T. HISAMATSU
KODAI MATH. J.
12 (1989), 339—345

A REMARK ABOUT THE TANIYAMA-WEIL CONJECTURE FOR AN ELLIPTIC CURVE DEFINED BY AN EQUATION $y^2=x^3+D^2x+D^3$

BY TATSUO HISAMATSU

For an elliptic curve over Q the conjecture of Taniyama-Weil is stated as follows. (As for notations and terminologies, see [1] or [2].)

CONJECTURE (Taniyama-Weil) *Let E be an elliptic curve over Q. Let N be its conductor, and let*

$$L(E\,;s)=\sum_{n=1}^{\infty}a(n)n^{-s},\quad (Re(s)>\frac{3}{2})$$

be its L-function. Then the function

$$f_E(z)=\sum_{n=1}^{\infty}a(n)e(nz),\quad (e(z)=e^{2\pi iz})$$

of z in the upper half plane, is a cusp form of weight 2 for the congruence subgroup $\Gamma_0(N)$ of the modular group $SL(2, Z)$, which is an eigenfunction for the Hecke operators $T(p)$ (p prime number).

Let D be a nonzero integer and let $E(D)$ be an elliptic curve defined by an equation

$$y^2=x^3+D^2x+D^3.$$

In this paper, we give a remark about the Taniyama-Weil conjecture for the elliptic curve $E(D)$.

THEOREM. *The following are equivalent.*
(a) *The conjecture is true for all $E(D)$.*
(b) *The conjecture is true for $E(-1)$.*

We shall divide the proof in the four steps.

1. For a prime number p, we denote by $E(D)_{(p)}$ the reduction of $E(D)$ at p and put

$$a_D(p)=1+p-\mathrm{Card}\,E(D)_{(p)}(F_p).$$

Received November, 7, 1988.

Notation. For an integer a and a non-zero integer b, we denote $\left(\frac{a}{b}\right)$ the "quadratic residue symbol" which is characterized by the following properties.

(i) $\left(\frac{a}{b}\right)=0$ if $(a, b)\neq 1$ or b is even.

(ii) If b is an odd prime, $\left(\frac{a}{b}\right)$ coincides with the ordinary quadratic residue symbol.

(iii) $\left(\frac{a}{-1}\right)=\mathrm{sign}(a)$ or 0 according as $a\neq 0$ or $a=0$.

Then we have

(iv) If $b>0$, the map $a\mapsto\left(\frac{a}{b}\right)$ defines a character modulo b.

(v) If $a\neq 0$, the map $b\mapsto\left(\frac{a}{b}\right)$ defines a character.

PROPOSITION 1. *For any prime number p, we have*

$$a_D(p)=\left(\frac{a}{b}\right)a_1(p). \tag{1}$$

Proof. First, assume that $E(D)$ has good reduction at p, namely p does't divide the discriminant Δ_D of $E(D)$, where $\Delta_D=-2^4 31D^6=-496D^6$. We denote by $A_D(p)$ the coefficient of x^{p-1} in $(x^3+D^2x+D^3)^{(p-1)/2}$. Simple calculations show

$$A_D(p)=\left(\sum_{n\in Z,\frac{p-1}{4}\leqq n\leqq\frac{p-1}{3}}\frac{\frac{p-1}{2}!}{\left(2n-\frac{p-1}{2}\right)!(p-1-3n)!\,n!}\right)D^{\frac{p-1}{2}}.$$

Moreover, as in the proof of Theorem 4.1 in [2], we have $a_D(p)\equiv -A_D(p)$ (mod p). This result and the Riemann hypothesis for $E(D)_{(p)}$, saying $|a_D(p)|\leqq 2\sqrt{p}$, imply $a_D(p)=\left(\frac{D}{p}\right)a_1(p)$ for $p\geqq 17$.

We show that (1) is also true for $p<17$.

If $p=3$ and $3\nmid D$, then $A_D(3)=0$, so that $a_D(3)=-3$, 0 or 3. Since a congruence equation $x^3+D^2x+D^3\equiv 0$ (mod 3) has a solution $x=D$, Card $E(D)_{(3)}(F_3)$ must be an even integer. Thus $a_D(3)=0$.

