k is not of the form $m^2,-Dm^2$ for any $m\in\mathbb{Z}$, applying Lemma 2.3 to $K_1=\mathbb{Q}(\sqrt{k},\sqrt{-D})$ and $K_2=\mathbb{Q}(\sqrt{k})$, we have

$$\begin{aligned}&\lim_{N\to\infty}\frac{1}{\pi(N)}\sum_{p\in M_0(N),\ (\frac{-D}{p})=1}-2\cdot(\frac{k}{p})\\ &= \lim_{N\to\infty}\frac{1}{\pi(N)}\sum_{p\in M_0(N)}(c_p(K_2)-c_p(K_1))=0.\end{aligned}$$

Therefore, by Lemma 2.1, we have our assertions. □

Lemma 2.7. *Let $\mathbb{E}$ be the elliptic curve defined by the equation $Y^2=X^3-X$. Put $e_p=a_p(\mathbb{E})$. Then for a non-zero integer k, we have*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{p\in M_0(N)}\frac{(\frac{k}{p})\cdot e_p^2}{p}\cdot\log p=\lim_{N\to\infty}\frac{1}{N}\sum_{p\in M(1,4,N)}\frac{(\frac{k}{p})\cdot e_p^2}{p}\cdot\log p$$

$$=\begin{cases}1 & \text{if } k=\pm m^2 \text{ for some } m\in\mathbb{Z},\\ 0 & \text{otherwise.}\end{cases}$$

Proof. Note that $\mathbb{E}$ has C.M. $\mathbb{Q}(\sqrt{-1})$. Applying Lemma 2.6 to the curve $\mathbb{E}$, we have our assertion. □

2.2. Shioda's Theorem

We shall use the following result of Shioda [8] to determine the $\mathbb{Q}(T)$-rank of elliptic curves.

Theorem (Shioda [8] Theorem A2). *Let Ω be a perfect field with characteristic $ch(\Omega) \neq 2, 3$, and let b_1, b_2, b_3 be distinct elements of Ω. Let $K = \Omega(T)$ be the rational function fields over Ω with a variable T. Then the K-rank of the elliptic curve $\mathcal{E} : Y^2 = (X - b_1)(X - b_2)(X - b_3) + T^2$ is 2 and $\mathcal{E}(K)$ has no non-trivial torsion elements. Further two points $P_1 = (b_1, T)$, $P_2 = (b_2, T)$ generate $\mathcal{E}(K)$.*
Proof. Cf. Theorem A2 of [8]. □

3. Proof of Theorems 1 and 2

We shall prove Theorems 1 and 2 in the following propositions 3.1 $\sim$ 3.6. In each proposition, we give explicitly $A_p(\mathcal{E})$, the limit of $S(N, \mathcal{E}_i)$ and $\mathbb{Q}(T)$-rank of $\mathcal{E}_i$, for $i = 1, 2, .., 6$, respectively. In this section, we denote by $r(\mathcal{E}_i)$ the $\mathbb{Q}(T)$-rank of $\mathcal{E}_i$. Further denote by $\mathbb{E}$ the elliptic curve defined by the equation: $Y^2 = X^3 - X$. To make the notation easy, we put $e_p = a_p(\mathbb{E})$. By [4, p.307], we know

$$e_p = \begin{cases} 0 & p \equiv 3 \bmod 4, \\ -2b & p \equiv 1 \bmod 4, \end{cases} \tag{3.1}$$

where b is the odd positive integer such that $p = a^2 + b^2$.

3.1. The curves $\mathcal{E}_1$ and $\mathcal{E}_2$

Proposition 3.1. *Let $\mathcal{E}_1$ be the elliptic curve defined in Theorem 1. Then*
(1) $A_p(\mathcal{E}_1) = 0$ for every prime p.
(2) $\lim_{N\to\infty} S(N, \mathcal{E}_1) = 0$.
(3) $r(\mathcal{E}_1) = 0$.
In particular, we have $\lim_{N\to\infty} S(N, \mathcal{E}_1) = r(\mathcal{E}_1)$.

Proof. The assertion (1) is trivial. Thus we have (2). To prove (3), put

$$f(X) = (X - \alpha)(X - \beta)(X - \gamma) \qquad (\alpha, \beta, \gamma \in \overline{\mathbb{Q}}).$$

Let $K = \mathbb{Q}(\sqrt{T}, \alpha, \beta, \gamma)$, and let σ be the element of $Gal(K/\mathbb{Q}(T))$ which maps $\sqrt{T}$ to $-\sqrt{T}$ and leaves α, β, γ unchanged. Let $P_1 = (\alpha, \sqrt{T})$ and $P_2 = (\beta, \sqrt{T})$. Then, by Shioda's Theorem in §2.2, $\mathcal{E}_1(K)$ is a free $\mathbb{Z}$-module of rank 2 and is generated by P_1 and P_2. Since

$$(n_1 P_1 + n_2 P_2)^\sigma = n_1 P_1^\sigma + n_2 P_2^\sigma = -n_1 P_1 - n_2 P_2,$$

we have that $\mathcal{E}_1(\mathbb{Q}(T)) = \{0\}$. □

Proposition 3.2. *Let $\mathcal{E}_2$ be the elliptic curve defined in Theorem 1. Then*

(1) $A_p(\mathcal{E}_2) = \begin{cases} -2, & \text{if } f(X) \bmod p \text{ factors completely,} \\ 1, & \text{if } f(X) \bmod p \text{ is irreducible,} \\ 0, & \text{otherwise.} \end{cases}$

(2) $\lim_{N\to\infty} S(N, \mathcal{E}_2) = \begin{cases} 2, & \text{if } f(X) \text{ factors completely,} \\ 0, & \text{if } f(X) \text{ is irreducible,} \\ 1, & \text{otherwise.} \end{cases}$

(3) $r(\mathcal{E}_2) = \begin{cases} 2, & \text{if } f(X) \text{ factors completely,} \\ 0, & \text{if } f(X) \text{ is irreducible,} \\ 1, & \text{otherwise.} \end{cases}$

In particular, we have $\lim_{N\to\infty} S(N, \mathcal{E}_2) = r(\mathcal{E}_2)$.

