COMPOSITIO MATHEMATICA

S. KAMIENNY

Modular curves and unramified extensions of number fields

Compositio Mathematica, tome 47, n° 2 (1982), p. 223-235

<http://www.numdam.org/item?id=CM_1982__47_2_223_0>

COMPOSITIO MATHEMATICA, Vol. 47, Fasc. 2, 1982, pag. 223–235

MODULAR CURVES AND UNRAMIFIED EXTENSIONS OF NUMBER FIELDS

S. Kamienny

1. Introduction

In recent years a great deal of attention has been focussed on two basic problems of number theory. The first of these problems is to explicitly construct the subfields of the Hilbert class field of a number field K. The second problem is to understand the relationship between various Bernoulli numbers and the ideal class groups of number fields.

We recall that the Bernoulli numbers B_k are defined by

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \cdot \frac{t^k}{k!}.$$

Thus, $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}, \ldots$ A prime p is called irregular if p divides the class number of the field $\mathbb{Q}(\zeta_p)$ of p^{th} roots of unity. Kummer was able to show that an odd prime p is irregular if and only if there is an even integer k with $2 \leq k \leq p-3$ such that p divides the numerator of B_k. Herbrand was able to strengthen Kummer's criterion as follows: Let C be the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$. The group $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts on C and we have a canonical decomposition $C = \bigoplus_{i \bmod (p-1)} C(\chi^i)$, where χ is the standard cyclotomic character $G \to \mathbb{F}_p^*$ defined by $\sigma(\zeta_p) = \zeta_p^{\chi(\sigma)}$, and $C(\chi^i) = \{a \in C : \sigma(a) = \chi^i(\sigma) \cdot a$ for all $\sigma \in G\}$. Herbrand proved that $C(\chi^{(1-k)}) \neq 0$ implies that $p | B_k$.

In 1976 Ribet [13] proved the converse, that $p | B_k$ implies $C(\chi^{(1-k)}) \neq 0$. His proof used two important ideas of Serre. The first is that there should be a two-dimensional $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ representation ρ giving the action of Galois on a certain subspace of the space of p-

0010-437X/82080223-13$00.20/0

division points of some simple quotient A of $J_1(p)$, and that ρ should cut out an unramified extension of $\mathbb{Q}(\zeta_p)$. The second idea is that the divisibility of a Bernoulli number by p should imply a congruence between an Eisenstein series and a cusp form f attached to A. These ideas have recently been exploited by Barry Mazur and Andrew Wiles [11] in their proof of the main conjecture for powers of the Teichmüller character.

In this paper we modify these ideas and, for certain $q \neq p$, study the $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ – representation R on the kernel of the q-Eisenstein prime (see §3). In §7 we show that R cuts out an everywhere unramified extension of a particular subfield of $\mathbb{Q}(\zeta_p, \zeta_q)$.

The contents of this paper were taken from the author's Harvard thesis [4]. The author would again like to thank his advisors, Barry Mazur and Andrew Wiles, for their constant help and encouragement, and David Kazhdan for reading the original version and offering valuable suggestions. Finally, thanks are due to Karl Rubin for many helpful and enjoyable conversations.

§2. Modular curves, Jacobians, and Hecke operators

Let $p \geq 13$ be a rational prime number, and let $\Gamma_1(p)$ be the group of matrices

$$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : a \equiv d \equiv 1, c \equiv 0 \pmod{p}\right\}.$$

If $\mathscr{H}$ is the upper half-plane we let $Y_1(p)_{\mathbb{C}}$ be the open Riemann surface $\Gamma_1(p)/\mathscr{H}$, and we let $X_1(p)_{\mathbb{C}}$ be the complete curve obtained by adjoining the $(p-1)$ cusps. Both of these curves have models over $\mathbb{Q}$ (Shimura [16]) which we denote by $Y_1(p)_{/\mathbb{Q}}$ and $X_1(p)_{/\mathbb{Q}}$.

Similarly, one defines the curves $Y_0(p)_{\mathbb{C}}$ and $X_0(p)_{\mathbb{C}}$ by replacing $\Gamma_1(p)$ by $\Gamma_0(p)$ in the above construction. See Mazur [8] for details. Both of these curves also have models over $\mathbb{Q}$ which we denote by $Y_0(p)_{/\mathbb{Q}}$ and $X_0(p)_{/\mathbb{Q}}$.

The $\left(\frac{p-1}{2}\right)$ cusps of $X_1(p)_{/\mathbb{Q}}$ which lie above the cusp 0 of $X_0(p)_{/\mathbb{Q}}$ are called 0-cusps. The remaining cusps of $X_1(p)_{/\mathbb{Q}}$ (i.e., those that lie above the cusp $\infty \in X_0(p)_{/\mathbb{Q}}$) are called ∞-cusps. Shimura has provided a convenient description of the cusps of $X_1(p)_{/\mathbb{Q}}$. Let $\Gamma_1(p)/\mathbb{P}^1(\mathbb{Q}) = X_1(p)_{\mathbb{C}} - Y_1(p)_{\mathbb{C}}$ be the cusps on the Riemann surface. Then if $\frac{a}{b} \in \Gamma_1(p)/\mathbb{P}^1(\mathbb{Q})$