If $p=5$ and $5\nmid D$, then $A_D(5)=2D^2$. For D such as $\left(\frac{D}{5}\right)=1$ (resp. $\left(\frac{D}{5}\right)=-1$), we have $2D^2\equiv 2$ (mod. 5) (resp. $2D^2\equiv -2$ (mod 5)). Thus $a_D(5)=-3$ or 2 (resp. $a_D(5)=-2$ or 3). Since the following three polynomials

$$x^3+D^2x+D^3\equiv\begin{cases} x^3+x+1\left(\left(\frac{D}{5}\right)=1\right), \\ x^3-x-2\ (D\equiv 2\ (\mathrm{mod}\ 5)), \\ x^3-x+2\ (D\equiv 3\ (\mathrm{mod}\ 5))\end{cases}$$

have no roots modulo 5, $\operatorname{Card} E(D)_{(5)}(F_5)$ must be odd, thus $a_D(5)=\left(\frac{D}{5}\right)\cdot(-3)$.

If $p=7$ and $7 \nmid D$, then $A_D(7)=3D^3$. As above,

$$x^3+D^2x+D^3\equiv\begin{cases} x^3+x+\left(\frac{D}{7}\right) & (D\equiv 1,\, 6 \pmod 7), \\ x^3+4x+\left(\frac{D}{7}\right) & (D\equiv 2,\, 5 \pmod 7), \\ x^3+2x+\left(\frac{D}{7}\right) & (D\equiv 3,\, 4 \pmod 7) \end{cases}$$

have no roots modulo 7, $\operatorname{Card} E(D)_{(7)}(F_7)$ must be odd. Thus $a_D(7)=\left(\frac{D}{7}\right)\cdot 3$.

If $p=11$ and $11 \nmid D$, we have $A_D(11)=20D^5$ and $|a_D(11)|\leqq 2\sqrt{11}<2\cdot 4=8$. Thus $a_D(11)=\left(\frac{D}{11}\right)\cdot(-2)$.

Finally, if $p=13$ and $13 \nmid D$, we have $A_D(13)=35D^6$ and $|a_D(13)|\leqq 2\sqrt{13}<8$. Thus $a_D(13)=\left(\frac{D}{13}\right)\cdot(-4)$.

Therefore (1) is true for $p<17$.

Next, assume that $E(D)$ has bad reduction at p, namely $p\,|\,\Delta_D$. If $p\,|\,2\cdot D$, then $E(D)$ has additive reduction at p and $a_D(p)=0$. On the other hand, if $p=31$ and $31 \nmid D$, then $E(D)$ has multiplicative reduction at 31 and $a_D(31)=1$ or -1 according as $\left(\frac{D}{31}\right)=-1$ or 1, respectively. (cf. [2; Prop. 5.1].)

Finally, we have (1) for all prime numbers.

2. Suppose N_D is the conductor of $E(D)$. This quantity can be explicitly computed by using the algorithm of Tate ([4]). The result is as follows.

(2)

	$31 \nmid D$	$31\,|\,D$
$2 \nmid D$, $D\equiv 1 \pmod 4$	$2^4 31 D_0^2$	$2^4 D_0^2$
$2 \nmid D$, $D\equiv -1 \pmod 4$	$2^3 31 D_0^2$	$2^3 D_0^2$
$2\,|\,D$	$2^4 31 D_0^2$	$2^4 D_0^2$

where

(3) $$D_0=\operatorname{sign}(D)\prod_{\substack{p \text{ prime number} \\ \operatorname{ord}_p(D)\equiv 1 \pmod 2}} p.$$

3. We define a function $\Psi_D\colon Z\to\{1, 0, -1\}$ by

$$\Psi_D(0)=0, \quad \Psi_D(a)=\left(\frac{-D}{a}\right) \quad (a\neq 0).$$

PROPOSITION 2.

(i) *If* $D\equiv 1 \pmod 4$, *then* Ψ_D *is a primitive character* $\bmod 2^2D_0$.

(ii) *If* $D\equiv -1 \pmod 4$, *then* Ψ_D *is a primitive character* $\bmod 2D_0$.

(iii) *If* $2|D$, *then* Ψ_D *is a primitive character* $\bmod 2^2D_0$.

Proof. We have $\Psi_D=\Psi_{D_0}$ by (3) and we can see the equivalence of $D\equiv\pm 1 \pmod 4$ and $D_0\equiv\pm 1 \pmod 4$. Therefore, it is enough to prove the proposition in the case of $D=D_0$, namely, square-free D.

