RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

TAIRA HONDA

Invariant differentials and *L*-functions. Reciprocity law for quadratic fields and elliptic curves over Q

Rendiconti del Seminario Matematico della Università di Padova, tome 49 (1973), p. 323-335

<http://www.numdam.org/item?id=RSMUP_1973__49__323_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 49 (1973)

Invariant Differentials and L-Functions.
—Reciprocity Law for Quadratic Fields and Elliptic Curves over Q.—

TAIRA HONDA (*)

1. There are two kinds of Dirichlet series in number theory. Among one kind of series there are L-functions with class- and Grössen-character and Dirichlet series defined by Hecke operators. They are defined as infinite sums, continued analytically throughout the whole plane, and satisfy functional equations of ordinary type. Let us call these *L-functions of Hecke type*. To the other kind of series belong Artin L-functions in algebraic number theory and zeta-functions of algebraic varieties defined over finite algebraic number fields. To get them one first defines their local factors and then the whole series as Euler products. We shall call such an L-function an *L-function of Artin type*.

In many cases one cannot obtain analytic properties of an L-function of Artin type immediately from its definition and it often comes as an important problem to prove that it is also of Hecke type. For example the fact that an Artin L-function with respect to a relatively abelian number field is also a Hecke L-function with a suitable class-character is known as reciprocity law and was proved by Artin. Hasse conjectured that the L-function of an elliptic curve defined over an algebraic number field would be of Hecke type and Weil [6] gave a more detailed conjecture about an elliptic curve over the ra-

(*) Indirizzo dell'A.: Dept. of Mathematics - Osaka University - Toyonaka, Osaka, 560 Giappone.

tional number field Q in connection with Dirichlet series defined by Hecke operators with respect to $\Gamma_0(N)$.

In the previous papers [3] and [4] we showed that the canonical invariant differential on a (one-dimensional) algebraic formal group over Z has an intimate connection with the L-function of Artin type of this algebraic group. In the present article we try to connect this invariant differential directly with a suitable L-function of Hecke type and thus to get a « reciprocity law » for this algebraic group.

First we apply this idea to the group $x+y+Sxy$, where S is a Gaussian sum with a quadratic character, and get a new interpretation and a proof of quadratic reciprocity law.

Secondly we confirm the Weil conjecture for several elliptic curves by this method. Although his conjecture for these curves has already been settled by other methods and our results are not new, one should note that in our method one needs formal groups and more analysis, but little algebraic geometry, and one has nothing to do with the number of rational points of reduced curves.

2. Let q be a fixed odd prime number and choose $\varepsilon = \pm 1$ so that $\varepsilon q \equiv 1 \pmod 4$. If we denote by p $(\neq q)$ a variable odd prime, the famous law of quadratic reciprocity reads

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2\cdot(q-1)/2} \tag{1}$$

or

$$\left(\frac{\varepsilon q}{p}\right) = \left(\frac{p}{q}\right). \tag{2}$$

The equivalence of (2) to (1) follows immediately from

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

Put $K = \mathbb{Q}(\sqrt{\varepsilon q})$. Then the left hand side of (2) is Artin symbol and indicates the behaviour of the prime p in K. We get the Artin L-function

$$L(s, K) = \prod_p \left(1 - \left(\frac{\varepsilon q}{p}\right) p^{-s}\right)^{-1} \tag{3}$$

which is the simplest L-function of Artin type, noting

$$\left(\frac{\varepsilon q}{2}\right) = (-1)^{(q^2-1)/8} \quad \text{and} \quad \left(\frac{\varepsilon q}{q}\right) = 0$$

as Artin symbol.

On the other hand the right-hand side of (2) is the quadratic character mod q. By putting

$$\chi(n) = \left(\frac{n}{q}\right), \quad \text{for } q \nmid n,$$
$$= 0, \quad \text{for } q \mid n,$$

we have the L-function of Hecke type

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}. \tag{4}$$

Since it is obvious that $L(s, \chi)$ has the Euler product

$$\prod_p (1 - \chi(p) p^{-s})^{-1},$$

(2) is equivalent to the fact that the two L-functions are the same thing (possibly except for 2-factors).