with a, b relatively prime integers, we let $\begin{bmatrix} a \\ b \end{bmatrix}$ be the associated point on $X_1(p)_{/\mathbb{Q}}$. The cusps of $X_1(p)_{/\mathbb{Q}}$ are represented by equivalence classes

$$\left\{\begin{bmatrix} a \\ b \end{bmatrix} : a, b \in \mathbb{Z}/p\mathbb{Z};\ a, b \text{ not both zero}\right\}$$

under the relation "$\begin{bmatrix} a \\ b \end{bmatrix}$ is equivalent to $\pm\begin{bmatrix} a + rb \\ b \end{bmatrix}$ for all $r \in \mathbb{Z}$". We may take as a set of representatives of the O-cusps $\left\{\begin{bmatrix} 0 \\ x \end{bmatrix} : 1 \le x \le \frac{p-1}{2}\right\}$. Similarly, the representatives of the ∞-cusps may be taken to be $\left\{\begin{bmatrix} y \\ 0 \end{bmatrix} : 1 \le y \le \frac{p-1}{2}\right\}$. In our model of $X_1(p)_{/\mathbb{Q}}$ the 0-cusps are rational over $\mathbb{Q}$, and the ∞-cusps are rational over $\mathbb{Q}(\zeta_p)^+$, the maximum totally real subfield of the field of p^{th} roots of unity.

We let $J_1(p)_{/\mathbb{Q}}$ (respectively, $J_0(p)_{/\mathbb{Q}}$) be the jacobian of $X_1(p)_{/\mathbb{Q}}$ (respectively, $X_0(p)_{/\mathbb{Q}}$). Igusa has shown that $J_1(p)_{/\mathbb{Q}}$ has good reduction at every prime l of residue characteristic different from p, and Deligne and Rapoport have shown that $J_1(p)/J_0(p)$ attains everywhere good reduction over $\mathbb{Q}(\zeta_p)^+$.

If we embed $X_1(p)_{/\mathbb{Q}}$ into its jacobian, sending a 0-cusp to zero, then the classes of the 0-cusps generate a rational subgroup of $J_1(p)_{/\mathbb{Q}}$. Manin and Drinfeld have shown that this is a finite group, and Kubert and Lang [6] have computed its order to be $Q = p \cdot \prod \frac{1}{4}\mathbb{B}_{2,\chi}$, where the product is taken over all even characters of $(\mathbb{Z}/p\mathbb{Z})^*$. Here $\mathbb{B}_{2,\chi}$ is the periodic generalized Bernoulli number (see Lang [7]). The classes of the ∞-cusps generate a subgroup, of the same order Q, rational over $\mathbb{Q}(\zeta_p)^+$. The following table gives the value of Q in the first seven interesting cases. There were computed by Glenn Stevens on a computing machine.

p	Q
13	19
17	$2^3 \cdot 73$
19	$3^2 \cdot 487$
23	$11 \cdot 37181$
29	$2^6 \cdot 3 \cdot 7 \cdot 43 \cdot 17837$
31	$2^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 2302381$
37	$3^2 \cdot 5 \cdot 7 \cdot 19 \cdot 37 \cdot 73 \cdot 577 \cdot 17209$

Table 1

The standard Hecke operators T_l (for $l \neq p$), and $\langle a \rangle$ (for $a \in (\mathbb{Z}/p\mathbb{Z})^*/(\pm 1)$) induce endomorphisms of $J_1(p)_{/\mathbb{Q}}$. For a detailed description of these see Wiles [17]. We recall that all of these operators are defined over $\mathbb{Q}$, and that all commute pairwise. We define the Hecke algebra $\mathbb{T}$ to be the ring of endomorphisms of $J_1(p)_{/\mathbb{Q}}$ generated over $\mathbb{Z}$ by the T_l, and $\langle a \rangle$. We recall the action of the Hecke operators on the cusps:

$$\langle a \rangle \begin{bmatrix} y \\ 0 \end{bmatrix} = \begin{bmatrix} a^{-1}y \\ 0 \end{bmatrix}$$

$$T_l \begin{bmatrix} y \\ 0 \end{bmatrix} = (l + \langle l \rangle) \begin{bmatrix} y \\ 0 \end{bmatrix}$$

$$\langle a \rangle \begin{bmatrix} 0 \\ x \end{bmatrix} = \begin{bmatrix} 0 \\ ax \end{bmatrix}$$

$$T_l \begin{bmatrix} 0 \\ x \end{bmatrix} = (1 + l\langle l \rangle) \begin{bmatrix} 0 \\ x \end{bmatrix}$$

3. Quotients of $J_1(p)$ and completions of $\mathbb{T}$

Let $\langle a \rangle$ be a generator for the group $U = \{\langle a \rangle : a \in (\mathbb{Z}/p\mathbb{Z})^*/(\pm 1)\}$. For each integer i dividing $\dfrac{p-1}{2}$ let $J^{(i)}$ be the maximal quotient of $J_1(p)_{/\mathbb{Q}}$ on which $\langle \alpha \rangle$ acts as a primitive i^{th} root of unity. With this notation we see that $J^{(1)}$ is isogenous to $J_0(p)_{/\mathbb{Q}}$, and that $J_1(p)_{/\mathbb{Q}}$ is isogenous to the product $\prod_{i|(p-1)/2} J^{(i)}$. The abelian variety $J^{(i)}$attains everywhere good reduction over the subfield of $\mathbb{Q}(\zeta_p)^+$ whose degree over $\mathbb{Q}$ is equal to i (see Deligne–Rapoport [1], p. 111).