Proof. we have:

$$\begin{aligned} -pA_p(\mathcal{E}_2) &= \sum_{t=0}^{p-1} -a_p(E_t) \\ &= \#\{(x,y,t) \in \mathbf{A}^3(\mathbb{F}_p) | y^2 = f(x) + t^2\} - p^2 \\ &= (\sum_{x=0}^{p-1} \#\{(y,t) \in \mathbf{A}^2(\mathbb{F}_p) | y^2 = f(x) + t^2\}) - p^2 \\ &= (\sum_{x=0}^{p-1} \#\{(y,t) \in \mathbf{A}^2(\mathbb{F}_p) | (y-t)(y+t) = f(x)\}) - p^2. \end{aligned}$$

On the other hand, for any $a \in \mathbb{F}_p$, we have

$$\#\{(y,t) | (y-t)(y+t) = a\} = \begin{cases} 2p-1 & \text{if } a = 0, \\ p-1 & \text{if } a \neq 0. \end{cases}$$

Therefore
$-pA_p(\mathcal{E}_2) =$

$$\begin{cases} 3(2p-1) + (p-3)(p-1) - p^2, & \text{if } f(X) \bmod p \text{ factors completely,} \\ p \cdot (p-1) - p^2, & \text{if } f(X) \bmod p \text{ is irreducible,} \\ 2(2p-1) + (p-2)(p-1) - p^2, & \text{otherwise.} \end{cases}$$

This shows (1). Next we shall prove (2). Assume $f(X)$ factors into three polynomials of degree 1 in $\mathbb{Q}[T]$. Then we see $A_p(\mathcal{E}_2) = -2$ for almost all primes p by (1). Further, Lemma 2.2 implies

$$\lim_{N\to\infty} \frac{1}{N} \sum_{p \in M_0(N)} -\log p \cdot A_p(\mathcal{E}_2) = 2.$$

Therefore we have the desired result in this case. We shall consider the other cases. Write $f(X) = (X-\alpha)(X-\beta)(X-\gamma)$, $\alpha, \beta, \gamma \in \overline{\mathbb{Q}}$, $\beta, \gamma \notin \mathbb{Q}$. Let $K = \mathbb{Q}(\beta)$. For any prime number p, we put

$$c_p = \#\{\wp : \text{prime ideals in } K \mid N(\wp) = p\}.$$

Let $\mathcal{F}_p(X)$ be the polynomial of $\mathbb{F}_p[X]$ obtained by reducing $f(X)$ mod p. For a prime p such that $\mathcal{F}_p(X)$ has no double roots, we shall show $A_p(\mathcal{E}_2) = 1 - c_p$. We shall prove this fact only for the case $\mathbb{Q}(\alpha, \beta, \gamma)$ is a S_3-extension over $\mathbb{Q}$, because other cases can be treated similarly. Let p be a prime with the described property. Then we have

$$c_p = 3 \Leftrightarrow \mathcal{F}_p(X) \text{ factors completely} \Leftrightarrow -A_p = 2,$$

$$c_p = 0 \Leftrightarrow \mathcal{F}_p(X) \text{ is irreducible} \Leftrightarrow -A_p = -1,$$

$$c_p = 1 \Leftrightarrow \mathcal{F}_p(X) \text{ factors into two polynomials} \Leftrightarrow -A_p = 0.$$

Thus we have $A_p(\mathcal{E}_2) = 1 - c_p$. By Lemma 2.3, we see

$$\begin{aligned} &\lim_{N\to\infty} \frac{1}{N} \sum_{p \in M_0(N)} -\log p \cdot A_p(\mathcal{E}_2) \\ &= \lim_{N\to\infty} \frac{1}{N} \Big(\sum_{p \in M_0(N)} \log p \cdot c_p - \sum_{p \in M_0(N)} \log p \Big) \\ &= 1 - 1 = 0. \end{aligned}$$

Because, for almost all p, $f(X)$ mod p has no double roots, this shows (2).

Now we shall prove (3). If $f(X)$ factors into three polynomials of degree 1 ($\alpha, \beta, \gamma \in \mathbb{Q}$), Shioda's Theorem in §2.2 implies that $r(\mathcal{E}_2) = 2$. Assume $f(X)$ factors into two irreducible polynomials of degree 1 and of degree 2 ($\alpha \in \mathbb{Q}$, $\beta, \gamma \in \overline{\mathbb{Q}}$). Let $\Omega = \mathbb{Q}(\beta)$ and $K = \mathbb{Q}(\beta, T)$, and let σ be the element of $Gal(K/\mathbb{Q}(T))$ which maps β to γ. Put $P_1 = (\alpha, T)$ and $P_2 = (\beta, T)$. Since $P_1 + P_2 = (\gamma, -T) = -P_2^\sigma$, we have
$(n_1P_1 + n_2P_2)^\sigma = n_1P_1^\sigma + n_2P_2^\sigma = n_1P_1 - n_2(P_1 + P_2)$.
Thus we see that the σ-invariant elements of $\mathcal{E}(K)$ are nP_1, $n \in \mathbb{Z}$. So we have $\mathcal{E}_1(\mathbb{Q}(T)) =< P_1 >$.

Consider the case $f(X)$ is irreducible. Let $\Omega = \mathbb{Q}(\alpha, \beta)$, $K = \mathbb{Q}(\alpha, \beta, T)$, and σ the element of $Gal(K/\mathbb{Q}(T))$ such that it maps α to β and β to γ. Put $P_1 = (\alpha, T), P_2 = (\beta, T)$. Then we have
$(n_1P_1 + n_2P_2)^\sigma = n_1P_1^\sigma + n_2P_2^\sigma = n_1P_2 + n_2(-P_1 - P_2) = -n_2P_1 - (n_1 + n_2)P_2$.
Thus we see that $\mathcal{E}_2(\mathbb{Q}(T)) = \{0\}$. □

3.2. The curve $\mathcal{E}_3$

Proposition 3.3. *Let $\mathcal{E}_3$ be the elliptic curve defined in Theorem 1. Then*

(1) $$A_p(\mathcal{E}_3) = \begin{cases} 2 & if\ p \equiv 3 \mod 4\ , p \neq 3, \\ -4b^2/p & if\ p \equiv 5 \mod 8, \\ (-4b^2 - 4p)/p & if\ p \equiv 1 \mod 8, \end{cases}$$

where, in the cases $p \equiv 1 \mod 4$, b is the odd positive integer such that $p = a^2 + b^2$.

(2) $\lim_{N\to\infty} S(N, \mathcal{E}_3) = 1$.

(3) $r(\mathcal{E}_3) = 1$.

In particular, we have $\lim_{N\to\infty} S(N, \mathcal{E}_3) = r(\mathcal{E}_3)$.