Now put $\zeta = \exp[2\pi i/q]$ and define the Gaussian sum:

$$S = \sum_{n=1}^{q} \chi(n) \zeta^n. \tag{5}$$

As it is well known, one can easily see that

$$\begin{cases} S^2 = \varepsilon q, \\ \sum_{n=1}^{q} \chi(n) \zeta^{mn} = \chi(m) S, \quad \text{for } m \in \mathbb{Z}. \end{cases} \tag{6}$$

From (6) we get $S = \pm\sqrt{\varepsilon q}$. To determine this sign is not so easy. But we do not need to know the sign of S in the following. Consider the formal group $F(x, y) = x + y + Sxy$. The canonical invariant differential on F (cf. [3]) is $dx/(1 + Sx)$. Let $\mathfrak{O}$ be the ring of integers in K.

THEOREM 1. *Let* $\varphi(x)\in K[[x]]$ *be the (unique) solution of the differential equation*

$$\frac{dy}{1+Sy}=\sum_{n=1}^{\infty}\chi(n)x^{n-1}dx \tag{7}$$

such that $\varphi(x)\equiv x \pmod{\deg 2}$. *Then* $\varphi(x)\in\mathfrak{O}[[x]]$.

PROOF. Put $P(x)=\prod_{a}(1-\zeta^a x)$ and $Q(x)=\prod_{b}(1-\zeta^b x)$, where a (resp. b) ranges over all quadratic residues (resp. non-residues) mod q. First we shall show that

$$\varphi(x)=\big(Q(x)-P(x)\big)/SP(x)\,. \tag{8}$$

Since $S=\sum_{a}\zeta^a-\sum_{b}\zeta^b$, it is obvious that $\varphi(x)\equiv x \pmod{\deg 2}$. Now

$$\begin{aligned}
\varphi'(x) &= S^{-1}(Q/P)' \\
&= \frac{Q}{SP}\left(\log\frac{Q}{P}\right)' \\
&= \frac{Q}{SP}\left(\sum_{a}\frac{-\zeta^a}{1-\zeta^a x}-\sum_{b}\frac{-\zeta^b}{1-\zeta^b x}\right) \\
&= \frac{Q}{SP}\left(\sum_{n=1}^{q}\frac{\chi(n)\zeta^n}{1-\zeta^n x}\right) \\
&= (Q/SP)\sum_{n=1}^{q}\chi(n)\sum_{m=1}^{\infty}\zeta^{mn}x^{m-1} \\
&= (Q/SP)\sum_{m=1}^{\infty}\left(\sum_{n=1}^{q}\chi(n)\zeta^{mn}\right)x^{m-1} \\
&= (Q/P)\sum_{m=1}^{\infty}\chi(m)x^{m-1}.
\end{aligned}$$

Therefore

$$\begin{aligned}
\frac{d\varphi(x)}{1+S\varphi(x)} &= \frac{(Q/P)\sum_{m=1}^{\infty}\chi(m)x^{m-1}dx}{1+S(Q-P)/SP} \\
&= \sum_{m=1}^{\infty}\chi(m)x^{m-1}dx\,.
\end{aligned}$$

To complete the proof we have only to show that the coefficients of φ are integral at the prime divisor of q in K. Let σ be the generator of $\mathrm{Gal}(K/\mathbb{Q})$. By (6), K is a quadratic subfield of $\mathbb{Q}(\zeta)$, and it is easy to see that $P(x), Q(x) \in K[[x]]$ and $P^\sigma = Q$, $Q^\sigma = P$. Consequently $(Q-P)^\sigma = -(Q-P)$, and the coefficients of $Q-P$ are of the form $c\sqrt{\varepsilon q}$, where $c \in \mathbb{Z}$. By (6) this shows that $\varphi(x) \in \mathfrak{O}[[x]]$, which completes the proof of our theorem.

Let $\mathfrak{p}$ be a prime divisor of p in K. We get the quadratic reciprocity law (2) easily from the fact that φ is $\mathfrak{p}$-integral. From our theorem follows:

$$\sum_{n=1}^{\infty} (-S)^{n-1} \varphi(x)^n / n = \sum_{n=1}^{\infty} \chi(n) x^n / n \,. \tag{9}$$

From (9) we easily see that $(-S)^{p-1}/p - \chi(p)/p$ is $\mathfrak{p}$-integral. But this implies

$$(\varepsilon q)^{(p-1)/2} \equiv \chi(p) \mod p \,,$$

which is equivalent to (2) by Euler's criterion.