Let $\mathbb{T}^{(i)}$ denote the projection of $\mathbb{T}$ to $J^{(i)}$. Then the dimension of $J^{(i)}$ is $[\mathbb{T}^{(i)} \otimes \mathbb{Q} : \mathbb{Q}]$. Of course, $\mathbb{T}^{(i)}$ contains an isomorphic copy of the group of i^{th} roots of unity, namely the image of the group U. Thus, the dimension of $J^{(i)}$ is a multiple of $r = [\mathbb{T}^{(i)} \otimes \mathbb{Q} : \mathbb{Q}(\zeta_i)]$. We call r the *reduced genus* of $J^{(i)}$. For abelian varieties of reduced genus one we note the following: The ring $\mathbb{Z}[\langle \alpha \rangle] = \mathbb{Z}[\zeta_i]$ is integrally closed. Moreover, the endomorphisms T_l are integral over $\mathbb{Z}$ (since they generate a finite $\mathbb{Z}$-algebra). Thus, the T_l lie in $\mathbb{Z}[\zeta_i]$, and this is the entire Hecke ring $\mathbb{T}^{(i)}$.

From now on we fix an integer $i \neq 1$ dividing $\dfrac{p-1}{2}$. Let C be the projection to $J^{(i)}$ of the group generated by the rational cusps. The Hecke ring $\mathbb{T}$ preserves the group C. Define the Eisenstein ideal I to be

the kernel of the homomorphism $\mathbb{T} \to \mathbb{T}^{(i)} \to \mathrm{End}(C)$. The ideal I contains elements of the form $T_l - (1 + l\langle l\rangle)$ for $l \neq p$, and $f_i(\langle\alpha\rangle)$, where $f_i(x)$ is the primitive cyclotomic polynomial defining the field $\mathbb{Q}(\zeta_i)$. If q is a prime number dividing the order of the cuspidal group C we let C_q be the q-Sylow subgroup of C, and we define the q-Eisenstein prime π to be the maximal ideal of $\mathbb{T}$, above q, in the support of I.

Let $\mathbb{T}_q$ be the completion of $\mathbb{T}$ at the ideal generated by q. Since $\mathbb{T}$ is a free $\mathbb{Z}$-module of finite type we have that $\mathbb{T}_q = \mathbb{T} \otimes Z_q$. Denote by $\mathbb{T}_\pi$ the completion of $\mathbb{T}$ with respect to the Eisenstein prime π, i.e., $\mathbb{T}_\pi = \varprojlim_n \mathbb{T}/\pi^n \cdot \mathbb{T}$. Since $\mathbb{T}_q$ is a semi-local ring, $\mathbb{T}_\pi$ is a direct factor of $\mathbb{T}_q$. Letting $\mathbb{T}'_\pi$ be the complementary factor, we write $\mathbb{T}_q = \mathbb{T}_\pi \times \mathbb{T}'_\pi$. Corresponding to this we have an idempotent decomposition of the identity

$$1 = e_\pi \times e'_\pi \qquad \ldots(\#)$$

Let $J[\pi]_{/\mathbb{Q}}$ be the kernel of the q-Eisenstein prime π in the Jacobian $J_1(p)_{/\mathbb{Q}}$, i.e., $J[\pi]_{/\mathbb{Q}} = \bigcap_{\alpha\in\pi} (\ker\alpha \text{ in } J_1(p)_{/\mathbb{Q}}) = \bigcap_{\alpha\in\pi} (\ker\alpha \text{ in } J_1(p)[q]_{/\mathbb{Q}})$. We define $J[\pi]_{/\mathbb{Z}}$ to be the Zariski closure of $J[\pi]_{/\mathbb{Q}}$ in the Néron model $J_{/\mathbb{Z}}$ of $J_1(p)_{/\mathbb{Q}}$ over $\mathbb{Z}$. If q is different from p the group scheme $J[\pi]_{/\mathbb{Z}}$ is a finite, flat subgroup of $J_{/\mathbb{Z}}$. Note, however, that $J[\pi]_{/\mathbb{Z}}$ may not be the full scheme theoretic kernel of π in $J_{/\mathbb{Z}}$, since $J_{/\mathbb{Z}}$ need not be an abelian scheme.

To the ideal $\pi \subseteq \mathbb{T}$ we associate another ideal γ_π, that is the kernel of the map $\mathbb{T} \to \mathbb{T}_\pi$. We let $\gamma_\pi J \subset J_1(p)_{/\mathbb{Q}}$ be the abelian subvariety generated by the images $\alpha \cdot J_1(p)_{/\mathbb{Q}}$ for $\alpha \in \gamma_\pi$. Define the π-Eisenstein quotient $J^{(\pi)}$ of $J_1(p)_{/\mathbb{Q}}$ by the exactness of the sequence

$$0 \to \gamma_\pi \cdot J_1(p)_{/\mathbb{Q}} \to J_1(p)_{/\mathbb{Q}} \to J^{(\pi)} \to 0.$$

Note that $J^{(\pi)}$ is a simple abelian variety if $\mathbb{T}_\pi$ is a discrete valuation ring.

