M. Koike
Nagoya Math. J.
Vol. 98 (1985), 109–115

# HIGHER RECIPROCITY LAW, MODULAR FORMS OF WEIGHT 1 AND ELLIPTIC CURVES

MASAO KOIKE

## §0. Introduction

In this paper, we study higher reciprocity law of irreducible polynomials $f(x)$ over $\boldsymbol{Q}$ of degree 3, especially, its close connection with elliptic curves rational over $\boldsymbol{Q}$ and cusp forms of weight 1. These topics were already studied separately in a special example by Chowla-Cowles [1] and Hiramatsu [2]. Here we bring these objects into unity.

Let

$\mathscr{C}_0 =$ the set of number fields $K$ over $\boldsymbol{Q}$ such that

(1) $K$ is a Galois extension over $\boldsymbol{Q}$ with $\mathrm{Gal}(K/\boldsymbol{Q}) \cong S_3$, the symmetric group of degree 3,

(2) $K$ contains an imaginary quadratic field $k$.

For any $K$ in $\mathscr{C}_0$, we can associate three other objects: (1) $f(x)$: irreducible polynomials over $\boldsymbol{Q}$ of degree 3, (2) $F(\tau)$: cusp forms of weight 1, (3) $E$: elliptic curves rational over $\boldsymbol{Q}$;
let

$\mathscr{C}_1 =$ the set of all irreducible polynomials $f(x)$ over $\boldsymbol{Q}$ of degree 3 whose splitting field $K_f$ over $\boldsymbol{Q}$ belongs to $\mathscr{C}_0$.

$\mathscr{C}_2 =$ the set of all normalized cusp forms $F(\tau)$ of weight 1 on $\Gamma_0(N)$ whose Mellin transform is $L$-function with an ideal character $\chi$ of degree 3 of imaginary quadratic field $k$ and the abelian extension $K_F$ over $k$ which corresponds to the kernel of $\chi$ belongs to $\mathscr{C}_0$.

$\mathscr{C}_3 =$ the set of all elliptic curves $E$ rational over $\boldsymbol{Q}$ such that the field $E_2$ generated by coordinates of 2-division points on $E$ belongs to $\mathscr{C}_0$.

Received March 17, 1984.

Therefore we can define maps $\varphi_i\colon \mathscr{C}_i \to \mathscr{C}_0\,(i = 1, 2, 3)$ as follows;

$$\varphi_1(f) = K_f, \quad \varphi_2(F) = K_F, \quad \varphi_3(E) = E_2\,.$$

For any $K$ in $\mathscr{C}_0$, let $f(x) \in \varphi_1^{-1}(K)$, $F(\tau) \in \varphi_2^{-1}(K)$ and $E \in \varphi_3^{-1}(K)$. Then our theorems give

( I ) the relation between the higher reciprocity law of $f(x)$ and Fourier coefficients of $F(\tau)$, which is called the arithmetic congruence relation.

(II) the relation between the higher reciprocity law of $f(x)$ and $L$-function of $E$.

(III) congruences modulo 2 between $F(\tau)$ and $L$-function of $E$.

These results are a generalization of an example given in [1] and [2].

The author would like to express his hearty thanks to Prof. Hiramatsu for giving him a lecture on this subject and invaluable conversation.

## §1. Proof of (I)

Hereafter we fix $K$ in $\mathscr{C}_0$. Let $f(x) = ax^3 + bx^2 + cx + d$ be an element in $\varphi_1^{-1}(K)$. Let $M$ be the product of all primes which appear in $a, b, c$ and $d$.

For any prime $p$, $p \nmid M$, put $f_p(x) = f(x) \bmod p$. Then $f_p(x)$ is a polynomial over $\boldsymbol{F}_p$, the finite field with $p$ elements, of degree 3. We define $\mathrm{Spl}\,\{f(x)\}$ to be the set of primes such that the polynomial $f_p(x)$ factors into a product of distinct linear polynomials over $\boldsymbol{F}_p$. By the higher reciprocity law for $f(x)$, we mean a rule to determine the set $\mathrm{Spl}\,\{f(x)\}$ up to finite set of primes.