3. Let C be an elliptic curve over $\mathbb{Q}$, defined by the equation

$$Y^2 + \lambda XY + \mu Y = X^3 + \alpha X^2 + \beta X + \gamma \quad (\lambda, \mu, \alpha, \beta, \gamma \in \mathbb{Z}) \tag{10}$$

in affine form. We may assume that C is a Weierstrass minimal model, namely a model whose discriminant is as small as possible in absolute value ([5]). For this model the reduction C_p of C mod p is an irreducible curve for every prime p. Following Weil [6] we define the local L-function $L_p(s, C)$ of C as follows:

(I) If C_p is non-singular, it has genus 1. We put

$$L_p(s, C) = (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

where $1 - a_p U + pU^2$ is the numerator of the zeta-function of C_p.

(II) If C_p has a node, we put $a_p = +1$ or -1 according as the tangents at this node are rational over $GF(p)$ or not, and define

$$L_p(s, C) = (1 - a_p p^{-s})^{-1} \,.$$

(III) If C_p has a cusp, we put

$$L_p(s, C) = 1 .$$

Now the L-function of C is the product of all $L_p(s, C)$;

$$L(s, C) = \prod_p L_p(s, C) .$$

Write $L(s, C) = \sum_{n=1}^{\infty} a_n n^{-s}$ and form

$$g(x) = \sum_{n=1}^{\infty} a_n x^n/n , \qquad G(x, y) = g^{-1}(g(x) + g(y)) .$$

Furthermore, let $F(x, y)$ be the formalization of the abelian variety C with respect to the parameter $t = X/Y$. We know that $F, G \in \mathbb{Z}[[x, y]]$ and that $F \approx G$ (strongly isomorphic) over $\mathbb{Z}$ (see [4], Theorem 9).

Let $f(x)$ be the transformer of $F(x, y)$, namely let $f(x)\mathbb{Q} \in [[x]]$ be such that $f(x) \equiv x \pmod{\deg 2}$ and $F(x, y) = f^{-1}(f(x) + f(y))$. Then we know that $\omega = f'(t)dt$ is the t-expansion of a differential of the first kind on C and that the differential equation

$$f'(y)dy = \sum_{n=1}^{\infty} a_n x^{n-1} dx$$

has a solution $y = \varphi(x) = x + \ldots$ in $\mathbb{Z}[[x]]$.

Now take a new parameter $v = t + \ldots \in \mathbb{Z}[[t]]$. Then $t = v + \ldots \in \mathbb{Z}[[t]]$. Let $h(v)dv$ be the v-expansion of ω. On the other hand, let $L(s) = \sum_{n=1}^{\infty} a'_n n^{-s} (a'_n \in \mathbb{Z})$ be an L-function (of Hecke type) with an Euler product of the form

$$(11) \qquad \begin{cases} L(s) = \prod_p L_p(s) , \\ L_p(s) = \prod_p (1 - a'_p p^{-s} + \eta'_p p^{1-2s})^{-1} . \end{cases}$$

THEOREM 2. *Suppose a formal power series* $\varphi(u) = u + \ldots \in [[\mathbb{Z}u]]$ *to satisfy*

$$h(\varphi(u))d\varphi(u) = \sum_{n=1}^{\infty} a'_n u^{n-1} du .$$

Then $L_p(s)=L_p(s, C)$ *in case* (I). *In case* (II) $p-a_pT$ *divides* $p-a_p'T+\eta_p'T^2$. *In case* (III) p *divides* a_p' *and* η_p'.

PROOF. We use the results of [4]. By the assumptions the formal group whose canonical invariant differential is $h(\varphi(x))d\varphi(x)$ is strongly isomorphic to F over $\mathbb{Z}$. Therefore the formal group $H(x, y)$ obtained from $L(s)$ ([4], § 6) is strongly isomorphic to F over $\mathbb{Z}$. Thus we see that $G\approx H$ over $\mathbb{Z}$. Now we consider G and H over $\mathbb{Z}_p$, the ring of p-adic integers. They correspond to special elements $p-a_pT+\eta_pT^2$ (where $\eta_p=1$ in case (I), $\eta_p=0$, $a_p=\pm 1$ in case (II) and $\eta_p=a_p=0$ in case (III)) and $p-a_p'T+\eta_p'T^2$ respectively ([4], Theorem 8). By Proposition 2.6 of [4], $p-a_pT+\eta_pT^2$ must divide $p-a_p'T+\eta_p'T^2$ for every p. Our theorem follows from this immediately.