Proof. The assertion (1) was conjectured by the author on the computer experiment and proved by the author, Ishida, and Ishikawa (See appendix of this paper). The assertion (3) is proved by Kuwata [6]. Therefore we will show (2).

By (3.1), we have

$$\begin{aligned}
&\lim_{N\to\infty} S(N,\mathcal{E}_3)\\
&= \lim_{N\to\infty}\frac{1}{N}\Big(\sum_{p\in M(1,4,N)}\frac{4b^2\cdot\log p}{p}+\sum_{p\in M(1,8,N)}4\cdot\log p+\sum_{p\in M(3,4,N)}-2\cdot\log p\Big)\\
&= \lim_{N\to\infty}\frac{1}{N}\Big(\sum_{p\in M(1,4,N)}\frac{e_p^2\cdot\log p}{p}+\sum_{p\in M(1,8,N)}4\cdot\log p+\sum_{p\in M(3,4,N)}-2\cdot\log p\Big).
\end{aligned}$$

By Lemmas 2.4 and 2.7, we know this limit is equal to 1. Therefore we have (2). □

3.3. The curves $\mathcal{E}_4$ and $\mathcal{E}_5$

Proposition 3.4. *Let $\mathcal{E}_4$ be the elliptic curve defined in Theorem 1. Then*
(1) $A_p(\mathcal{E}_4) = -\frac{1}{p}\cdot(\frac{k}{p})\cdot e_p^2$.
(2) $\lim_{N\to\infty} S(N,\mathcal{E}_4) = \begin{cases} 1 & \text{if } k=\pm m^2 \text{ for some } m\in\mathbb{Z},\\ 0 & \text{otherwise.}\end{cases}$
(3) $r(\mathcal{E}_4) = \begin{cases} 1 & \text{if } k=\pm m^2 \text{ for some } m\in\mathbb{Z},\\ 0 & \text{otherwise.}\end{cases}$
In particular, we have $\lim_{N\to\infty} S(N,\mathcal{E}_4) = r(\mathcal{E}_4)$.

Proof. Let E_t be the curve obtained from $\mathcal{E}_4$ by the specialization $T\to t$ $(t\in\mathbb{Q})$. Since the curve $Y^2 = X^3 - k^2\cdot(t^3-t)^2\cdot X$, $(k,t\in\mathbb{Z})$ is a twist of the curve $\mathbb{E}: Y^2 = X^3 - X$, we see easily that

$$a_p(E_t) = (\frac{k\cdot(t^3-t)}{p})\cdot e_p.$$

So we have

$$pA_p(\mathcal{E}_4) = \sum_{t=0}^{p-1}(\frac{k\cdot(t^3-t)}{p})\cdot e_p = (\frac{k}{p})\cdot e_p\cdot\sum_{t=0}^{p-1}(\frac{(t^3-t)}{p}) = -(\frac{k}{p})e_p^2.$$

This shows (1). Next we shall prove (2). By (1), we know

$$A_p(\mathcal{E}_4) = -\frac{1}{p}\cdot(\frac{k}{p})\cdot e_p^2.$$

Thus

$$S(N,\mathcal{E}_4) = \lim_{N\to\infty}\frac{1}{N}\sum_{p\in M(1,4,N)}\frac{(\frac{k}{p})\cdot e_p^2\cdot\log p}{p}.$$

By Lemma 2.7, we have (2). Now we shall prove (3). Our proof is similar to that of [2] but, in our case, more precise analysis is required. Let $K = \overline{\mathbb{Q}}(T, S)$, where T and S are variables satisfying a relation $S^2 = T^3 - T$. It is well known that the endomorphism ring of $\mathbb{E} : Y^2 = X^3 - X$ is isomorphic to $\mathbb{Z}[\sqrt{-1}]$. The element $r + s\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$ acts on the point (X, Y) in the following manner:

$$(X, Y) \to r \cdot (X, Y) + s \cdot (-X, \sqrt{-1} \cdot Y).$$

So, we see easily that K-rational points of $\mathbb{E}$ are given by

$$\{r \cdot (T, S) + s \cdot (-T, \sqrt{-1} \cdot S) + (x_0, y_0) \mid r, s \in \mathbb{Z},\ (x_0, y_0) \in \mathbb{E}(\overline{\mathbb{Q}})\}.$$

Since the curve $\mathcal{E}_4$ is defined by the equation $Y^2 = X^3 - k^2 \cdot (T^3 - T)^2 \cdot X$, $\mathbb{E}$ is K-isomorphic to $\mathcal{E}_4$ by the map $\phi : (X, Y) \to (k \cdot S^2 \cdot X, k^{3/2} \cdot S^3 \cdot Y)$. Put

$$P = \phi(T, S) = (k \cdot T \cdot S^2, \sqrt{k} \cdot k \cdot S^4)$$

and

$$Q = \phi(-T, \sqrt{-1} \cdot S) = (-k \cdot T \cdot S^2, \sqrt{-k} \cdot k \cdot S^4).$$

Then all K-rational points of $\mathcal{E}_4$ are given by

$$\{r \cdot P + s \cdot Q + \phi(x_0, y_0) \mid r, s \in \mathbb{Z},\ (x_0, y_0) \in \mathbb{E}(\overline{\mathbb{Q}})\}.$$

Let σ be an element of $Gal(K/\overline{\mathbb{Q}}(T))$ such that $S^\sigma = -S$. We have easily $P^\sigma = P$, $Q^\sigma = Q$, and

$$y_0 = 0 \Leftrightarrow \phi(x_0, y_0)^\sigma = \phi(x_0, y_0).$$

So we see $\overline{\mathbb{Q}}(T)$-rational points of $\mathcal{E}_4$ are given by

$$\{r \cdot P + s \cdot Q + n_0(0, 0) + n_1(S^2, 0) + n_2(-S^2, 0) \mid r, s \in \mathbb{Z},\ n_0, n_1, n_2 \in \mathbb{Z}/2\mathbb{Z}\}.$$

Thus if $k = m^2$ for some $m \in \mathbb{Z}$, we have easily

$$\mathcal{E}_4(\mathbb{Q}(T)) = \{r \cdot P + n_0(0, 0) + n_1(S^2, 0) + n_2(-S^2, 0) \mid r \in \mathbb{Z},\ n_0, n_1, n_2 \in \mathbb{Z}/2\mathbb{Z}\}.$$

Further, if $k = -m^2$ for some $m \in \mathbb{Z}$, we have also

$$\mathcal{E}_4(\mathbb{Q}(T)) = \{r \cdot Q + n_0(0, 0) + n_1(S^2, 0) + n_2(-S^2, 0) \mid r \in \mathbb{Z},\ n_0, n_1, n_2 \in \mathbb{Z}/2\mathbb{Z}\}.$$