Let $F(\tau) = \sum_{n=1}^{\infty} a(n)e[n\tau]$, $e[\tau] = \exp(2\pi\sqrt{-1}\tau)$, be a normalized cusp form of weight 1 in $\varphi_2^{-1}(K)$. Let $\chi$ be the non-trivial ideal character of $k$ corresponding to the abelian extension $K$ over $k$. Let $-D$ and $\mathfrak{f}$ denote the discriminant of $k$ and the conductor of $\chi$. Then

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

and $F(\tau)$ is a cusp form of weight 1 on $\Gamma_0(DN\mathfrak{f})$ with the character $(-D/*)$ where $N\mathfrak{f}$ denotes the norm of $\mathfrak{f}$ on $k$ over $\boldsymbol{Q}$. Let $\rho$ denote the complex conjugation. From the assumption, it follows that $\chi(\mathfrak{a})^\rho = \chi(\mathfrak{a}^\rho)$ for any integral ideal $\mathfrak{a}$ of $k$.

THEOREM 1 (arithmetic congruence relation). *Let $p$ be any prime such that $p \nmid M \cdot D \cdot N\mathfrak{f}$. Then we have*

$$\#\{\alpha \in \boldsymbol{F}_p \mid f_p(\alpha) = 0\} = a(p)^2 - \left(\frac{-D}{p}\right).$$

*Proof.* The proof is similar to that of Theorem 2 in [2]. Let $p$ be a prime as above. It is easily seen that

$a(p) = 0 \Longleftrightarrow (-D/p) = -1,$

$\Longleftrightarrow$ the splitting field of $f_p(x)$ over $\boldsymbol{F}_p$ is a quadratic extension over $\boldsymbol{F}_p$,

$\Longleftrightarrow f_p(x)$ has exactly 1 linear factor over $\boldsymbol{F}_p$.

Now we assume that $(-D/p) = 1$. Then $p$ decomposes into a product of two prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$ where $\mathfrak{p}'$ is the conjugate of $\mathfrak{p}$. It is clear that

$a(p) = 2 \Longleftrightarrow \chi(\mathfrak{p}) = 1,$

$\Longleftrightarrow \mathfrak{p}$ splits completely in $K$,

$\Longleftrightarrow f_p(x)$ has exactly 3 distinct linear factors over $\boldsymbol{F}_p$.

And also it is clear that

$a(p) = -1 \Longleftrightarrow \chi(\mathfrak{p}) = \omega$, a non-trivial cube root of unity,

$\Longleftrightarrow \mathfrak{p}$ remains prime in $K$.

$\Longleftrightarrow$ the splitting field of $f_p(x)$ over $\boldsymbol{F}_p$ is a cubic extension over $\boldsymbol{F}_p$,

$\Longleftrightarrow f_p(x)$ has no linear factor over $\boldsymbol{F}_p$.

Summarizing these results, we obtain a proof of Theorem 1. Q.E.D.

COROLLARY 1. $\mathrm{Spl}\,\{f(x)\}$ *coincides with the set*

$$\{p\colon prime \mid p \nmid M \cdot D \cdot N\mathfrak{f},\ a(p) = 2\}$$

*up to finite set of primes.*

*Proof.* This is obvious from Theorem 1. Q.E.D.

## §2. Proof of (II)

Let $E$ be an elliptic curve rational over $\boldsymbol{Q}$ in $\varphi_3^{-1}(K)$, which is defined by $y^2 = f(x)$ where $f(x)$ is a polynomial of degree 3 over $\boldsymbol{Q}$; $f(x) = ax^3 + bx^2 + cx + d$, $a, b, c, d \in \boldsymbol{Q}$. Let $N$ denote the conductor of $E$ over $\boldsymbol{Q}$. Let $E_2$ denote the field generated by the coordinates of 2-division points on $E$

over $\boldsymbol{Q}$. Then $E_2$ coincides with the splitting field of $f(x)$ over $\boldsymbol{Q}$. Let $p$ be an odd prime such that $p \nmid N$, and let $\tilde{E}_p$ denote the reduction modulo $p$ of $E$ which is an elliptic curve over $\boldsymbol{F}_p$. Let $N_p = N_p(E)$ denote the number of $\boldsymbol{F}_p$-rational points of $\tilde{E}_p$. Further we assume that $p$ is prime to $MDN$† as in Section 1, and put $f_p(x) = f(x) \bmod p$. Then we can prove

