J. Math. Kyoto Univ. (JMKYAZ)
14-2 (1974) 243-255

On the fields generated by certain points of finite order on Shimura's elliptic curves*

By

Masatoshi YAMAUCHI

(Received, July 12, 1973)

As the title indicates our object of study is an abelian variety B (in the present paper, we are interested only in the one-dimensional case), which was investigated by Shimura [5], [6]. Using such an abelian variety B, he has shown some important relation between the arithemtic of real quadratic fields and the cusp forms of "Neben"-type in Hecke's sense. Here we repeat the result briefly. B is defined over a real quadratic field $k=\boldsymbol{Q}(\sqrt{q})$, whose transform B^{ε} by the non-trivial automorphism ε of k is isogenous to B. Such a B can be obtained from the eigen-function $f(z)=\sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ for all Hecke operators acting on the space $S_2(\Gamma_0(q), \chi)$ of cusp forms of "Neben"-type of weight 2. The eigen-values of Hecke operators for $S_2(\Gamma_0(q), \chi)$ are closely ocnnected with the reciprocity law in certain abelian extenions of k, moreover, such extensions can be generated by the coordinates of some specific section point (c-section point in [6, Th. 2.2. p. 141]) of B. It was observed that two rational integers c and $\mathrm{tr}_{k/\boldsymbol{Q}}(\varepsilon_q)$ have non-trivial common factors where ε_q is the fundamental unit of k [6, § 3] and the Fourier coefficients a_p of $f(z)$ has a certain congruence property with respect to c. As a continuation of this theory, the same investigation was made for the space of cusp forms of "Haupt"-type, by Doi and the present author [2].

* This work was partially supported by the Sakkokai Foundation.

Now Doi [1] has found some arithmetical congruence (with respect to a prime factor l of the numerator of the generalized Bernoulli number $B_{\kappa,\chi}$) for the Fourier coefficients a_p of $f(z)$ of $S_\kappa(\Gamma_0(q), \chi)$ for arbitrary weight $\kappa \geqq 2$ (see text). Thus, as a next task of the investigations which we explained above, we are naturally led to consider the field K_l generated over k by the coordinates of l-section point of B. In fact, in the present note, we shall treat as a typical examples the case where $q=29$, 37 and investigate the field K_l.

Theorem. *The following assertions* (1), (2) *hold* (*at least*) *for* $q=29$, 37, *and* (3) *holds for* $q=29$.

(1) *Let* l *be an odd prime factor of* $B_{2,\chi}$, *and* K_l *be the field generated over* $k=\boldsymbol{Q}(\sqrt{q})$ *by the* l*-section point of the elliptic curve* B. *Then there is an isomorphism* $\sigma \to R_l(\sigma)$ *of the Galois group* $\mathrm{Gal}(K_l/k)$ *onto the group*

$$\left\{\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \in GL_2(\boldsymbol{Z}/l\boldsymbol{Z}) \mid \quad b \in \boldsymbol{Z}/l\boldsymbol{Z},\ d \in (\boldsymbol{Z}/l\boldsymbol{Z})^\times \right\}.$$

(2) *We have* $K_l = k(\zeta, \sqrt[l]{\varepsilon_q})$ *where* ε_q *is the fundamental unit of* k, *and* ζ *is a primitive* l*-th root of unity.*

(3) K_l *is unramified over* $k(\zeta)$.

For the precise definition and notation will be explained in the test.

Finally, we consider this investigation as a suggestive example for the general treatment of such extensions and one can expect similar results for K_l in the higher dimensional case.

1. Shimura's elliptic curves.

We recall here Shimura's theory for the abelian variety associated to cusp forms. For a prime q, let $\Gamma_0(q)$ be a congruence subgroup of $SL_2(\boldsymbol{Z})$,

$$\Gamma_0(q) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\boldsymbol{Z}) \mid \quad c \equiv 0 \pmod{q}\right\},$$

and $S_2(\Gamma_0(q), \chi)$ denote the vector space of holomorphic cusp forms $f(z)$ of weight 2 on the complex upper half plane, which satisfy

$$f\left(\frac{az+b}{cz+d}\right)=\chi(d)(cz+d)^2 f(z)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(q)$. Throughout this paper we assume that $q \equiv 1 \bmod 4$ and the character χ of $(\boldsymbol{Z}/q\boldsymbol{Z})^\times$ is of order 2. We denote by k the real quadratic field corresponding to the kernel of χ, namely $k=\boldsymbol{Q}(\sqrt{q})$. Let $f(z)=\sum_{n=1}^{\infty} a_n e^{2\pi i n z}$, with $a_1=1$, be an element of $S_2(\Gamma_0(q), \chi)$, that is a common eigen-function of Hecke operator T_m for all m. Let K be the field generated by the numbers a_n over $\boldsymbol{Q}$ for all n. Then we know K is totally imaginary, and the eigen-value of T_n satisfies

$$a_n^\rho=\chi(n)a_n,$$

if n is prime to q, where ρ denotes the complex conjugation.