4. In this Section we apply the above theorem to two simplest curves:

$$C_1\colon\ Y^2=X(X^2-1)\,,$$

$$C_2\colon\ Y^2=X^3+1\,.$$

First we recall some basic properties of the following three theta-functions:

$$\vartheta_2=\sum_{n=-\infty}^{\infty}q^{(n+\frac{1}{2})^2},\qquad \vartheta_3=\sum_{n=-\infty}^{\infty}q^{n^2},\qquad \vartheta_4=\sum_{n=-\infty}^{\infty}(-1)^n q^{n^2}.$$

We treat them only as formal power series of q. Consider

$$Q_0=\prod_{n=1}^{\infty}(1-q^{2n})\,,\qquad Q_1=\prod_{n=1}^{\infty}(1+q^{2n})\,,$$

$$Q_2=\prod_{n=1}^{\infty}(1+q^{2n-1})\,,\qquad Q_3=\prod_{n=1}^{\infty}(1-q^{2n-1})\,.$$

Then it is easy to see that

$$Q_1Q_2Q_3=1\,. \tag{12}$$

The ϑ_i can also be written as infinite products:

$$\vartheta_2=2q^{\frac{1}{4}}Q_0Q_1^2,\qquad \vartheta_3=Q_0Q_2^2,\qquad \vartheta_4=Q_0Q_3^2. \tag{13}$$

Now we have the famous identity of Jacobi:

$$\vartheta_2^4 + \vartheta_4^4 = \vartheta_3^4 . \tag{14}$$

It is also known that

$$\vartheta_3^4 = \Big(\sum_{n=-\infty}^{\infty} q^{n^2} \Big)^4$$

$$= 1 + 8 \sum_{n=1}^{\infty} a_4(n) q^n ,$$

where $a_4(n) = \sum_{\substack{d|n \\ d \not\equiv 0(4)}} d$. For a positive integer n, put $\sigma(n) = \sum_{d|n} d$ and $\sigma_2(n) = \sum_{\substack{d|n \\ d \not\equiv 0(2)}} d$. Write $n = 2^\nu m$, with $\nu \geqslant 0$ and an odd integer m. If $\nu = 0$, then $a_4(n) = \sigma(n) = \sigma_2(n)$. But if $\nu > 0$, then

$$a_4(n) = \sigma(m) + 2\sigma(m) = 3\sigma_2(n) .$$

Summing up, we get

$$\vartheta_3^4 = 1 + 8 \sum_{n=1}^{\infty} \{2 + (-1)^n\} \sigma_2(n) q^n . \tag{15}$$

By replacing q by $-q$ in (15) we get

$$\vartheta_4^4 = 1 + 8 \sum_{n=1}^{\infty} \{1 + (-1)^n 2\} \sigma_2(n) q^n . \tag{16}$$

From (14), (15) and (16) follows

$$\vartheta_2^4 = 16 \sum_{n=1}^{\infty} \sigma(2n-1) q^{2n-1} . \tag{17}$$

Now we consider the curve C_1. Its conductor is 2^5 (Ogg [5]). By a simple transformation C_1 is isomorphic to

$$C_1' : Y^2 = X(X^2 - 2^4)$$

over Q. It is a minimal model at every odd p and hence we can apply Theorem 2 to C_1' for $p \neq 2$. Take a parameter v such that $v^{-2} = x$. Then

$$t = \frac{X}{Y} = \frac{X}{\sqrt{X(X^2 - 2^4)}} = \frac{v}{\sqrt{1 - 2^4 v^4}} \in \mathbb{Z}v[[]] ,$$

as is easily checked; and $dv/\sqrt{1 - 2^4 v^4}$ is a differential of the first kind on C_1'.

We shall show that

$$\varphi(u) = u \prod_{n=1}^{\infty} (1 + u^{8n})^2 (1 + u^{4(2n-1)})^{-2}$$

satisfies

$$\frac{d\varphi(u)}{\sqrt{1 - 2^4 \varphi(u)^4}} = \prod_{n=1}^{\infty} (1 - u^{4n})^2 (1 - u^{8n})^2 du . \tag{18}$$

To apply theta-functions, we use the parameter q. We have

$$\begin{aligned} \frac{q\varphi'(q)}{\varphi(q)} &= 1 + 8 \prod_{n=1}^{\infty} \frac{2nq^{8n}}{1 + q^{8n}} - 8 \prod_{n=1}^{\infty} \frac{(2n-1) q^{8n-4}}{1 + q^{8n-4}} \\ &= 1 + 8 \prod_{m,n=1}^{\infty} (-1)^{m-1} 2n q^{8mn} - 8 \prod_{m,n=1}^{\infty} (-1)^{m-1} (2n-1) q^{4(2n-1)m} . \end{aligned}$$