Let $k \neq \pm m^2$ for any $m \in \mathbb{Z}$. Consider two elements τ and ν of $Gal(\overline{\mathbb{Q}}(T)/\mathbb{Q}(T))$ such that $\sqrt{-1}^\tau = -\sqrt{-1}$ and $\sqrt{k}^\nu = -\sqrt{k}$. Then, $P^\nu = -P$ and $Q^{\tau\nu} = -Q$. Therefore we see $\mathbb{Q}(T)$-rational points of $\mathcal{E}_4$ are only 2-torsion points. This shows (3). □

Proposition 3.5. *Let $\mathcal{E}_5$ be the elliptic curve defined in Theorem 1. Then*
(1) $A_p(\mathcal{E}_5) = -\frac{1}{p} \cdot \left(\left(\frac{2k}{p}\right) \cdot e_p^2 + \left(\frac{k}{p}\right) \cdot e_p \right)$.
(2) $\lim_{N \to \infty} S(N, \mathcal{E}_5) = \begin{cases} 1 & \text{if } k = \pm 2m^2 \text{ for some } m \in \mathbb{Z}, \\ 0 & \text{otherwise.} \end{cases}$
(3) $r(\mathcal{E}_5) = \begin{cases} 1 & \text{if } k = \pm 2m^2 \text{ for some } m \in \mathbb{Z}, \\ 0 & \text{otherwise.} \end{cases}$
In particular, we have $\lim_{N \to \infty} S(N, \mathcal{E}_5) = r(\mathcal{E}_5)$.

Proof. Let N_1 and N_2 be the number of $\mathbb{F}_p$-rational solutions (x, y) of the equations $y^2 = x^3 - x$ and $y^2 = x^4 + 1$ respectively. Then, by Koblitz [5, p.56-57], we have $N_1 = N_2 - 1$. Since the curve $y^2 = x^3 - 4x$ is isomorphic to the curve $2y^2 = x^3 - x$, we have

$$\sum_{t=0}^{p-1}(\frac{t^4+1}{p}) = \sum_{t=0}^{p-1}(\frac{t^3-4t}{p}) - 1 = (\frac{2}{p})\cdot\sum_{t=0}^{p-1}(\frac{t^3-t}{p}) - 1.$$

Thus we have

$$\sum_{t=0}^{p-1}(\frac{t^4+1}{p}) = -(\frac{2}{p})\cdot e_p - 1.$$

Let E_t be the curve obtained from $\mathcal{E}_5$ by the specialization $T \to t$ $(t \in \mathbb{Q})$. We see easily that

$$a_p(E_t) = (\frac{k\cdot(t^4+t)}{p})\cdot e_p.$$

So we have

$$pA_p(\mathcal{E}_5) = \sum_{t=0}^{p-1}(\frac{k\cdot(t^4+1)}{p})\cdot e_p = (\frac{k}{p})\cdot e_p\cdot\sum_{t=0}^{p-1}(\frac{(t^4+1)}{p}) = -((\frac{2k}{p})\cdot e_p^2 + (\frac{k}{p})\cdot e_p).$$

This shows (1). Next we shall prove (2). Since

$$A_p(\mathcal{E}_5) = -\frac{1}{p}\cdot((\frac{2k}{p})\cdot e_p^2 + (\frac{k}{p})\cdot e_p),$$

$$\lim_{N\to\infty} S(N, \mathcal{E}_5) = \lim_{N\to\infty}\frac{1}{N}\sum_{p\in M_0(N)}(\frac{2k}{p})\cdot e_p^2\cdot\log p + \lim_{N\to\infty}\frac{1}{N}\sum_{p\in M_0(N)}(\frac{k}{p})\cdot e_p\cdot\log p.$$

It is easy to see that the first limit is equal to

$$\begin{cases} 1 & if\ k \in \pm 2m^2 \text{ for some } m \in \mathbb{Z}, \\ 0 & otherwise. \end{cases}$$

The second limit is easily shown to be 0, since $|e_p| \le 2\sqrt{p}$. So we have (2).
Now we shall prove (3). Let $K = \overline{\mathbb{Q}}(T, S)$, where T and S are variables satisfying a relation $S^2 = T^4 + 1$. Put $U = T^2 - S$ and $V = \sqrt{2}\cdot T\cdot(T^2 - S)$. Then we have $V^2 = U^3 - U$ and $K = \overline{\mathbb{Q}}(U, V)$. So, we see easily that K-rational points of $\mathbb{E}$ are given by

$$\{r\cdot(U,V) + s\cdot(-U, \sqrt{-1}\cdot V) + (x_0, y_0) \mid r, s \in \mathbb{Z},\ (x_0, y_0) \in \mathbb{E}(\overline{\mathbb{Q}})\}.$$

Since the equation of the curve $\mathcal{E}_5$ is $Y^2 = X^3 - k^2\cdot(T^4+1)^2\cdot X$, $\mathbb{E}$ is K-isomorphic to $\mathcal{E}_5$ by the map $\phi: (X, Y) \to (k\cdot S^2\cdot X, k^{3/2}\cdot S^3\cdot Y)$.
Put

$$P = \phi(U, V) = (k\cdot S^2\cdot(T^2 - S), \sqrt{2k}\cdot k\cdot T\cdot S^3\cdot(T^2 - S))$$

and

$$Q = \phi(-U, \sqrt{-1}\cdot V) = (-k\cdot T\cdot S^2\cdot(T^2 - S), \sqrt{-2k}\cdot k\cdot T\cdot S^3\cdot(T^2 - S)).$$

Then K-rational points of $\mathcal{E}_5$ are given by

$$\{r \cdot P + s \cdot Q + \varphi(x_0, y_0) \mid r, s \in \mathbb{Z},\ (x_0, y_0) \in \mathbb{E}(\overline{\mathbb{Q}})\}.$$