By virtue of [5, Th. 7.14] we obtain an abelian variety A and an isomorphism θ of K into $\mathrm{End}_{\boldsymbol{Q}}(A)$. A and $\theta(a)$ for all $a \in K$ are rational over $\boldsymbol{Q}$. Further A has an automorphism μ rational over k, such that

$$\mu^2=1, \qquad \mu\theta(a)=\theta(a^\rho)\mu \qquad (a \in K),$$

$$\mu^\varepsilon=-\mu,$$

where ε denotes the generator of $\mathrm{Gal}(k/\boldsymbol{Q})$. We put

$$B=(1+\mu)A\,.$$

Then B is an abelian subvariety of A rational over k, and

$$A=B+B^\varepsilon, \qquad B^\varepsilon=(1-\mu)A.$$

Hereafter we restrict ourselves to the case $\dim B=1$.

For a prime number l and a natural number n, put

$$B[l^n]=\{t \in B \mid l^n t=0\},$$

$$B[l^{\infty}]=\bigcup_{n=1}^{\infty} B[l^n].$$

It is well known that $B[l^n]$ (resp. $B[l^{\infty}]$) is isomorphic to $\boldsymbol{Z}/l^n\boldsymbol{Z}\oplus\boldsymbol{Z}/l^n\boldsymbol{Z}$ (resp. $\boldsymbol{Q}_l/\boldsymbol{Z}_l\oplus\boldsymbol{Q}_l/\boldsymbol{Z}_l$) where $\boldsymbol{Q}_l$ denotes the l-adic number field and $\boldsymbol{Z}_l$ the ring of l-adic integers. Let K_{l^n} (resp. $K_{l\infty}$) be the field generated over k by the coordinates of the points in $B[l^n]$ (resp. $B[l^{\infty}]$). It can be easily seen that K_{l^n} (resp. $K_{l\infty}$) is a finite (resp. an infinite) Galois extension of k. Taking a basis of $B[l^n]$ (resp. $B[l^{\infty}]$) we obtain a representation R_n (resp. R_{∞})

$$R_n\colon \mathrm{Gal}(K_{l^n}/k) \longrightarrow GL_2\ (\boldsymbol{Z}/l^n\boldsymbol{Z})$$

$$R_{\infty}\colon \mathrm{Gal}(K_{l\infty}/k) \longrightarrow GL_2(\boldsymbol{Z}_l)\,.$$

We may assume that

$$R_n(\sigma')\equiv R_{\infty}(\sigma) \qquad (\mathrm{mod}\ l^n), \tag{1.1}$$

if σ' is the restriction of an element σ of $\mathrm{Gal}(K_{l\infty}/k)$ to K_l.

Let $\mathfrak{p}$ be a prime ideal not dividing q, then B has good reduction modulo $\mathfrak{p}$. We denote by $\tilde{B}$ the elliptic curve obtained from B by reduction modulo $\mathfrak{p}$. Let $\varphi_{\mathfrak{p}}$ denote the Frobenius endomorphism of $\tilde{B}$ of degree $N\mathfrak{p}$, and $\mathfrak{R}_l$ the l-adic representation of $\mathrm{End}(\tilde{B})$. Then we have (see [5, (7. 6. 15)])

$$\det(1_2-u\mathfrak{R}_l(\varphi_{\mathfrak{p}}))=1-a_pu+pu^2 \qquad \text{if} \quad (p)=\mathfrak{p}\cdot\mathfrak{p}', \tag{1.2}$$

$$\det(1_2-u^2\mathfrak{R}_l(\varphi_{\mathfrak{p}}))=(1-a_pu-pu^2)$$

$$\times(1-a_p^{\rho}u-pu^2) \qquad \text{if} \quad N\mathfrak{p}=p^2,$$

provided that l is prime to $N\mathfrak{p}$. Let $\mathfrak{P}$ be a prime divisor of K_l which divides $\mathfrak{p}$ and σ a Forbenius element of $\mathrm{Gal}(K_{l\infty}/k)$ for $\mathfrak{P}$. Then we obtain