Assume that a and $2D$ are relatively prime. First we prove

$$\Psi_D(a+4|D|)=\Psi_D(a). \tag{4}$$

By the definition of Ψ_D, we have

$$\Psi_D=\Psi_{\mathrm{sign}(D)}\prod_{\substack{p \text{ prime number}\\ p|D}}\Psi_{-p}. \tag{5}$$

For each factor in the right hand side of (5), we check (4) in the cases

$$\begin{cases} \text{i)} & a+4|D|>0 \text{ and } a>0. \\ \text{ii)} & a+4|D|>0 \text{ and } a<0. \\ \text{iii)} & a+4|D|<0 \text{ (so } a<0). \end{cases} \qquad \begin{cases} 1) & D>0. \\ 2) & D<0. \end{cases}$$

Assume D is *odd*.

$\Psi_{\mathrm{sign}(D)}(a+4|D|)$; In the case 2), $\Psi_{\mathrm{sign}(D)}=\Psi_{-1}$ is a trivial character, thus

$$\Psi_{\mathrm{sign}(D)}(a+4|D|)=\Psi_{\mathrm{sign}(D)}(a)$$

is always true. In the case i)-1),

$$\Psi_{\mathrm{sign}(D)}(a+4|D|)=\left(\frac{-1}{a+4|D|}\right)=(-1)^{\frac{a-1}{2}}=\left(\frac{-1}{a}\right)=\Psi_{\mathrm{sign}(D)}(a),$$

in the case ii)-1),

$$\begin{aligned}\Psi_{\mathrm{sign}(D)}(a+4|D|)&=\left(\frac{-1}{a+4|D|}\right)=(-1)^{\frac{a-1}{2}}=-(-1)^{\frac{-a-1}{2}}=-\Psi_{\mathrm{sign}(D)}(-a)\\ &=\Psi_{\mathrm{sign}(D)}(-1)\Psi_{\mathrm{sign}(D)}(-a)\\ &=\Psi_{\mathrm{sign}(D)}(a),\end{aligned}$$

in the case iii)-1),

$$\begin{aligned}\Psi_{\mathrm{sign}(D)}(a+4|D|)&=\Psi_{\mathrm{sign}(D)}(-1)\Psi_{\mathrm{sign}(D)}(-a-4|D|)\\ &=\Psi_{\mathrm{sign}(D)}(-1)\Psi_{\mathrm{sign}(D)}(-a)\\ &=\Psi_{\mathrm{sign}(D)}(a).\end{aligned}$$

So we have

$$\Psi_{\mathrm{sign}(D)}(a+4|D|)=\Psi_{\mathrm{sign}(D)}(a)$$

for all cases.

$\Psi_{-p}(a+4|D|)$; In the case i),

$$\Psi_{-p}(a+4|D|)=\left(\frac{p}{a+4|D|}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}\left(\frac{a}{p}\right)=\left(\frac{p}{a}\right)=\Psi_{-p}(a)$$

by the quadratic reciprocity law. Similarly, in the case ii),

$$\begin{aligned}\Psi_{-p}(a+4|D|)&=\left(\frac{p}{a+4|D|}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}\left(\frac{a}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{-a-1}{2}}\left(\frac{-a}{p}\right)=\left(\frac{p}{-a}\right)\\&=\Psi_{-p}(-a)=\Psi_{-p}(-1)\Psi_{-p}(a)\\&=\Psi_{-p}(a),\end{aligned}$$

and in the case iii),

$$\Psi_{-p}(a+4|D|)=\Psi_{-p}(-1)\Psi_{-p}(-a-4|D|)=\Psi_{-p}(-a)=\Psi_{-p}(a).$$

By these results and by (5), we have (4) if D is odd. Similar computations show

$$\Psi_D(a+2|D|)=\Big[\Psi_D(-1)\prod_{\substack{p \text{ prime number}\\ p|D}}(-1)^{\frac{p-1}{2}}\Big]\Psi_D(a). \tag{6}$$

If we put

$$t=\mathrm{Card}\{p\,|\,\text{prime number, } p|D \text{ and } p\equiv -1 \pmod 4\},$$

then whether t is even or odd is as follows.

(7)

	$D\equiv 1 \pmod 4$	$D\equiv -1 \pmod 4$
$D>0$	even	odd
$D<0$	odd	even

By (6) and (7),

$$\Psi_D(a+2|D|)=\Psi_D(a)$$

if and only if $D\equiv -1 \pmod 4$. Thus we have (i) and (ii).