LEMMA 1. *With the notation as above, we have*

$$(*) \qquad N_p - 1 \equiv \sharp\{\alpha \in \boldsymbol{F}_p \mid f_p(\alpha) = 0\} \pmod 2\,.$$

*Proof.* The proof was given in a special case in [1], but for the completeness of the paper, we give here the proof in detail. It is known that the number of solutions of $y^2 \equiv f(x) \pmod p$ in $\boldsymbol{F}_p^2$ is equal to $N_p - 1$. We notice that the right hand side of $(*)$ is odd if and only if $f_p(x)$ has at least one linear factor over $\boldsymbol{F}_p$. And, it is clear that $f_p(x)$ has a linear factor if and only if the number of solutions of $y^2 \equiv f(x) \pmod p$ is odd.

Q.E.D.

THEOREM 2. *With the notation as above, we have the following equivalences:*

(1) *$f_p(x)$ has exactly one linear factor over $\boldsymbol{F}_p$ if and only if $N_p - 1$ is odd and $(-D/p) = -1$.*

(2) *$f_p(x)$ is irreducible over $\boldsymbol{F}_p$ if and only if $N_p - 1$ is even and $(-D/p) = 1$.*

(3) *$f_p(x)$ has three distinct linear factors over $\boldsymbol{F}_p$ if and only if $N_p - 1$ is odd and $(-D/p) = 1$.*

*Proof.* (2) is obvious from Lemma 1. (1) is already proved in the proof of Theorem 1. Hence (3) is also proved. Q.E.D.

*Remark* 1. The Galois group of $E_2$ over $\boldsymbol{Q}$ is isomorphic to $S_3$ if and only if $E$ has no $\boldsymbol{Q}$-rational points of order 2 and the discriminant of $E$ is not square.

*Remark* 2. We should remark that, in the proofs of Lemma 1 and Theorem 2, we need not use the condition that $K_f(=E_2)$ contains an imaginary quadratic field. This condition is needed only for assuring the existence of cusp forms of weight 1.

*Remark* 3. Let $E, E'$ be in $\varphi_3^{-1}(K)$. Let $N$ and $N'$ denote the conductors of $E$ and $E'$. Let $p$ be any odd prime such that $p \nmid NN'$. Then Lemma 1 shows that, for almost all $p$,

$$N_p(E) \equiv N_p(E') \pmod 2 .$$

## § 3. Proof of (III)

Let $E$ be in $\varphi_3^{-1}(K)$ and $F(\tau) = \sum_{n=1}^{\infty} a(n)e[n\tau]$ in $\varphi_2^{-1}(K)$. We use same notation as in Section 1 and Section 2. Combining Theorem 1 and Theorem 2, we obtain

THEOREM 3. *Let $p$ be any odd prime such that $p \nmid NMDN\mathfrak{f}$. Then we have*

$$N_p(E) \equiv a(p) \pmod 2 .$$

For elliptic curves rational over $\boldsymbol{Q}$, there is a famous Taniyama-Weil conjecture. If we assume this conjecture, for the elliptic curve $E$ in Section 2, there exists the normalized cusp form $G(\tau) = \sum_{n=1}^{\infty} c(n)e[n\tau]$ of weight 2 on $\Gamma_0(N)$ such that

$$N_p(E) = 1 + p - c(p), \qquad \text{for any prime } p, p \nmid N .$$

Hence, we get

COROLLARY. *With the above assumption, we get the congruence* mod 2 *between $F(\tau)$ and $G(\tau)$:*

$$c(p) \equiv a(p) \pmod 2$$

*for any odd prime $p$, such that $p \nmid NMDN\mathfrak{f}$.*

*Remark.* In a special example treated in [1], this type of congruences mod 2 means that

$$\eta(\tau)^2\eta(11\tau)^2 \equiv \eta(2\tau)\eta(22\tau) \pmod 2 ,$$

which follows easily from the fact, $(1 - x)^2 \equiv 1 - x^2 \pmod 2$.