$$R_{\infty}(\sigma)=\mathfrak{R}_l(\varphi_{\mathfrak{p}}) \tag{1.3}$$

by choosing suitable basis of $B[l^{\infty}]$ and $\tilde{B}[l^{\infty}]$, since we see easily $t^{\sigma}\mathrm{mod}\,\mathfrak{P}=\varphi_{\mathfrak{p}}(t\ \mathrm{mod}\,\mathfrak{P})$. Hence comparing (1.3) with (1.2), we know the characteristic polynomial of $R_n(\sigma')$ coincides with that of $\mathfrak{R}_l(\varphi_\mathfrak{p})$ modulo l^n. Further we can prove that K_l contains a primitive l^n-th root of unity ζ_n, and

$$\zeta_n^\tau = \zeta_n^{\det R_n(\tau)} \tag{1.4}$$

for every $\tau \in \mathrm{Gal}(K_{l^n}/k)$.

2. A congruence for a_p (due to Doi).

We now define the generalized Bernoulli number $B_{\kappa,\chi}$. Let χ be the character of order 2 with a prime conductor q and let

$$F_\chi(t) = \sum_{a=1}^{q} \frac{\chi(a)t \cdot e^{at}}{e^{qt}-1} .$$

Expanding this into power series we have

$$F_\chi(t) = \sum_{\kappa=1}^{\infty} B_{\kappa,\chi} \cdot \frac{t^\kappa}{\kappa!} .$$

The number $B_{\kappa,\chi}$ defined as above is called the generalized Bernoulli number. It has been proved in [1],

$$\det(1+\chi(p)p^{k-1} - T_{p,\kappa}) \equiv 0 \qquad (\mathrm{mod}\, l) \tag{2.1}$$

where l is an odd prime factor of the numerator of $(2\kappa)^{-1} \cdot B_{\kappa,\chi}$, and $T_{p,\kappa}$ is the Hecke operator acting on the space $S_\kappa(\Gamma_0(q), \chi)$ of weight κ. Since we have assumed that the abelian variety B over k is of one-dimensional, the Fourier coefficient a_p of the corresponding cusp form $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ is contained in $\boldsymbol{Q}$ or an imaginary quadratic field according as $\chi(p)=1$ or -1. Hence, in our case, the congruence (2.1) becomes (setting $k=2$)

$$\begin{aligned} &1+p-a_p \equiv 0\ (l) && \text{if } \chi(p)=1 \\ &(1-p)^2 - a_p^2 \equiv 0\ (l) && \text{if } \chi(p)=-1 , \end{aligned} \tag{2.2}$$

where l is an odd prime factor of the numerator of $4^{-1} \cdot B_{2,\kappa}$.

3. Some Lemmas.

We give here some lemmas which is necessary to prove our Theorem.

Lemma 1. *For an odd prime l, let G be a subgroup of $GL_2(Z/lZ)$ satisfying the following conditions*: (1) *G has elements of order l and $l-1$.* (2) *Any element of G has an eigen-value* 1. *Then G is isomorphic to the group* $\left\{\begin{pmatrix}1 & b\\ 0 & d\end{pmatrix}\in GL_2(\boldsymbol{Z}/l\boldsymbol{Z})\,|\,b\in\boldsymbol{Z}/l\boldsymbol{Z},\ d\in(\boldsymbol{Z}/l\boldsymbol{Z})^\times\right\}$ *of order $l(l-1)$.*

Proof. Put $G'=G\cap PSL_2(\boldsymbol{Z}/l\boldsymbol{Z})$, then G/G' is a subgroup of $GL_2(\boldsymbol{Z}/l\boldsymbol{Z})/PSL_2(\boldsymbol{Z}/l\boldsymbol{Z})$, hence $[G:G']$ is prime to l. Therefore G contains an element of order l by the assumption (1). By virtue of the assumption (2), any element g' of G' is conjugate to $\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}$, hence $g'^l=1$. Therefore G' is an l-group and is also an l-Sylow subgroup of $PSL_2(\boldsymbol{Z}/l\boldsymbol{Z})$ by considering the order of $PSL_2(\boldsymbol{Z}/l\boldsymbol{Z})$. Hence G' is conjugate to the group $\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}\middle|\, b\in\boldsymbol{Z}/l\boldsymbol{Z}\right\}$. Since G normalizes the group G', G is isomorphic to the group $\left\{\begin{pmatrix}1 & b\\ 0 & d\end{pmatrix}\middle|\, b\in\boldsymbol{Z}/l\boldsymbol{Z},\ d\in\mathfrak{h}\right\}$ where $\mathfrak{h}$ is a subgroup of $(\boldsymbol{Z}/l\boldsymbol{Z})^\times$. Now G contains an element of order $l-1$, therefore $\mathfrak{h}=(\boldsymbol{Z}/l\boldsymbol{Z})^\times$. This completes the proof of our lemma 1.