Let σ be an element of $Gal(K/\overline{\mathbb{Q}}(T))$ such that $S^\sigma = -S$. Since

$$(T^2 - S)^\sigma = T^2 + S = \frac{-1}{T^2 - S},$$

we have $P^\sigma = P + (0,0)$, $Q^\sigma = Q + (0,0)$, and

$$y_0 = 0 \Leftrightarrow \phi(x_0, y_0)^\sigma = \phi(x_0, y_0).$$

So we see $\overline{\mathbb{Q}}(T)$-rational points of $\mathcal{E}_5$ are given by
$\{r \cdot P + s \cdot Q + n_0(0,0) + n_1(S^2, 0) + n_2(-S^2, 0) \mid$
$r, s \in \mathbb{Z},\ r + s \in 2\mathbb{Z},\ n_0, n_1, n_2 \in \mathbb{Z}/2\mathbb{Z}\}$.
Thus we have easily

$$\mathcal{E}_5(\mathbb{Q}(T)) = \{2r \cdot P + n_0(0,0) + n_1(S^2, 0) + n_2(-S^2, 0) \mid r \in \mathbb{Z},\ n_0, n_1, n_2 \in \mathbb{Z}/2\mathbb{Z}\}$$

in case of $k = 2m^2$ for some $m \in \mathbb{Z}$, and

$$\mathcal{E}_5(\mathbb{Q}(T)) = \{2r \cdot Q + n_0(0,0) + n_1(S^2, 0) + n_2(-S^2, 0) \mid r \in \mathbb{Z},\ n_0, n_1, n_2 \in \mathbb{Z}/2\mathbb{Z}\}$$

in case of $k = -2m^2$ for some $m \in \mathbb{Z}$.

Now we will consider the case $k \neq \pm 2m^2$ for any $m \in \mathbb{Z}$. Let τ be an element of $Gal(\overline{\mathbb{Q}}(T)/\mathbb{Q}(T))$ such that $\sqrt{k}^\tau = -\sqrt{k}$.

Then, $P^\tau = -P$ and $Q^\tau = -Q$. Hence we see $\mathbb{Q}(T)$-rational points of $\mathcal{E}_5$ are only 2-torsion points. □

3.4. The curve $\mathcal{E}_6$

Proposition 3.6. *Let $\mathcal{E}_6$ and $f(X)$ be the elliptic curve and the polynomial defined in Theorem 2 respectively. Let $\mathbb{E}^*$ be the elliptic curve defined by the equation $Y^2 = f(X)$. For a prime number p, put $f_p = a_p(\mathbb{E}^*)$. Then*
(1) $A_p(\mathcal{E}_6) = -f_p^2$.
(2) $\lim_{N \to \infty} S(N, \mathcal{E}_6) = 1$, *under the Sato-Tate conjecture.*
(3) $r(\mathcal{E}_6) = 1$.

In particular, we have $\lim_{N \to \infty} S(N, \mathcal{E}_6) = r(\mathcal{E}_6)$, *under the Sato-Tate conjecture.*

Proof. Let E_t be the curve over $\mathbb{Q}$ obtained from $\mathcal{E}_6$ by the specialization $T \to t$ ($t \in \mathbb{Q}$). We see easily that

$$a_p(E_t) = \left(\frac{f(t)}{p}\right) \cdot f_p.$$

Thus we have

$$pA_p(\mathcal{E}_6) = \sum_{t=0}^{p-1} \left(\frac{f(t)}{p}\right) \cdot f_p = -f_p^2.$$

This shows (1). Next we shall prove (2). Let

$$c_2 = \lim_{N\to\infty} \frac{1}{\pi(N)} \sum_{p\in M_0(N)} \frac{f_p^2 - 2p}{p} \log p.$$

Then applying Sato-Tate conjecture (cf. Tate [9, p.106]) to the curve $\mathbb{E}^*$, we have $c_2 = -1$.
Therefore we have, by Lemma 2.1,

$$\begin{aligned} \lim_{N\to\infty} S(N, \mathcal{E}_6) &= \lim_{N\to\infty} \frac{1}{N} \sum_{p\in M(N)} f_p^2 \cdot \log p \\ &= c_2 + \lim_{N\to\infty} \frac{1}{N} \sum_{p\in M_0(N)} 2\log p \\ &= c_2 + 2 = 1. \end{aligned}$$

This shows (2). Now we shall prove (3). Let $K = \overline{\mathbb{Q}}(T, S)$ where T and S are variables satisfying a relation $S^2 = f(T)$. It is well known that the endomorphism ring of $\mathbb{E}^*$ is isomorphic to $\mathbb{Z}$. So, we see easily that K-rational points of $\mathbb{E}^*$ are given by

$$\{r \cdot (T, S) + (x_0, y_0) \mid r \in \mathbb{Z},\ (x_0, y_0) \in \mathbb{E}^*(\overline{\mathbb{Q}})\}.$$

Since the curve $\mathcal{E}_6$ is also defined by the equation $f(T) \cdot Y^2 = f(X)$, $\mathbb{E}^*$ is K-isomorphic to $\mathcal{E}_6$ by the map $\phi : (X, Y) \to (X, Y/S)$. Put

$$P = \phi(T, S) = (T, 1).$$

Then K-rational points of $\mathcal{E}_6$ are given by

$$\{r \cdot P + \phi(x_0, y_0) \mid r \in \mathbb{Z},\ (x_0, y_0) \in \mathbb{E}^*(\overline{\mathbb{Q}})\}.$$

Let σ be an element of $Gal(K/\overline{\mathbb{Q}}(T))$ such that $S^\sigma = -S$. We have easily $P^\sigma = P$, and

$$y_0 = 0 \Leftrightarrow \phi(x_0, y_0)^\sigma = \phi(x_0, y_0).$$

Therefore we see that $\overline{\mathbb{Q}}(T)$-rational points of $\mathcal{E}_6$ are given by

$$\{r \cdot P + \phi(x_0, y_0) \mid r \in \mathbb{Z},\ (x_0, y_0) \in \mathbb{E}^*(\overline{\mathbb{Q}})[2]\}.$$

Hence,

$$\mathcal{E}_6(\mathbb{Q}(T)) = \{r \cdot P + (x_0, y_0) \mid r \in \mathbb{Z},\ \phi(x_0, y_0) \in \mathbb{E}^*(\mathbb{Q})[2]\}.$$

This shows (3). □

Appendix

On the weighted average of the number of $\mathbb{F}_p$ rational points of the elliptic curve $\mathcal{E} : Y^2 = X^3 - 3T^4X - T^2(T^8+1)$

Nobuhiko Ishida [1]
Tsuneo Ishikawa [2]
Koh-ichi Nagao [3]
1. Dept. of Math.. Osaka Prefecture University. 1-1 Gakuen-cho Sakai 593 Japan
2. Dept. of Math., Osaka Institute of Technology, 5-16-1 Omiya Asahi Osaka 535 Japan
3. Shiga Polytechnic College, 1414 Furukawa Oh-mihachiman Shiga 523 Japan