Assume D is even. As for about Ψ_{-2}, in the case (i),

$$\Psi_{-2}(a+4|D|)=\left(\frac{2}{a+4|D|}\right)=(-1)^{\frac{(a+4|D|)^2-1}{8}}=(-1)^{\frac{a^2-1}{8}}=\left(\frac{2}{a}\right)=\Psi_{-2}(a),$$

in the case ii),

$$\Psi_{-2}(a+4|D|)=(-1)^{\frac{a^2-1}{8}}=\left(\frac{2}{-a}\right)=\Psi_{-2}(-a)=\Psi_{-2}(a),$$

and in the case iii),

$$\Psi_{-2}(a+4|D|)=\Psi_{-2}(-a-4|D|)=\Psi_{-2}(-a)=\Psi_{-2}(a).$$

From these results, we know that

$$\Psi_D(a+4|D|)=\Psi_D(a)$$

is also true for even D. The similar calculations show

$$\Psi_D(a+2|D|)=-\Psi_D(a).$$

Thus Ψ_D is a primitive character mod 2^2D_0. Finally we have (iii).

This completes the proof.

By Proposition 1 and the definition of Ψ_D, for any positive integer n, we have

$$a_D(n)=\Psi_D(n)a_{-1}(n). \tag{8}$$

4. *Proof of Theorem.* Assume that the Conjecture is true for $E(-1)$. We apply the following fact from [1].

THEOREM. *Let N be a positive integer, s be a divisor of N and m be an integer and we put*

$$N'=l.c.m.\ (N, m^2, ms).$$

Let Ψ, χ be a primitive Dirichret character mod m, mod s, *respectively. For*

$$f(z)=\sum_{n=1}^{\infty} a(n)e(nz)\in S_k(N, \chi) \quad (\textit{Fourier expansion of } f \textit{ at } i\infty), \tag{9}$$

we define

$$f_\Psi(z)=\sum_{n=1}^{\infty}\Psi(n)a(n)e(nz).$$

Then $f_\Psi(z)\in S_k(N', \Psi^2\chi)$.

[1; Prop. 3. 64].

If we put $N=N_{-1}=2^3 31=248$, $\Psi=\Psi_D$ and $\chi=1$ (trivial character), then N' coincides with N_D. So $f_{E(D)}$ belongs to $S_k(\Gamma_0(N_D))$.

For an positive integer m, denote by $T(m)$ the m-th Hecke operator. The operation of $T(m)$ on $f(z)$ of (9) in the case $\chi=1$ is

$$(T(m)f)(z)=\sum_{n=1}^{\infty} a(n, T(m)f)e(nz),\ a(n, T(m)f=\sum_{\substack{d\mid(m,n)\\ d>0}} d^{k-1}a\left(\frac{np}{d^2}\right).$$

From the hypothesis for $f_{E(-1)}$, for each prime number p,

$$T(p)f_{E(-1)}=a_{-1}(p)f_{E(-1)}$$

holds, so that

$$a(n,\ T(p)f_{E(D)})=\sum_{\substack{d\mid(p,n)\\ d>0}} d\,a\left(\frac{np}{d^2},\ f_{E(D)}\right)=\sum_{\substack{d\mid(p,n)\\ d>0}} d\Psi_D\left(\frac{np}{d^2}\right)a_{-1}\left(\frac{np}{d^2}\right),$$

If $p \nmid n$, then

$$=\Psi_D(np)a_{-1}(np)=a_D(p)a_D(n).$$

Otherwise, if $p\mid n$, then by using the expression $n=mp^k$ $((p,\ m)=1)$,

$$\begin{aligned}
&=\Psi_D(mp^{k+1})a_{-1}(mp^{k+1})+p\Psi_D(mp^{k-1})a_{-1}(mp^{k-1})\\
&=a_D(m)\Psi_D(p^{k+1})[a_{-1}(p^{k+1})+pa_{-1}(p^{k-1})]\\
&=a_D(m)\Psi_D(p^{k+1})\cdot a_{-1}(p^k)a_{-1}(p)\\
&=a_D(p)a_D(n).
\end{aligned}$$

Therefore we have

$$T(p)f_{E(D)}=a_D(p)f_{E(D)}.$$

This implies that the Conjecture is true for $E(D)$ also.

References

[1] Shimura, G., Introduction to the Arithmetic Theory of Automorphic Functions. Publ. Math. Soc. Japan 11, Iwanami Shoten Publishers and Princeton Univ. Press (1971).

[2] Silverman, J., The Arithmetic of Elliptic Curves, Springer-Verleg 1985.

[3] Tate, J., The arithmetic of elliptic curves. Invent. Math. **23** (1974), 179-206.

[4] Tate, J., Algorithm for determining the type of a singular fiber in an elliptic pencil. Modular Functions of One Variable IV Lecture Notes in Math. 476, Springer-Verlag, 1975, 33-52.

Department of Mathematics
Tokyo Institute of Technology