We quote here a lemma given in ([4, p. 213]).

Lemma 2. (*Shimura*). *Let g be an element of $GL_2(\boldsymbol{Z}/l\boldsymbol{Z})$, whose characteristic polynomial is congruent to X^2-a_pX+p modulo l, where p is a prime and a_p is an integer. If $a_p^2-4p=ld$ with an integer d which is not divisible by d, then g is conjugate to a matrix of the form* $\begin{pmatrix}b & 1\\ 0 & b\end{pmatrix}$.

Let K be a finite Galois extension over an algebraic number field k, whose Galois group $\mathrm{Gal}(K/k)$ is isomorphic to the group $\left\{\begin{pmatrix}1 & b\\ 0 & d\end{pmatrix}\middle|\, b\in\boldsymbol{Z}/l\boldsymbol{Z}, d\in(\boldsymbol{Z}/l\boldsymbol{Z})^\times\right\}$, where l is an odd prime. Further assume that K contains a primitive l-th root of unity $\zeta=e^{\frac{2\pi i}{l}}$. Under these situations we obtain the following assertion.

Lemma 3. *If* $\zeta^{\eta}=\zeta^{\det\eta}=\zeta^{d}$ *for* $\eta=\begin{pmatrix}1 & b\\ 0 & d\end{pmatrix}\in \mathrm{Gal}(K/k)$, *Then there exists an element* α *of* $K^{\times}$ *such that* $K=k(\zeta,\alpha)$ *with* $\alpha^{l}\in k^{\times}$.

Proof. It is easy to see that the Galois group $\mathrm{Gal}(K/k)$ is generated by $\sigma=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, and $\tau=\begin{pmatrix}1 & 0\\ 0 & d\end{pmatrix}$ where d is a primitive root modulo l. Since $\zeta^{\sigma}=\zeta$ and $\zeta^{\tau}=\zeta^{d}$, K is a Kummer extension over $k(\zeta)$ of degree l. Hence there exists an element β of $K^{\times}$ such that $K=k(\zeta,\beta)$ with $\beta^{l}\in k(\zeta)$. Now $(\beta^{\sigma})^{l}=(\beta^{l})^{\sigma}=\beta^{l}$, therefore we may assume β satisfies $\beta^{\sigma}=\zeta\beta$ (Consider a suitable power of β instead of β, if necessary). We see

$$\{x\in K^{\times}\mid x^{l}\in k(\zeta)\}=\bigcup_{\nu=0}^{l-1}k(\zeta)^{\times}\beta^{\nu},$$

so there exists an element γ of $k(\zeta)^{\times}$ and an integer ν $(0\leqq\nu\leqq l-1)$ such that $\beta^{\tau}=\gamma\beta^{\nu}$. Since $\tau\sigma^{d}=\sigma\tau$, we obtain $\gamma\zeta^{d\nu}\beta^{\nu}=\beta^{\tau\sigma^{d}}=\beta^{\sigma\tau}=(\zeta\beta)^{\tau}=\zeta^{d}\gamma\beta^{\nu}$, hence $\zeta^{d\nu}=\zeta^{d}$, thus $\nu=1$. Namely, we obtain $\beta^{\tau}=\gamma\beta$ therefore we have $N_{k(\zeta)/k}(\gamma)=1$. Thus there exists an element δ of $k(\zeta)$ such that $\gamma=\delta/\delta^{\tau}$. Define $\alpha=\beta\delta$ then we see $\alpha^{\tau}=\alpha$ and $\alpha^{l}\in k(\zeta)^{\times}$ therefore $\alpha^{l}\in k$. Hence we have $K=k(\zeta,\alpha)$ with $\alpha^{l}\in k$. This completes our proof of lemma 2.

4. A Proof of the Theorem.

For primes $q=29, 37$, we have $\dim S_2(\Gamma_0(q),\chi)=2$, namely the abelian variety B over $k=\boldsymbol{Q}(\sqrt{q})$ is of one dimensional.
Further we observe that $B_{2,\chi}=12, 20$ for $q=29$ and 37, respectively.