Let C_n be the coefficient of q^{4n}. Then

$$C_n = 8 \sum_{\substack{d|n \\ d \equiv 0(2)}} (-1)^{(n/d)-1} d - 8 \sum_{\substack{d|n \\ d \equiv 1(2)}} (-1)^{(n/d)-1} d .$$

If n is odd, then $C_n = -8 \sum_{d|n} d = -8\sigma(n) = -8\sigma_2(n)$. If n is even, write $n = 2^\nu m$ (where $\nu > 0$, m odd). Then, for $\nu = 1$,

$$C_n = 8 \times 2\sigma(m) + 8\sigma_2(n) = 24\sigma_2(n) .$$

For $\nu \geqq 2$,

$$C_n = 8\left(2^\nu - \sum_{\mu=1}^{\nu-1} 2^\mu\right) \sigma_2(n) + 8\sigma_2(n) = 24\sigma_2(n) .$$

In each case

$$C_n = 8\{1 + (-1)^n 2\}\sigma_2(n)\,. \tag{19}$$

Thus we get

$$q\varphi'(q)/\varphi(q) = \vartheta_4^4(q^4) \tag{20}$$

from (16), (19).

Now, by (13),

$$\varphi(q) = qQ_1(q^4)^2/Q_2(q^4)^2\,,$$

and

$$2^4\varphi(q)^4 = (2q)^4Q_1(q^4)^8/Q_2(q^4)^8 = \vartheta_2(q^4)^4/\vartheta_3(q^4)^4\,.$$

Therefore, instead of (18), we have only to prove

$$\frac{\vartheta_4^4Q_1^2/Q_2^2}{\sqrt{1-(\vartheta_2/\vartheta_3)^4}} = \prod_{n=1}^{\infty}(1-q^n)^2(1-q^{2n})^2. \tag{21}$$

By (12), (13) and (14) the left hand side of (21) is

$$\vartheta_3^2\vartheta_4^2Q_1^2/Q_2^2 = Q_0^4Q_1^2Q_2^2Q_3^4 = Q_0^4Q_3^2$$
$$= \prod_{n=1}^{\infty}(1-q^{2n})^4(1-q^{2n-1})^2 = \prod_{n=1}^{\infty}(1-q^n)^2(1-q^{2n})^2\,,$$

which was to be proved.

Now put

$$\Gamma_0(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbf{Z});\ c \equiv 0 \pmod{N}\right\}$$

as usual, and denote by $g(\Gamma_0(N))$ the genus of the field of automorphic functions with respect to $\Gamma_0(N)$. It is perhaps known and can be shown without difficulty that

$$q\prod_{n=1}^{\infty}(1-q^{4n})^2(1-q^{8n})^2 \qquad (q = \exp[2\pi i\tau]) \tag{22}$$

is a cusp form of dimension -2 with respect to $\Gamma_0(2^5)$. Since $g(\Gamma_0(2^5))=1$ (see [1]), the Dirichlet series $L(s)$ with the same coefficients as (22) has an Euler product of the form (11) by Hecke [2]. Therefore, by Theorem 2 and (18) we have

$$L_p(s) = L_p(s, C_1) \qquad \text{for } p \neq 2 .$$

Moreover,

$$L_2(s, C_1) = 1 = L_2(s) ,$$

since C_1 mod 2 has a cusp. Hence we have

$$L(s, C_1) = L(s) ,$$

and the conjecture of Weil has been proved completely for C_1.

As for C_2 its conductor is 36, $g(\Gamma_0(36)) = 1$ and $q\prod_{n=1}^{\infty}(1-q^{6n})^4$ is a cusp form of dimension -2 with respect to $\Gamma_0(36)$. We take a curve

$$C_2' : Y^2 = X^3 + 2^6$$

which is isomorphic to C_2 over $\mathbf{Q}$, and a parameter v such that $v^{-2} = x$. Here we will prove that

$$\varphi(u) = u\prod_{n=1}^{\infty}(1+u^{6n})^4$$

satisfies

$$\frac{d\varphi(u)}{\sqrt{1+2^6\varphi(u)^6}} = \prod_{n=1}^{\infty}(1-u^{6n})^4 du \tag{23}$$

and omit all the other details, which will be left to the reader.