4. π-divisible groups and Tate modules

Let $J_q = \varinjlim_n J[q^n]_{/\mathbb{Q}}$, and let $J_\pi = \varinjlim_n J[\pi^n]_{/\mathbb{Q}}$.

Then J_q (respectively, J_π) is a q-divisible group over $\mathbb{Q}$ which admits a natural action of $\mathbb{T}_q$ (respectively, $\mathbb{T}_\pi$). Corresponding to the idempotent

decomposition (#) of §3 we have a decomposition of q-divisible groups

$$J_q = J_\pi \times J'_\pi.$$

We define the π-adic Tate module $\mathrm{Ta}(\pi)$ to be the Galois module $\mathrm{Hom}(\mathbb{Q}_q/\mathbb{Z}_q, J_\pi(\bar{\mathbb{Q}}))$. This is, in a natural way, a module over $\mathbb{T}_\pi$. Similarly, we may define the q-adic Tate module to be the Galois module $\mathrm{Hom}(\mathbb{Q}_q/\mathbb{Z}_q, J_q(\bar{\mathbb{Q}}))$.

Let $J_{\mathbb{C}}$ be the complex Lie group associated to $J_1(p)_{/\mathbb{C}}$, and let $\tilde{U}$ be the universal covering group of $J_{\mathbb{C}}$. We may identify the singular homology group $H_1(X_1(p)_{\mathbb{C}}; \mathbb{Z})$ with the kernel of the homomorphism $\tilde{U} \to J_{\mathbb{C}}$. This identification gives rise to an isomorphism

$$J_q(\mathbb{C}) = H^1(X_1(p)_{\mathbb{C}}; \mathbb{Z}) \otimes \mathbb{Q}_q/\mathbb{Z}_q = H^1(X_1(p)_{\mathbb{C}}; \mathbb{Q}_q/\mathbb{Z}_q).$$

This, in turn, yields an isomorphism

$$\mathrm{Ta}(J_q(\mathbb{C})) = \mathrm{Ta}(q) = H_1(X_1(p)_{\mathbb{C}}; \mathbb{Z}_q).$$

The idempotent e_π ((#) of §3) when applied to $\mathrm{Ta}(q)$ gives

$$\mathrm{Ta}(\pi) = H_1(p)_{\mathbb{C}}; \mathbb{Z}_q) \otimes_{\mathbb{T}_q} \mathbb{T}_\pi = H_1(X_1(p)_{\mathbb{C}}; \mathbb{Z}) \otimes_{\mathbb{T}} \mathbb{T}_\pi.$$

The following proposition is based on 3.1 of [17] and 7.7 of [8].

PROPOSITION 1: $\mathrm{Ta}(\pi)$ *is free of rank* 2 *over* $\mathbb{T}_\pi \otimes \mathbb{Q}$.

PROOF: Let Ω be, as usual, the $\mathbb{C}$-vector space of holomorphic 1-forms on $X_1(p)_{\mathbb{C}}$. There is an injection

$$H_1(X_1(p)_{\mathbb{C}}; \mathbb{Z}) \hookrightarrow \mathrm{Hom}(\Omega, \mathbb{C}) \ldots (\#\#)$$

where the map is given by $\omega \mapsto (\gamma \mapsto \int_\omega \gamma)$ By the above discussion it suffices to show that $H_1(X_1(p)_{\mathbb{C}}, \mathbb{Q})$ is free of rank 2 over $\mathbb{T} \otimes \mathbb{Q}$, or the same with $\mathbb{R}$ in place of $\mathbb{Q}$. However, over $\mathbb{R}$ (##) is an isomorphism, so it is enough to show that $\mathrm{Hom}(\Omega, \mathbb{C})$ or even Ω is free of rank 2 over $\mathbb{R}$. Finally, by the Multiplicity One Theorem for $\Gamma_1(p)$ (see [7], p. 125) Ω is free of rank 1 over $\mathbb{T} \otimes \mathbb{C}$. Thus, over $\mathbb{R}$, Ω is free of rank 2. □

As a corollary we obtain

PROPOSITION 2: *Suppose that* $\mathbb{T}_\pi$ *is a principal ideal domain. Then* $\mathrm{Ta}(\pi)$ *is free of rank* 2 *over* $\mathbb{T}_\pi$.

PROOF: $\mathrm{Ta}(\pi)$ is a rank 2 torsion-free module over $\mathbb{T}_\pi$. The assertion of proposition 2 follows from the structure theorem for modules over principal ideal domains. □

5. The representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the kernel of I

From now on we assume that the q-Eisenstein prime π is locally principal and that $\mathbb{T}_\pi$ is an unramified extension of $\mathbb{Z}_q$. Under these conditions the abelian varieties $J_1(p)_{/\mathbb{Q}}$ and $J^{(\pi)}$ have isomorphic π-adic Tate modules.