First we shall discuss the case $q=29$. We consider the field K_3 generated over $k=\boldsymbol{Q}(\sqrt{29})$ by the coordinates of points on B of order $l=3$. There is an isomorphism $\sigma\to R_l(\sigma)$ of the Galois group $\mathrm{Gal}(K_3/k)$ onto a subgroup of $GL_2(\boldsymbol{Z}/3\boldsymbol{Z})$. Let p be a prime different from 3, 29 and $\mathfrak{p}$ be a prime divisor of p in K_3. Let $\sigma_{\mathfrak{p}}$ be a Frobenius automorphism for $\mathfrak{p}$, then by (1.2) and (1.3) we have

$$\det(x\cdot 1_2 - R_l(\sigma_{\mathfrak{p}})) \equiv \begin{cases} x^2 - a_p x + p & (\bmod 3) \quad \text{if } \chi(p)=1 \\ x^2 - (a_p^2 + 2p)x + p^2 & (\bmod 3) \quad \text{if } \chi(p)=-1 . \end{cases}$$

By Virtue of (2.2), $R_l(\sigma_{\mathfrak{p}})$ has an eigen value 1 for any p. We assert that $R_l(\mathrm{Gal}(K_3/k))$ contains elements of order 3 and 2. Take $p=7$, from the table (I) we get $a_7=2$. Hence $R_l(\mathrm{Gal}(K_3/k))$ contains an element g whose characteristic polynomial is

$$X^2-2X+7\equiv(X-1)^2 \qquad (\bmod 3),$$

and since $a_7^2-4\cdot 7=-24$, we can verify by lemma 2 that g is conjugate to a matrix of the form $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Hence $R_l(\mathrm{Gal}(K_3/k))$ contains an element of order 3. Applying the same to $p=5$ we find an element of order 2 in $R_l(\mathrm{Gal}(K_3/k)$.

Hence $\mathrm{Gal}(K_3/k)$ satisfies the assumptions in lemma 1. Thus wez have

$$\mathrm{Gal}(K_3/k)\simeq\left\{\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}\in Gl_2(\boldsymbol{Z}/3\boldsymbol{Z})\,|\,b\in\boldsymbol{Z}/3\boldsymbol{Z},\ d\in(\boldsymbol{Z}/3\boldsymbol{Z})^\times\right\}$$

Next we shall determine the field K_3 explicitly.

As we know K_3 contains a primitive third root of unity $\zeta=e^{\frac{2\pi i}{3}}$ and $\zeta^\sigma=\zeta^{\det\sigma}$ (see (1.4)), the extension K_3 over k satisfies the assumptions in lemma 3. Hence there exists an element α of K_3 such that $K_3=k(\zeta,\alpha)$ with $\alpha^3\in k$. Now we must prove that α^3 can be taken as the fundamental unit $\varepsilon=\dfrac{5+\sqrt{29}}{2}$ of k. By the property of the field generated by l-section point, we know that any prime divisor $\mathfrak{p}$ of $k(\zeta)$ is unramified in K_3, if $\mathfrak{p}$ does not divide $3\cdot\sqrt{29}$. So we can put α^3 of k so as $\alpha^3=3^a\cdot\sqrt{29}^b\cdot\varepsilon^c$ where $0\leqq a, b, c\leqq 2$ (Note that $\chi(3)=-1$). More precisely, we may put $\alpha^3=3$, $3^a\cdot\sqrt{29}$ or $3^a\cdot\sqrt{29}^b\cdot\varepsilon$ with $0\leqq a, b\leqq 2$. Hence there are 13 possibilities of the choice of α^3. We shall show that $\alpha^3=\varepsilon$ by examining the decompotion law of several prime divisors of $k(\zeta)$ in K_3.

(I) *the case* $q=29$*

p	a_p	a_p^2-4p	r	$\mathrm{Ind}_r 3$	$\mathrm{Ind}_r 29$	$\mathrm{Ind}_r \varepsilon$
5	-3					
7	2	-24	3	1	6	1, 2
13	-1	-51	6	8	8	7, 11
67	8	-204	2	39		
547	38	-744	17	39	342	