The aim of this appendix is to prove the assertion (1) of Proposition 3.3 of §3. Let $\mathcal{E}$ be the elliptic curve defined by

$$\mathcal{E} : Y^2 = X^3 - 3T^4 \cdot X - T^2 \cdot (T^8+1). \tag{1}$$

We shall prove, for prime numbers $p \geq 5$,

$$A_p(\mathcal{E}) = \begin{cases} 2 & if\ p \equiv 3 \bmod 4,\ p \neq 3, \\ -4b^2/p & if\ p \equiv 5 \bmod 8, \\ (-4b^2-4p)/p & if\ p \equiv 1 \bmod 8, \end{cases} \tag{2}$$

where, in the case $p \equiv 1 \bmod 4$, b is the odd positive integer such that $p = a^2 + b^2$. Let us consider the variable T as a parameter. Then we have a family of projective curves parametrized by T.

$$\mathcal{E}(T) : Z \cdot Y^2 = X^3 - 3 \cdot T^4 \cdot X \cdot Z^2 - T \cdot (T^8+1) \cdot Z^3$$

in 2-dimensional projective space $\mathbb{P}^2$. Let E_t be the curve obtained from $\mathcal{E}$ by the specialization: $T \to t$. Since $\#E_t(\mathbb{F}_p) = \#\mathcal{E}(t)(\mathbb{F}_p)$ for any $t \in \mathbb{F}_p$, we know

$$p \cdot A_p(\mathcal{E}) = p^2 + p - \sum_{t \in \mathbb{F}_p} \#\mathcal{E}(t)(\mathbb{F}_p). \tag{3}$$

Let S be an elliptic surface in $\mathbb{P}^3$ defined by

$$S : A^4 + B^4 = C^4 + D^4.$$

Then, due to Eichler, we know that $\mathcal{E}$ is a Weierstrass model of S (cf.[6]) and we have a map of $S(\mathbb{F}_p)$ to a family $\{\mathcal{E}(t)(\mathbb{F}_p)\}_{t \in \mathbb{F}_p}$. Therefore we can relate $\#A_p(\mathcal{E})$ to $\#S(\mathbb{F}_p)$.

Proposition 1. Let p be a prime number greater than 3. Then

$$\#S(\mathbb{F}_p) = \sum_{t \in \mathbb{F}_p} \#\mathcal{E}(t)(\mathbb{F}_p) + \begin{cases} 3p+1 & if\ p \equiv 3 \bmod 4, \\ 9p+1 & if\ p \equiv 5 \bmod 8, \\ 13p+1 & if\ p \equiv 1 \bmod 8. \end{cases}$$

Further we have

$$pA_p(\mathcal{E}) = p^2 + p - \#S(\mathbb{F}_p) + \begin{cases} 3p+1 & if\ p \equiv 3 \bmod 4, \\ 9p+1 & if\ p \equiv 5 \bmod 8, \\ 13p+1 & if\ p \equiv 1 \bmod 8. \end{cases}$$

Proof. Substituting $A+C$, $A-C$, $D+B$, and $D-B$ by E,F,G and H respectively, we know that S is also defined by the equation:

$$E \cdot F \cdot (E^2 + F^2) = G \cdot H \cdot (G^2 + H^2).$$

Consider the intersection $S_2(T)$ of S and a hyperplane $G = T \cdot E \in \mathbb{P}^3$. Then $S_2(T)$ is given by

$$S_2(T) : E \cdot (F^3 + F \cdot E^2 - TH^3 - T^3 \cdot E^2 \cdot H) = 0.$$

Let $C_1(T)$ be a curve in $\mathbb{P}^2$ defined by

$$C_1(T) : F^3 + F \cdot E^2 = TH^3 + T^3 \cdot E^2 \cdot H.$$

Then we see that $\mathbb{F}_p$-rational points on S with non-zero E-coordinate bijectively correspond to $\mathbb{F}_p$-rational points with non-zero E-coordinate contained in a family of curves $C_1(t)(\mathbb{F}_p)$ $(t \in \mathbb{F}_p)$. Further we see easily

$$\#\{S(\mathbb{F}_p) \cap \{E = 0\}\} = \begin{cases} 2p+1 & if\ p \equiv 3 \bmod 4, \\ 4p+1 & if\ p \equiv 1 \bmod 4. \end{cases}$$

$$\sum_{t \in \mathbb{F}_p} \#\{C_1(T)(\mathbb{F}_p) \cap \{E = 0\}\} = p.$$

Therefore we have

$$\#S(\mathbb{F}_p) = \sum_{t \in \mathbb{F}_p} \#C_1(t)(\mathbb{F}_p) + \begin{cases} p+1 & if\ p \equiv 3 \bmod 4 \quad p \neq 3, \\ 3p+1 & if\ p \equiv 1 \bmod 4. \end{cases} \tag{4}$$

Then the curve $C_1(T)$ is transformed to $\mathcal{E}(T)$ by applying three transformations

$$\xi_i(T) : C_i(T) \to C_{i+1}(T) \qquad (i = 1, 2, 3, \qquad C_4(T) = \mathcal{E}(T))$$

successively, where

$$\xi_1(T) : Z = T^3 \cdot H - F,$$
$$C_2(T) : Z \cdot E^2 = (T^9 - T) \cdot H^3 - 3T^6 \cdot H^2 \cdot Z + 3T^3 \cdot H \cdot Z^2 - Z^3,$$
$$\xi_2(T) : Y = (T^9 - T) \cdot E, X' = (T^9 - T) \cdot H,$$
$$C_3(T) : Z \cdot Y'^2 = X'^3 - 3T^6 \cdot X'^2 \cdot Z + 3T^3 \cdot (T^9 - T) \cdot X' \cdot Z^2 - (T^9 - T)^2 \cdot Z^3,$$
$$\xi_3(T) : X' = X + T^6 \cdot Z,$$
$$C_4(T) = \mathcal{E}(T) : Z \cdot Y'^2 = X^3 - 3T^4 \cdot X \cdot Z^2 - T^2 \cdot (1 + T^8) \cdot Z^3.$$