Since $J_1(p)_{/\mathbb{Q}}$ has good reduction outside of p, its Néron model over $\mathrm{Spec}\, Z\left[\frac{1}{p}\right]$ is an abelian scheme, whose fibre over l we denote by $J_{/\mathbb{F}_l}$. The Eichler–Shimura relation gives the formula

$$T_l = \mathrm{Frob}_l + l\langle l\rangle/\mathrm{Frob}_l$$

on $J_{/\mathbb{F}_l}$. Here Frob_l is the Frobenius endomorphism of the group scheme $J_{/\mathbb{F}_l}$. Now, reduction to characteristic l preserves π-power division points, so the relation $T_l = \mathrm{Frob}_l + l\langle l\rangle/\mathrm{Frob}_l$ is valid on $J_\pi(\bar{\mathbb{Q}})$ (where Frob_l now means any l-Frobenius automorphism in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$). It follows that any $\mathrm{Frob}_l \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ satisfies the quadratic Eichler–Shimura equation

$$X^2 - T_l \cdot X + l\langle l\rangle = 0$$

in its action on $J_\pi[I](\bar{\mathbb{Q}}) = J_\pi^{(\pi)}[I](\bar{\mathbb{Q}})$.

We write f for the residue class degree $[\mathbb{T}_\pi/\pi\cdot\mathbb{T}_\pi]$. If ε is a character of $(\mathbb{Z}/p\mathbb{Z})^*/(\pm 1)$ of order i we write β for the greatest integer for which π^β divides $\mathbb{B}_{2,\varepsilon}$. Since the rational cuspidal group C_q is contained in $J_\pi^{(\pi)}[I](\bar{\mathbb{Q}})$ we see that there is a representation

$$R: \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{T}_\pi/\pi^\beta\cdot\mathbb{T}_\pi)$$

(given by the natural action of Galois on the module of π^β-division points) whose image consists of matrices of the form

$$\begin{pmatrix} 1 & * \\ 0 & \eta \end{pmatrix}$$

for a suitable choice of basis of $J_\pi[I](\bar{\mathbb{Q}})$. Restricted to $I\langle l\rangle$ acts as a

character $\varepsilon(l)$ of order i, and T_l acts as $1 + l \cdot \varepsilon(l)$. Thus, the quadratic Eichler–Shimura equation becomes

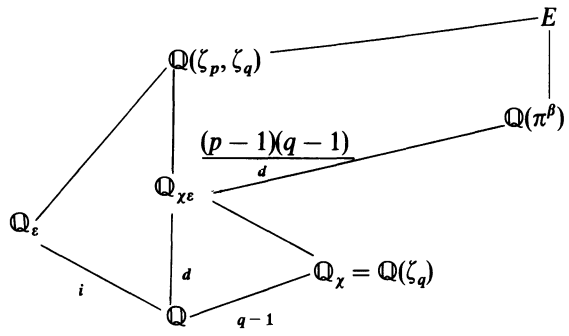
$$X^2 - (1 + l \cdot \varepsilon(l))X + l \cdot \varepsilon(l) = 0.$$

Then $\det(R(\mathrm{Frob}_l)) = l \cdot \varepsilon(l)$ and $\mathrm{Tr}(R(\mathrm{Frob}_l)) = 1 + l \cdot \varepsilon(l)$ so that we may express the character η as the product $\chi \cdot \varepsilon$, where χ is the standard cyclotomic character giving the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on q^{th} roots of 1, and ε is the "nebentypus" character of the simple abelian variety $J^{(\pi)}$ (see Shimura [16]).

6. The diagram of fields

We assume that q is prime to $2 \cdot i \cdot p$. For a character η of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ we let $\mathbb{Q}_\eta$ be the field "cut out" by η, i.e., $\mathbb{Q}_\eta$ is the fixed field of $\ker \eta$. Let $\mathbb{Q}(\pi^\beta)$ be the field obtained from $\mathbb{Q}$ by adjoining the coordinates of the π^β division points of $J^{(\pi)}$. In other words, $\mathbb{Q}(\pi^\beta)$ is the field "cut out" by the representation R.

Let us, temporarily, assume that the representation R does not split (see §7). Then we obtain the following diagram of fields:



Here numbers indicate the degrees of the various field extensions. In particular, $d = \text{l.c.m.}\ (q-1, i)$. The field E is obtained by translating $\mathbb{Q}(\pi^\beta)$ to $\mathbb{Q}(\zeta_p, \zeta_q)$.

We view χ and ε as characters of the idèles: χ is trivial on U_p (the local p-units) so $\chi\varepsilon|_{U_p} = \varepsilon|_{U_p}$ has order i. Similarly, ε is trivial on U_q (the local q-units) so $\chi\varepsilon|_{U_q} = \chi|_{U_q}$ has order $(q-1)$. Thus, q has ramification degree $(q-1)$ in $\mathbb{Q}_{\chi\varepsilon}$, and p has ramification degree i.

7. The nontriviality of $\mathbb{Q}(\pi^\beta)$

For the benefit of the reader we quickly review our notation:

– p is a prime number ≥ 13.

– ε, the nebentypus character of $J^{(\pi)}$, is a nontrivial character (of order i) of $(\mathbb{Z}/p\mathbb{Z})^*/(\pm 1)$.

– q is a rational prime number, relatively prime to $2 \cdot i \cdot p$, dividing the order of the projection C of the rational cuspidal group to $J^{(\pi)}$.