Let $\sigma_{\mathfrak{p}}$ be the Frobenius automorphism for $\mathfrak{p}$ of K_3 where $\mathfrak{p}$ is dividing one of 7, 13 and 547. Then by lemma 2, we verify $R_l(\sigma_{\mathfrak{p}})$ is of order 3, hence any prime divisor of $k(\zeta)$ which divides one of 7, 13 and 547 does not decompose in K_3. On the other hand, as the table shows, we have for $p=547$

$$(3^a\cdot\sqrt{29^b})^{\frac{p-1}{3}}\equiv 1 \qquad (\mathrm{mod}\ \mathfrak{p})$$

where $\mathfrak{p}$ is any prime factor of 547 in $k(\zeta)$. This shows that the Frobenius automorphism $\sigma_{\mathfrak{p}}$ for $\mathfrak{p}$ of the extension $k\left(\zeta, \sqrt[3]{3^a\cdot\sqrt{29^b}}\right)$ over $k(\zeta)$ is trivial since

$$\sqrt[3]{3^a\cdot\sqrt{29^b}}\,\sigma_{\mathfrak{p}}\equiv\sqrt[3]{3^a\sqrt{29^b}}^{\,p} \qquad (\mathrm{mod}\ \mathfrak{p})$$

$$\equiv\sqrt[3]{3^a\sqrt{29^b}} \qquad (\mathrm{mod}\ \mathfrak{p}).$$

Hence a prime factor $\mathfrak{p}$ of 547 in $k(\zeta)$ decomposes completely in $k\left(\zeta, \sqrt[3]{3^a\sqrt{29^b}}\right)$. Thus we can not have $\alpha^3=3\ 3^a\cdot\sqrt{29}$. Next we take $p=7$ then

$$(3^2\sqrt{29^b}\cdot\varepsilon)^{\frac{p-1}{3}}\equiv 1\ (\mathfrak{p}) \qquad \text{if } \mathfrak{p} \text{ divides } 6+\sqrt{29},$$

$$(3\cdot\sqrt{29^b}\cdot\varepsilon)^{\frac{p-1}{3}}\equiv 1\ (\mathfrak{p}) \qquad \text{if } \mathfrak{p} \text{ divides } 6-\sqrt{29},$$

* The meaning of this table is as follows: r denotes a primitive root modulo p, $\mathrm{Ind}_r\, n$ the index of n with respect to r. $\varepsilon=\frac{5+\sqrt{b}}{2}$, where $b^2\equiv 29 \bmod p$.

for any b. Thus by the same reasoning as for $p=547$, we can not have $\alpha^3=3\cdot\sqrt{29}^b\varepsilon$, $3^2\cdot\sqrt{29}^b\varepsilon$ for any b $(0\leqq b\leqq 2)$. Further, take $p=13$ we see

$$(\sqrt{29}^2\cdot\varepsilon)^{\frac{p-1}{3}}\equiv 1 \ (\mathfrak{p}) \qquad \text{if } \mathfrak{p} \text{ divides } \frac{9-\sqrt{29}}{2},$$

$$(\sqrt{29}\cdot\varepsilon)^{\frac{p-1}{3}}\equiv 1 \ (\mathfrak{p}) \qquad \text{if } \mathfrak{p} \text{ divides } \frac{9+\sqrt{29}}{2},$$

thus we can not have $\alpha^3=\sqrt{29}\varepsilon$, $\sqrt{29}^2\varepsilon$. Summing up above facts we must have $\alpha^3=\varepsilon$. This completes the proof of (2) for the case $q=29$. Lastly, we must show that K_3 is unramified over $k(\zeta)$. Since we proved $K_3=k(\zeta, \sqrt[3]{\varepsilon})$, a prime divisor $\mathfrak{p}$ of $k(\zeta)$ is unramified in K_3 unless $\mathfrak{p}$ divides 3. Now assume $\mathfrak{p}=(1-\zeta)$, which divides 3, is ramified in K_3, then the prime ideal (3) of k is also totally ramified in $k(\sqrt[3]{\varepsilon})$. Let w be the additive (3)-adic valuation of the (3)-adic field of $k(\sqrt[3]{\varepsilon})$. normalized as $w(3)=1$. Define the element x of $k(\sqrt[3]{\varepsilon})$ as $\sqrt[3]{\varepsilon}=x+\varepsilon^3$, then x satisfies

$$x^3+3\varepsilon^3x^2+\varepsilon^9-\varepsilon=-3\varepsilon^6x.$$

Because $\mathfrak{p}=(3)$ is totally ramified in $k(\sqrt[3]{\varepsilon})$,

$$\begin{aligned} w(x) &= \frac{1}{3}w(N_{k(\sqrt[3]{\varepsilon})/k}(x)) \\ &= \frac{1}{3}w(\varepsilon^9-\varepsilon). \end{aligned}$$