## § 4.

Let $F(\tau) = \sum_{n=1}^{\infty} a(n)e[n\tau]$ be an element in $\mathscr{C}_2$. We assume that there exists a cusp form $H(\tau) = \sum_{n=1}^{\infty} b(n)e[n\tau]$ of weight 2 satisfying

(1) $H(\tau)$ is a normalized primitive cusp form,
(2) $b(n) \in \boldsymbol{Z}$ for all $n \geqq 1$,
(3) For almost all primes $p$, $a(p) \equiv b(p) \pmod 2$.

By the assumptions (1) and (2), there exists an elliptic curve $E$ defined over $\boldsymbol{Q}$ associated with $H(\tau)$ as in Section 3.

https://doi.org/10.1017/S0027763000021401 Published online by Cambridge University Press

THEOREM 4. *Under the above assumption, we have*

$$K_F = E_2 \,.$$

*Namely, $E$ belongs to $\mathscr{C}_3$ and $\varphi_3(E) = \varphi_1(F)$.*

*Proof.* We denote the defining equation of $E$ by $y^2 = g(x)$ where $g(x)$ is a polynomial over $\boldsymbol{Q}$ of degree 3. For any good prime $p$ for $E$, let $N_p$ denote the number of $\boldsymbol{F}_p$-rational points of the reduction mod $p$ of $E$. Then the assumption (3) shows that

$$N_p \equiv a(p) \pmod 2, \qquad \text{for almost all odd, good primes}\,.$$

Put $T_1 = \{p\colon \text{good prime} \mid a(p) = 2\}$, $T_2 = \{p\colon \text{good prime} \mid a(p) = 0\}$, and $T_3 = \{p\colon \text{good prime} \mid a(p) = -1\}$. Applying Tchebotarev density theorem to $K_F$, we know that the densities of $T_1$, $T_2$ and $T_3$ are 1/6, 1/2 and 1/3 respectively. The above congruence shows that $T_3 = \{p\colon \text{prime} \mid N_p \text{ is odd}\}$ up to finite set of primes.

If $g(x)$ is reducible over $\boldsymbol{Q}$, $N_p$ is even for any good prime; this contradicts the above result. Hence $g(x)$ is irreducible over $\boldsymbol{Q}$. We assume that the splitting field $K_g$ of $g(x)$ is abelian over $\boldsymbol{Q}$. Then the densities of sets of primes $U_1 = \{p\colon \text{prime} \mid g_p(x) \text{ is a product of linear factors over } \boldsymbol{F}_p\}$ and $U_2 = \{p\colon \text{prime} \mid g_p(x) \text{ is irreducible over } \boldsymbol{F}_p\}$ are 1/3 and 2/3 respectively; this contradicts the above result. Hence $[K_g\colon \boldsymbol{Q}] = 6$. Let $k'$ denote the quadratic field contained in $K_g$. We assume that $k \neq k'$, Let $(k/p)$ denote the Kronecker symbol. Then $(k/p) = -1$ induces $a(p) = 0$, hence $N_p$ is even. Also $(k'/p) = -1$ induces that $N_p$ is even. Since $k \neq k'$, the density of the set of primes $\{p\colon \text{prime} \mid (k/p) = -1 \text{ or } (k'/p) = -1\}$ is 3/4; this contradicts the above result. Hence $K_g \supset k$. Since $K_f/k$ and $K_g/k$ are abelian extensions and the decomposition rule of primes of $k$ in $K_f$ and $K_g$ coincides to each other, we get $K_f = K_g$. Q.E.D.

## REFERENCES

[1] S. Chowla and M. Cowles, On the coefficients $c_n$ in the expansion $x\prod_{n=1}^{\infty}(1-x^n)^2(1-x^{11n})^2 = \sum_1^{\infty} c_n x^n$, J. reine angew. Math., **292** (1977), 115–116.

[2] T. Hiramatsu, Higher reciprocity law and modular forms of weight one, Comm. Math. Univ. St. Paul, **31** (1982), 75–85.

[3] T. Hiramatsu and Y. Mimura, The modular equation and modular forms of weight one, preprint.

[4] T. Hiramatsu, N. Ishii and Y. Mimura, On indefinite modular forms of weight one, preprint.

[5] C. Moreno, The higher reciprocity law: an example, J. Number Theory, **12** (1980), 57–70.

*Department of Mathematics*
*Nagoya University*
*Chikusa-ku, Nagoya 464*
*Japan*