We have

$$\begin{aligned}\frac{u\varphi'(u)}{\varphi(u)} &= 1 + \sum_{n=1}^{\infty}\frac{24nu^{6n}}{1+u^{6n}} \\ &= 1 + 24\sum_{m,n=1}^{\infty}(-1)^{m-1}nu^{6mn} \\ &= 1 + 24\sum_{n=1}^{\infty}\sigma_2(n)x^{6n},\end{aligned}$$

since $\sum_{d|n}(-1)^{(n/d)-1}d=\sigma_2(n)$, which can be checked as before. Thus (23) is equivalent to

$$\frac{1+24\sum_{n=1}^{\infty}\sigma_2(n)q^n}{\sqrt{1+2^6q\prod_{n=1}^{\infty}(1+q^n)^{24}}}=\prod_{n=1}^{\infty}\left(\frac{1-q^n}{1+q^n}\right)^4. \tag{24}$$

Since

$$\begin{aligned}\prod_{n=1}^{\infty}(1-q^n)^4(1+q^n)^{-4}&=(Q_0Q_3/Q_1Q_2)^4,\\&=(Q_0Q_3^2)^4,\\&=\vartheta_4^4,\end{aligned}$$

(24) is transformed into

$$\left\{\left(1+24\sum_{n=1}^{\infty}\sigma_2(n)q^n\right)\Big/\vartheta_4^4\right\}^2-1=2^6q(Q_1Q_2)^{24}. \tag{25}$$

Recalling (15), (16) and (17),

$$\begin{aligned}&\left(1+24\sum_{n=1}^{\infty}\sigma_2(n)q^n\right)^2-\vartheta_4^8\\&=\left(1+24\sum_{n=1}^{\infty}\sigma_2(n)q^n+\vartheta_4^4\right)\left(1+24\sum_{n=1}^{\infty}\sigma_2(n)q^n-\vartheta_4^4\right)\\&=\left[2+16\sum_{n=1}^{\infty}\{2+(-1)^n\}\sigma_2(n)q^n\right]\times 32\sum_{n=1}^{\infty}\sigma(2n-1)q^{2n-1}\\&=2^2\vartheta_3^4\vartheta_2^4.\end{aligned}$$

Therefore the left hand side of (25) is

$$\begin{aligned}2^4\vartheta_3^4\vartheta_2^4/\vartheta_4^8&=2^6q(Q_1Q_2/Q_3^2)^8\\&=2^6q(Q_1Q_2)^{24},\end{aligned}$$

which completes the proof of (23).

It is known that $g(\Gamma_0(14))=g(\Gamma_0(15))=1$ (Fricke [1]). In his book the equations satisfied by the generators of automorphic func-

tion fields with respect to $\Gamma_0(14)$ and $\Gamma_0(15)$ are given in the form

$$Y^2 = P(X), \tag{26}$$

where $P(X)$ has coefficients in $\mathbf{Z}$ and is of fourth degree in each case. But in his book everything which appears in Theorem 2 is explicitly given for these curves (though parameters may not be normalized). So our method will be applicable to the curves (26) with a slight modification.

REFERENCES

[1] F. Fricke, *Die elliptischen Funktionen und ihre Anwendungen*, Leipzig and Berlin, 1922.

[2] E. Hecke, *Über Modulfunktionen und die Dirichletscher Reihen mit Eulerscher Produktentwickelung II*, Math. Ann., **114** (1937), 316-351; Mathematische Werke, 672-707.

[3] T. Honda, *Formal groups and zeta-functions*, Osaka J. Math., **5** (1958), 199-213.

[4] T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan, **22** (1970), 213-246.

[5] A. P. Ogg, *Abelian curves of 2-power conductor*, Proc. Camb. Phil. Soc., **62** (1966), 143-148.

[6] A. Weil, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann., **168** (1967), 149-156.

Manoscritto pervenuto in redazione il 7 novembre 1972.

Reciprocity law for quadratic fields and elliptic curves over Q.Â A relation between formal groups and reciprocity laws is studied following the approach initiated by Honda. Let Î¾ denote an mth primitive root of unity. For a character Ï‡ of order m, we define two one-dimensional formal groups over â„¤[Î¾] and prove the existence of an integral homomorphism between them with linear coefficient equal to the Gauss sum of Ï‡. This allows us to deduce a reciprocity formula for the mth residue symbol which, in particular, implies the cubic reciprocity law. View. Show abstract. Geometric proofs of reciprocity laws. Article. Sep 2005. Ordinary/supersingular elliptic curves over finite fields. The j-invariant of an elliptic curve. Supersingular elliptic curves.Â Let E/k be an elliptic curve over a eld of positive characteristic p. In Lecture 7 we proved that for any nonzero integer n, the multiplication-by-n map [n] is separable if and only if n is not divisible by p. This implies that the separable degree of the mulitplication-by-p map cannot be p2 = deg[p]