Now since $\varepsilon^4+1=\varepsilon^2\cdot\mathrm{tr}(\varepsilon^2)=\varepsilon^2\cdot\mathrm{tr}\left(\frac{27+5\sqrt{29}}{2}\right)=27\varepsilon^2$, $\varepsilon^4-1=\varepsilon^4+1-2\not\equiv 0$ (mod 3), we have $w(\varepsilon^9-\varepsilon)=3$. Thus $w(x)=1$. Hence $w(x^3+3\varepsilon^3x^2+\varepsilon^9-\varepsilon)\geqq 3$, while $w(-3\varepsilon^6x)=2$. This is a contradiction. Thus the prime divisor $\mathfrak{p}=(1-\zeta)$ of $k(\zeta)$ is unramified in $K_3=k(\zeta, \sqrt[3]{\varepsilon})$. This completes the proof of our Theorem for the case $q=29$.

[Remark] It was proved by Casselman (On abelian varieties with many endomorphisms and a conjecture of Shimura's, Inventiones math. 12 (1971), 225–236) that Shimura's elliptic curve for the case $q=29$ has good reduction at every primes of $k=\boldsymbol{Q}(\sqrt{29})$. So the prime $(\sqrt{29})$ is unramified in K_3. If we use this facts, there are only 4 possiblitities of α^3, namely $\alpha^3=3, 3\varepsilon$ $3^2\varepsilon$ and ε, which makes the proof of our Theorem a little simpler.

In [3, § 3.10] Serre has given an elliptic curve B' over $k=\boldsymbol{Q}(\sqrt{29})$ defined by the equation

$$B'\colon y^2+xy+\varepsilon^2 y=x^3$$

where $\varepsilon=\dfrac{5+\sqrt{29}}{2}$. B' has also good reduction at every primes of k. It is conjectured that B' is isomorphic to the Shimura's elliptic curve B for the case $q=29$ (see [6, § 10]). It was also remarked that the Galois group of the field K'_3 generated by the 3-section points of B' over k is isomorphic to the group

$$\left\{\begin{pmatrix}1 & b\\ 0 & d\end{pmatrix}\middle|\, b\in\boldsymbol{Z}/3\boldsymbol{Z},\ d\in(\boldsymbol{Z}/3\boldsymbol{Z})^\times\right\},$$

verifying the rational point (0, 0) on B' is of order 3. We note here that the field K'_3 coincides with K_3, which can be verified by examining the trace $\mathrm{tr}(\varphi'_{\mathfrak{p}})$ of the Frobenius automorphism of the elliptic curve $\tilde{B}$ obtained by the rdeuction modulo $\mathfrak{p}$, putting $N\mathfrak{p}=7, 13, 67$, (For these primes we have $\mathrm{tr}(\varphi'_{\mathfrak{p}})=a_p$).

Secondly, we treat the case $q=37$. In this case we have $B_{2,\chi}=20$. So we consider the field K generated over $k=\boldsymbol{Q}(\sqrt{37})$ by 5-section point of the elliptic curve B associated to the space $S_2(\Gamma_0(37), \chi)$. There is an isomorphism $\sigma\to R_l(\sigma)$ of the Galois group $\mathrm{Gal}(K_5/k)$ onto a subgroup of $GL_2(\boldsymbol{Z}/5\boldsymbol{Z})$. Let $\mathfrak{p}$ be a prime divisor of 11 in K_5. Then by the same reasoning as the case $q=29$, the characteristic polynomial of the image $R_l(\sigma_{\mathfrak{p}})$ of the Frobenius automorphism for $\mathfrak{p}$ is

$$X^2-a_{11}X+11=X^2+3X+11\equiv(X-1)^2 \pmod 5,$$

and since $a_{11}^2-4\cdot 11=-35$, we see that the order $R_l(\sigma_{\mathfrak{p}})$ is of order

5. Applying the same to $p=3$ we find an element of order 4 in $R_l(\mathrm{Gal}(K_5/k))$. Thus we have

$$\mathrm{Gal}(K_5/k) \cong \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \in GL_2(\boldsymbol{Z}/5\boldsymbol{Z}) \mid b \in \boldsymbol{Z}/5\boldsymbol{Z},\ d \in (\boldsymbol{Z}/5\boldsymbol{Z})^{\times} \right\},$$

by virtue of lemma 1. Thus there exists an element α of K_5 such that $K_5 = k(\zeta, \alpha)$ with $\alpha^5 \in k = \boldsymbol{Q}(\sqrt{37})$ and $\zeta = e^{\frac{2\pi i}{5}}$. By the same argument as the case $q=29$, α^5 of k can be taken as $\alpha^5 = 5^a \sqrt{37}^b \varepsilon^c$ where $0 \leqq a, b, c \leqq 4$ (Note that $\chi(5) = -1$). More precisely we can put $\alpha^5 = 5$, $5^a\sqrt{37}$, $5^a\sqrt{37}^b\varepsilon$ with $0 \leqq a, b \leqq 4$, where $\varepsilon = 6 + \sqrt{37}$ is the fundamental unit of k. Hence there are 31 possibilities of the choice of α^5. We shall show $\alpha^5 = \varepsilon$.