– I, The Eisenstein ideal, is the ideal of $\mathbb{T}$ annihilating C.

– π is the q-Eisenstein prime.

– f is the residue class degree of π, and β is the greatest integer with $\pi^\beta | \mathbb{B}_{2,\varepsilon}$.

The object of this paper is to prove the following:

THEOREM: *Suppose that $\mathbb{T}_\pi$ is an unramified extension of $\mathbb{Z}_q$. Then the representation $R: \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{T}_\pi/\pi^\beta \cdot \mathbb{T}_\pi)$ giving the action of Galois on π^β-division points of $J^{(\pi)}$ is not diagonalizable* mod π. *Moreover, the splitting field $\mathbb{Q}(\pi^\beta)$ of R is an everywhere unramified extension of $\mathbb{Q}_{\chi\varepsilon}$.*

COROLLARY: *Translating the above unramified extension of $\mathbb{Q}_{\chi\varepsilon}$ to $\mathbb{Q}(\zeta_p, \zeta_q)$ yields an everywhere unramified extension E of $\mathbb{Q}(\zeta_p, \zeta_q)$. In particular, q divides the class number of $\mathbb{Q}(\zeta_{pq})$.*

A PROOF OF THE THEOREM: We view the representation R as the reduction mod π^β of the representation ρ giving the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the π-adic Tate module $\mathrm{Ta}(\pi)$. We suppose that the (*) occurring in the upper right-hand corner of $\mathrm{Im}(R)$ is zero (mod π), so that the image of ρ is of the form $\begin{pmatrix} 1 & 0 \\ 0 & \chi\varepsilon \end{pmatrix}$ (mod π). Dividing $J^{(\pi)}$ by the subgroup corresponding to the character $\chi\varepsilon$ we obtain an isogenous abelian variety A for which $\mathrm{Im}(\rho)$ has the form $\begin{pmatrix} \psi & * \\ 0 & \eta \end{pmatrix}$ (mod $\pi^{(\beta+1)}$). We note that this isogeny may be seen on the π-adic Tate module as conjugation by $\begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix}$. We will show that ψ is an everywhere unramified character and this, for various reasons, will imply the theorem.

Since A has good reduction away from p, Theorem 1 of [15] shows that only p and q can ramify. The character ψ is trivial mod π and so has order a power of q. Then if p ramifies in $\mathbb{Q}_\psi$, its ramification degree e_p is a power of q. On the other hand, we know that A attains good reduction over the field $\mathbb{Q}_\varepsilon$, so that e_p must divide i. However, by assumption $q \nmid i$ so e_p must be 1 and ψ is unramified at p.

To show that ψ is unramified at q we use a minor variation of an idea of Ribet's contained in a letter to A. Wiles. Let $D \subseteq \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be a decomposition group for q. We often find it convenient to think of D as the local Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$. Let $\mathrm{Ta}(\pi)^\circ$ and $\mathrm{Ta}(\pi)^{\text{ét}}$ denote the Tate modules associated to the π-divisible groups A_π° and $A_\pi^{\text{ét}}$. These modules are each free of rank 1 over $\mathbb{T}_\pi$ (since $A[\pi]^\circ$ and $A[\pi]^{\text{ét}}$ are both non-zero). Then, corresponding to the exact sequence

$$0 \to A_\pi^\circ \to A_\pi \to A_\pi^{\text{ét}} \to 0$$

of π-divisible groups we have a sequence of $\mathbb{T}_\pi[D]$-modules

$$0 \to \mathrm{Ta}(\pi)^\circ \to \mathrm{Ta}(\pi) \to \mathrm{Ta}(\pi)^{\text{ét}} \to 0.$$

Let ϕ and τ be the characters giving the action of D on $\mathrm{Ta}(\pi)^{\text{ét}}$ and $\mathrm{Ta}(\pi)^\circ$. Then, of course, ϕ is unramified. Moreover, we have the following congruences:

(1) $\phi\tau \equiv \psi\eta \pmod{\pi^{\beta+1}}$
(2) $\phi + \tau \equiv \psi + \eta \pmod{\pi^{\beta+1}}$
(3) $\phi \equiv \psi \equiv 1 \pmod{\pi}$
(4) $\eta \equiv \tau \equiv \chi\varepsilon \pmod{\pi}$.

(1) and (2) show that $\phi(\psi+\eta) \equiv \phi(\phi+\tau) = \phi^2 + \phi\tau \equiv \phi^2 + \psi\eta \pmod{\pi^{\beta+1}}$. So, $(\phi-\psi)(\phi-\eta) \equiv 0 \pmod{\pi^{\beta+1}}$. Taken together with (3) and (4), this tells us that $\phi(\sigma) = \psi(\sigma)$ for all $\sigma \in D$ with $\chi\varepsilon(\sigma) \neq 1 \pmod{\pi}$. Thus, $\phi(\sigma) = \psi(\sigma)$ for all $\sigma \in D$ (if $\chi\varepsilon(\sigma) = 1$, write σ as $a^{-1} \cdot a\sigma$ with $\chi\varepsilon(a^{-1})$ and $\chi\varepsilon(a\sigma) \neq 1$). So ψ is trivial on the inertia subgroup I_q of D, i.e., ψ is unramified at q. Then ψ is an everywhere unramified character of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and so is trivial. It follows that $\eta \equiv \chi\varepsilon \pmod{\pi^{(\beta+1)}}$, so that our representation has the form $\begin{pmatrix} 1 & * \\ 0 & \chi\varepsilon \end{pmatrix} \pmod{\pi^{(\beta+1)}}$.