Since $\xi_1(t)$and $\xi_3(t)$ are isomorphisms for any $t \in \mathbb{F}_p$ and $\xi_2(t)$ is an isomorphism for $t \in \mathbb{F}_p$ with $t^9 \neq t$, we have

$$\#C_1(t)(\mathbb{F}_p) = \#C_2(t)(\mathbb{F}_p),\ \#C_3(t)(\mathbb{F}_p) = \#C_4(t)(\mathbb{F}_p),\ for\ any\ t \in \mathbb{F}_p,$$
$$\#C_2(t)(\mathbb{F}_p) = \#C_3(t)(\mathbb{F}_p),\quad for\ t \in \mathbb{F}_p, t^9 \neq t.$$

By (4), to prove our assertion, we have to calculate the difference between $\#C_2(t)(\mathbb{F}_p)$ and $\#C_3(t)(\mathbb{F}_p)$ for $t \in \mathbb{F}_p$, $t^9 \neq t$. The calculation of $\#C_2(0)(\mathbb{F}_p)$ and $\#C_3(0)(\mathbb{F}_p)$ is very easy. Thus we have

$$\begin{aligned} \#C_2(0)(\mathbb{F}_p) &= \begin{cases} p+1 & if\ p \equiv 3 \bmod 4 \qquad p \neq 3 \\ 3p+1 & if\ p \equiv 1 \bmod 4. \end{cases} \\ \#C_3(0)(\mathbb{F}_p) &= p+1. \end{aligned} \tag{5}$$

Let $t \in \mathbb{F}_p$, $t^8 = 1$. First we shall calculate $\#C_2(t)(\mathbb{F}_p)$. In this case, the curve $C_2(t)$ is defined by $Z \cdot E^2 = -3 \cdot t^6 \cdot H^2 \cdot Z + 3 \cdot t^3 \cdot H \cdot Z^2 - Z^3$. If $Z = 0$, this equation has $p+1$ $\mathbb{F}_p$-rational points. Suppose $Z \neq 0$. Since we work in $\mathbb{P}^2$, we may assume $Z = 1$. The equation becomes

$$E^2 = -3 \cdot t - 6 \cdot H^2 + 3 \cdot t^3 \cdot H - 1 = -3 \cdot (t^3 \cdot (H + \frac{1}{2}t^5))^2 - \frac{1}{4}.$$

The number of $\mathbb{F}_p$-rational solutions of the equation is given by Jacobi sums, that is,

$$\#\{C_2(t)(\mathbb{F}_p) \cap \{Z = 1\}\} = p + (\frac{3}{p}) \cdot J((\frac{-}{p}), (\frac{-}{p})),$$

where $(\frac{-}{p})$ denotes Legendre symbol modulo p and $J(\ ,\ )$ is the associated Jacobi symbol. By Theorem 1 on p. 93 in [4], we have

$$J((\frac{-}{p}), (\frac{-}{p})) = -(\frac{-1}{p}).$$

Therefore we see

$$\#C_2(t)(\mathbb{F}_p) = 2p + 1 - (\frac{-3}{p}). \tag{6}$$

Next we shall calculate $\#C_3(t)(\mathbb{F}_p)$. By the same argument as in case of $\#C_2(t)(\mathbb{F}_p)$, we have

$$\#\{C_3(t)(\mathbb{F}_p) \cap \{Z = 0\}\} = 1,$$

$$\begin{aligned} \#\{C_3(t)(\mathbb{F}_p) \cap \{Z = 1\}\} &= \sum_{X' \in \mathbb{F}_p} (1 + (\frac{X'^3 - 3 \cdot t^6 \cdot X'^2}{p})) \\ &= p + \sum_{w \neq 0, -3t^6} (\frac{w}{p}) = p - (\frac{-3}{p}). \end{aligned}$$

Therefore

$$\#C_3(t)(\mathbb{F}_p) = p + 1 - (\frac{-3}{p}). \tag{7}$$

Since the number N of solutions of $t^8 = 1$ in $\mathbb{F}_p$ is given by

$$N = \begin{cases} 2 & if\ p \equiv 3 \bmod 4, \\ 4 & if\ p \equiv 5 \bmod 8, \\ 8 & if\ p \equiv 1 \bmod 8, \end{cases}$$

we have, by (3) $\sim$ (7),

$$\sum_{t\in\mathbb{F}_p}\{\#C_1(t)(\mathbb{F}_p)-\#\mathcal{E}(t)(\mathbb{F}_p)\}=\begin{cases}2p & if\ p\equiv 3 \bmod 4,\\ 6p & if\ p\equiv 5 \bmod 8,\\ 10p & if\ p\equiv 1 \bmod 8.\end{cases} \tag{8}$$

Hence by (4), we have Proposition 1. □

To calculate $\#S(\mathbb{F}_p)$, we need some results for generalized Jacobi sums. For non-trivial character χ_1, χ_2 and χ_3 of $\mathbb{F}_p^*$, the generalized Jacobi sum $J(\chi_1,\chi_2,\chi_3)$ is defined by

$$J(\chi_1,\chi_2,\chi_3)=\sum_{t_1+t_2+t_3=1\ t_i\in\mathbb{F}_p}\chi_1(t_1)\cdot\chi_2(t_2)\cdot\chi_3(t_3).$$

Lemma 1. *If χ_1, χ_2, χ_3 and $\chi_1\cdot\chi_2\cdot\chi_3$ are non-trivial, then*

$$J(\chi_1,\chi_2,\chi_3)=\begin{cases}\chi_1(-1)\cdot p & if\ \chi_1\cdot\chi_2\ \textit{is trivial},\\ J(\chi_1,\chi_2)\cdot J(\chi_1\cdot\chi_2,\chi_3) & if\ \chi_1\cdot\chi_2\ \textit{is non-trivial}.\end{cases}$$

Proof. By Theorem 3 in Chapter 8 of [4], we have

$$J(\chi_1,\chi_2,\chi_3)=\frac{g(\chi_1)\cdot g(\chi_2)\cdot g(\chi_3)}{g(\chi_1\cdot\chi_2\cdot\chi_3)},$$

where $g(\chi_1),\ldots,g(\chi_1\cdot\chi_2\cdot\chi_3)$ are Gaussian sums. If $\chi_1\cdot\chi_2$ is trivial, then

$$J(\chi_1,\chi_2,\chi_3)=g(\chi_1)\cdot g(\overline{\chi_1})=\chi_1(-1)\cdot p$$

by the well-known property of Gaussian sums. If $\chi_1\cdot\chi_2$ is non-trivial, then by Theorem 1 in Chapter 8 of [4],

$$J(\chi_1,\chi_2)=\frac{g(\chi_1)\cdot g(\chi_2)}{g(\chi_1\cdot\chi_2)},$$

$$J(\chi_1\cdot\chi_2,\chi_3)=\frac{g(\chi_1\cdot\chi_2)\cdot g(\chi_3)}{g(\chi_1\cdot\chi_2\cdot\chi_3)}.$$