(II) *the case* $q=37$

p	a_p	a_p^2-4p	r	$\mathrm{Ind}_r 5$	$\mathrm{Ind}_r 37$	$\mathrm{Ind}_r \varepsilon$
3	-1					
11	-3	-35	2	4	2	3, 2
41	-3	-155	6	22	32	13, 7
181	-3	-715	10	48	38	149, 21
491	12	-1820	10	478	340	131, 114
601	-18	-2080	506	50	580	

Let $\sigma_{\mathfrak{p}}$ be the Frobenius automorphism for $\mathfrak{p}$ of K_5 where $\mathfrak{p}$ is dividing one of 11, 41, 181, 491 and 601, then as the table (II) shows the order of $R_l(\sigma_{\mathfrak{p}})$ is of order 5. Hence any prime divisor of $k(\zeta)$ which divides one of 11, 41, 181, 491, and 601 does not decompose in K_5. On the other hand, we have for $p=601$

$$(5^a\sqrt{37}^b)^{\frac{p-1}{5}} \equiv 1 \quad \mathrm{mod}\ \mathfrak{p},$$

where $\mathfrak{p}$ is any prime of $k(\zeta)$ dividing $p=601$. This shows we can not have $\alpha^5 = 5$, $5^a \cdot \sqrt{37}$ $(0 \leqq a \leqq 4)$. Next $p=491$, then

$$(5^2\sqrt{37}^b\varepsilon)^{\frac{p-1}{5}} \equiv 1 \ (\mathfrak{p}) \qquad \text{if } \mathfrak{p} \text{ divides } 48 - 7\sqrt{37},$$

$$(5^3\sqrt{37}^b\varepsilon)^{\frac{p-1}{5}}\equiv 1 \ (\mathfrak{p}) \qquad \text{if } \mathfrak{p} \text{ divides } 48+7\sqrt{37},$$

for any b. Thus we can not have $\alpha^5=5^2\sqrt{37}^b$, $5^3\sqrt{37}^b$ $(0\leqq b\leqq 4)$. Further applying the same to $p=11, 41$ and 181, it turns out that we can not have $\alpha^5=5^a\sqrt{37}^b\varepsilon$ for any a, b except $a=b=0$. Summing up all these facts we obtain $\alpha^5=\varepsilon$. Thus we have $K_5=k(\zeta, \sqrt[5]{\varepsilon})$. This completes the proof for the case $q=37$.

[Remark] We add a remark for the case $q=37$. Consider the extension $k(\sqrt[5]{\varepsilon})$ over $k=\boldsymbol{Q}(\sqrt{37})$. Then $k(\sqrt[5]{\varepsilon})$ is generated by $x=\sqrt[5]{\varepsilon}-\varepsilon^5$, which satisfies

$$x^5+5\varepsilon^5\cdot x^4+10\varepsilon^{10}\cdot x^3+10\varepsilon^{15}x^2+5\varepsilon^{20}x+\varepsilon^{25}-\varepsilon=0.$$

We can verify that $\varepsilon^{25}-\varepsilon$ is divisible by the prime ideal (5) of k but not divisible by $(5)^2$. Hence the above equation is the so-called Eisenstein equation. Thus the prime ideal (5) of k is totally ramified in $k(\sqrt[5]{\varepsilon})$. This means that the field K_5 is ramified over $k(\zeta)$.

KYOTO UNIVERSITY

References

[1] K. Doi, On a decompotion theorem for Dirichlet series associated with automorphic forms, to appear.

[2] K. Doi and M. Yamauchi, On th Hecke operators for $\Gamma_0(N)$ and class fields over quadratic number fields, to appear in J. Math. Soc. Japan.

[3] J. P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inventiones Math., 15 (1972), 259–331.

[4] G. Shimura, A reciprocity law in non-solvable extensions, J. Reine Angew. Math., 221 (1966), 209–220.

[5] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan, No. 11 Iwanami Shoten and Princetion University Press, 1971.

[6] G. Shimura, Class fields over real quadratic fields and Hecke operators, Ann of Math., 95 (1972), 130–190.