Let $g = \sum a_n q^n$ be a weight-two new form associated to A (see Shimura [16]). Then $\mathbb{T}|_A \cong \mathbb{Z}[\varepsilon][\{a_n : n = 1, 2, \ldots\}]$ under the map $a \mapsto \varepsilon(a)$ and $T_l \mapsto \dfrac{g|T_l}{g} = a_l$. Since T_l acts as the trace of Frobenius, what we have just shown is that $a_l \equiv 1 + l \cdot \varepsilon(l) \pmod{\pi^{(\beta+1)}}$. Let $G_{2,\varepsilon} = \dfrac{-\mathbb{B}_{2,\varepsilon}}{2} + \sum_{n>0} \sum_{d|n} \varepsilon(d) \cdot d \cdot q^n$ be the usual weight-two Eisenstein series for $\Gamma_0(p, \varepsilon)$. Then, except possibly for the constant terms, g and $G_{2,\varepsilon}$ agree (mod $\pi^{(\beta+1)}$). Thus, $g - G_{2,\varepsilon}$ is a weight-two holomorphic modular form having all of its q-coefficients (other than the constant term) in the ideal $\pi^{(\beta+1)}$. The q-expansion principle (as stated in Katz [3] is valid

here and tells us that the constant term $\frac{1}{2}\mathbb{B}_{2,\varepsilon}$ is in $\pi^{(\beta+1)}$ as well. This is, of course, contrary to hypothesis. Thus, (*) is non-zero.

REMARK: In any given example, the following elementary argument often allows us to bypass the study of the modular form g: We have seen that the image of ρ is of the form $\begin{pmatrix} 1 & * \\ 0 & \chi\varepsilon \end{pmatrix} \pmod{\pi^{(\beta+1)}}$. This means that there is a space of $(q^f)^{(\beta+1)}$ points on A rational over $\mathbb{Q}$. Since A has good reduction at 2, reduction of A modulo 2 is injective on the s-torsion points of A if s is a prime number $\neq 2$. Now, the number N of $\mathbb{F}_2$ – rational points on $A_{/\mathbb{F}_2}$ is precisely $\prod_{i=1}^{2\dim A}(1-\omega_i)$, where the ω_i are the eigenvalues of Frobenius. The Riemann hypothesis for abelian varieties over finite fields tell us that $|\omega_i| = \sqrt{2}$, so $N < (1+\sqrt{2})^{2\cdot\dim A}$. We write the order c of the projection of the rational cuspidal group to $J^{(\pi)}$ as $c = 2^a \cdot q^b \cdot l$ where l is prime to 2 and q. Then there are at least $l\cdot(q^f)^{(\beta+1)}$ points of A rational over $\mathbb{F}_2$. It often happens (in fact, it happens in every case I have checked) that $l\cdot(q^f)^{(\beta+1)} > (1+\sqrt{2})^{2\cdot\dim A}$. For example, the following table produces some values of q and the dimensions of $J^{(\pi)}$ in the first six cases. In each case, $J^{(\pi)}$ is some $J^{(i)}$ (see §3) and the appropriate value of i is given. Also, in each case, $\mathbb{T}_\pi \cong \mathbb{Z}_q$ (see [4] where several examples are explicitly computed).

p	q	$\dim J_1(p)$	$\dim J^{(\pi)}$	i
13	19	2	2	6
17	73	5	4	8
19	487	7	6	9
23	37181	12	10	11
29	17387	22	12	14
31	2302381	26	16	15

Table 2

Finally, to complete the proof of Theorem 1, we wish to show that the extension $\mathbb{Q}(\pi^\beta)/\mathbb{Q}_{\chi\varepsilon}$ is everywhere unramified. For this, it suffices to show that p and q are unramified (since $J^{(\pi)}$ has good reduction away from p). Over $\mathbb{Q}_\varepsilon$ A attains good reduction, so p can have ramification degree at most i in $\mathbb{Q}(\pi^\beta)$. But p already has ramification degree i in $\mathbb{Q}_{\chi\varepsilon}$ (see §6), so p can ramify no further in the extension $\mathbb{Q}(\pi^\beta)/\mathbb{Q}_{\chi\varepsilon}$. The following standard local argument shows that q cannot ramify.