This shows our assertion. □

Lemma 2. *Let p be a prime number such that $p\equiv 1 \bmod 4$ and χ a character of $\mathbb{F}_p^*$ of order 4. Let a and b be integers such that $p=a^2+b^2$, $b\equiv 1 \bmod 4$. Then*

$$J(\chi,\chi^2)=-(b+a\cdot\sqrt{-1}),\qquad J(\chi,\chi)=-\chi(-1)\cdot(b+a\cdot\sqrt{-1}).$$

Proof. See p.106 of [4]. □

Proposition 2.

$$\#S(\mathbb{F}_p)=\begin{cases}p^2+2p+1 & if\ p\equiv 3 \bmod 4,\\ p^2+10p+1+4b^2 & if\ p\equiv 5 \bmod 8,\\ p^2+18p+1+4b^2 & if\ p\equiv 1 \bmod 8.\end{cases}$$

Proof. Let N_0 be the number of $\mathbb{F}_p$-rational points on the hyper surface $A^4 + B^4 - C^4 - D^4 = 0$ in affine space $\mathbf{A}^4$. Then we have

$$\#S(\mathbb{F}_p) = (N_0 - 1)/(p-1). \tag{9}$$

Let $d = (p-1, 4)$. Then by Weil [5], we know

$$N_0 = p^3 + (p-1) \cdot \sum_{(i,j,k,l)} \chi^j(-1) \cdot J(\chi^j, \chi^k, \chi^l), \tag{10}$$

where (i, j, k, l) in the summation runs over all 4-tuples of integers such that

$$0 < i, j, k, l, < d, \qquad i + j + k + l \equiv 0 \bmod d,$$

and χ is a character of $\mathbb{F}_p^*$ of order d with $\chi(0) = 0$. Let $p \equiv 3 \bmod 4$. Then $d = 2$ and χ is the Legendre symbol. We have by (9), (10) and Lemma 1,

$\#S(\mathbb{F}_p) = p^2 + p + 1 + \chi(-1) \cdot J(\chi, \chi, \chi) = p^2 + p + 1 + \chi(-1)^2 \cdot p = p^2 + 2p + 1.$

Let $p \equiv 1 \bmod 4$. Then $d = 4$ and we have by (9), (10),

$$\#S(\mathbb{F}_p) = p^2 + p + 1 + \sum_{0<i,j,k,l<4,\ i+j+k+l\equiv 0 \bmod 4} \chi^j(-1) \cdot J(\chi^j, \chi^k, \chi^l).$$

Since $\overline{J(\chi^j, \chi^k, \chi^l)} = J(\chi^{4-j}, \chi^{4-k}, \chi^{4-l})$, the sum

$$\sum_{0<i,j,k,l<4,\ i+j+k+l\equiv 0 \bmod 4} \chi^j(-1) \cdot J(\chi, \chi^k, \chi^l) \tag{11}$$

equals to

$$2 \cdot \sum_{0<i,k,l<4,\ i+k+l\equiv 3 \bmod 4} \Re\{\chi(-1) \cdot J(\chi, \chi^k, \chi^l)\} + \sum_{0<i,k,l<4,\ i+k+l\equiv 2 \bmod 4} J(\chi^2, \chi^k, \chi^l), \tag{12}$$

where $\Re\{z\}$ denotes the real part of a complex number z. The first sum of (12) is equals to

$$\sum_{k=1}^{3} \Re\{\chi(-1) \cdot J(\chi, \chi^k, \chi^k)\} + 2 \cdot \sum_{1\le k<l\le 3,\ (k,l)\neq(1,2)} \Re\{\chi(-1) \cdot J(\chi, \chi^k, \chi^l)\}$$

$$= 2b^2 - p + p + p \cdot \chi(-1) + 4 \cdot p = 2 \cdot b^2 + (4 + \chi(-1)) \cdot p,$$

using Lemma 1 and Lemma 2. The second sum is equal to

$$\begin{aligned} J(\chi^2, \chi^2, \chi^2) + 2 \cdot \sum_{1\le k\le l\le 3} J(\chi^2, \chi^k, \chi^l) &= p + 2 \cdot (2p + \chi^3(-1) \cdot p) \\ &= p \cdot (5 + 2 \cdot \chi(-1)). \end{aligned}$$

Hence we have

$$\begin{aligned} \#S(\mathbb{F}_p) &= p^2 + p + 1 + 2 \cdot (2b^2 + 4p + p \cdot \chi(-1)) + 5p + 2 \cdot \chi(-1) \cdot p \\ &= p^2 + (14 + 4 \cdot \chi(-1)) \cdot p + 1 + 4b^2. \end{aligned}$$

This shows our assertions. □

Acknowledgement. The author would like to express his hearty thanks to Professor Noburo Ishii of Osaka Prefecture University and Professor Yoshio Mimura of Osaka Electro and Communication University for their advices in revising this note.

References

1. B. Birch and H. P. F. Swinnerton-Dyer, Notes on elliptic curves (I),(II), J. Reine Angew. Math **212** (1963),p.7–25, **218** (1965), p.79–108.
2. J.W.S. Cassels and A. Schinzel, Selmer's conjecture and families of elliptic curves, Bull. London Math. Soc., **14**, (1982), 345–348.
3. E. Hecke, Eine neue Art von Zeta functionen und ihre Beziehungen zur Verteilung der Primzahlen. Math. Zeitschr., **6** (1920), p.11–51.
4. K. Ireland and M. Rosen, A classical introduction to modern number theory Graduate text in Math., **84**, Springer-Verlag, New York (1972).
5. N. Koblitz, Introduction to Elliptic curves and modular forms, Graduate texts in Math.. **97**, Springer, (second edition) (1993)
6. M. Kuwata, Mordell-Weil groups and elliptic K3-surfaces, Dr. Thesis of Brown University (1989).
7. K. Nagao, Construction of high-rank elliptic curves, Kobe J. Math, **11** (1994), 211–219.
8. T. Shioda, Construction of elliptic curves with high-rank via the invariants of the Weyl groups, J. Math. Soc. Japan **43** (1991) p.673–719.
9. J. Tate, Algebraic cycles and poles of zeta functions, Arithmetic Algebraic Geometry, ed. Schlling, Harper and Row, (1965), p.93-111.

This article was processed by the author using the LaTeX style file *cljour1* from Springer-Verlag.