LEMMA: *The restriction of R to a q-decomposition group $D \subseteq \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is diagonalizable. Thus, over $\mathbb{Q}_{\chi\varepsilon}$ $R|_D$ is trivial.*

PROOF: We view D as the local Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}_q/\mathbb{Q}_q)$. Let N be the Néron model of $J^{(\pi)}$ over $\mathbb{Z}_q$, and let $N[\pi^\beta]$ be the Zariski closure of $J^{(\pi)}[\pi^\beta]$ in N. D acts trivially on a one-dimensional subspace $C_q \subseteq J^{(\pi)}[\pi^\beta]$ and via $\chi\varepsilon$ on the quotient $J^{(\pi)}[\pi^\beta]/C_q$. By Raynaud's theorem (as stated in Mazur [9], 1) the Zariski closure $\mathscr{C}$ of C_q in $N[\pi^\beta]$ is a constant (hence étale) subgroup scheme of $N[\pi^\beta]$ of order $(q^f)^\beta$ over $\mathbb{Z}_q$. Over $\mathbb{Z}_q$ there is the standard short exact sequence decomposing $N[\pi^\beta]$

$$0 \to N[\pi^\beta]^\circ \to N[\pi^\beta] \to N[\pi^\beta]^{\text{ét}} \to 0.$$

Since $N[\pi^\beta]^\circ$ and $N[\pi^\beta]^{\text{ét}}$ are each of order $(q^f)^\beta$ the étale subgroup scheme $\mathscr{C}$ provides us with a splitting of this sequence, $N[\pi^\beta] \cong \mathscr{C} \times N[\pi^\beta]^\circ$. Thus, the representation R restricted to D is diagonal. □

This concludes the proof of the Theorem.

REMARKS: (1) In [13] Ken Ribet considers the case $p = q$ and shows the existence of a continuous representation $\rho: \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F}_{p^t})$ that "cuts out" an unramified p-extension of $\mathbb{Q}(\zeta_p)$. His representation also comes from $J_1(p)$, but is not specifically related to a cuspidal group.

(2) We again suppose that $q = p$. Let $\theta: \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathbb{Z}_p^*$ be the character satisfying $\zeta^g = \zeta^{\theta(g)}$ for all $g \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. If A is the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$, we may decompose A as a direct sum $A = \bigoplus_{i \bmod (p-1)} A(\theta^i)$ where $A(\theta^i)$ is the θ^i-eigenspace of A. Let $n = v_p(\mathbb{B}_{2,\theta^{-i-1}})$. Wiles [17] constructs a quotient B of $J_1(p)/J_0(p)$ with the property that the splitting field of $B[I](\bar{\mathbb{Q}})$ (same I as above) is an unramified extension of $\mathbb{Q}(\zeta_{p^n})$ of degree p^n if $A(\theta^i)$ is cyclic. This has recently been generalized (eliminating the hypothesis that $A(\theta^i)$ is cyclic) by Mazur and Wiles [11] in their proof of the main conjecture for powers of the Teichmüller character.

(3) Our theorem simply says that there is no analogue of the Shimura subgroup ([8], Chapter II, §11) for $J_1(p)$.

REFERENCES

[1] P. DELIGNE and N. RAPOPORT: Schémas de modules de courbes elliptiques. *Lecture Notes in Mathematics 349*, Berlin-Heidelberg-New York, Springer-Verlag, 1973.

[2] M. DEMAZURE: Lectures on p-divisible groups. *Lecture Notes in Mathematics 302*, Berlin-Heidelberg-New York, Springer-Verlag, 1972.

[3] N. KATZ: p-adic properties of modular schemes and modular forms, Vol. III of the Proceedings of the International Summer School on Modular Functions, Antwerp, 1972. *Lecture Notes in Mathematics 350*, Berlin-Heidelberg-New York, Springer-Verlag, 1973.
[4] S. KAMIENNY: Harvard Ph.D. Thesis (December 1980).
[5] S. KAMIENNY and G. STEVENS: Special values of L-functions attached to $X_1(N)$, to appear.
[6] D. KUBERT and S. LANG: *Modular Units*, Berlin-Heidelberg-New York, Springer-Verlag, 1981.
[7] S. LANG: *Introduction to modular forms*, Berlin-Heidelberg-New York, Springer-Verlag, 1976.
[8] B. MAZUR: Modular curves and the Eisenstein ideal. *Publications Mathematiques I.H.E.S. 47* (1978).
[9] B. MAZUR: Rational isogenies of prime degree. *Inv. Math. 44* (1978) 129–162.
[10] B. MAZUR and J. TATE: Points of Order 13 on elliptic curves. *Inv. Math. 22* (1973) 41–49.
[11] B. MAZUR and A. WILES: Class fields of abelian extensions of $\mathbb{Q}$, in preparation.
[12] M. RAYNAUD: Schémas en groupes de type $(p,\ldots,p)$. *Bull. Soc. Math. France 102* (1974) 241–280.
[13] K. RIBET: A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$. *Inv. Math. 34* (1976) 151–162.
[14] J.-P. SERRE: Abelian l-adic representations and elliptic curves. Lectures at McGill University, New York-Amsterdam, W.A. Benjamin, Inc., 1968.
[15] J.-P. SERRE and J. TATE: Good reduction of abelian varieties. *Ann. of Math. 88* (1968) 492–517.
[16] G. SHIMURA: Introduction to the arithmetic theory of automorphic Forms. *Publ. Math. Soc. Japan 11*, Tokyo-Princeton, 1971.
[17] A. WILES: Modular curves and the class group of $\mathbb{Q}(\zeta_p)$. *Inv. Math. 58* (1980) 1–35.

(Oblatum 19-XI-1981 & 15-I-1982)

Department of Mathematics
University of California
Berkeley, CA 94720
U.S.A.