Canad. Math. Bull. Vol. **45** (3), 2002 pp. 337–348

# Surjectivity of mod $\ell$ Representations Attached to Elliptic Curves and Congruence Primes

Imin Chen

*Abstract.* For a modular elliptic curve $E/\mathbb{Q}$, we show a number of links between the primes $\ell$ for which the mod $\ell$ representation of $E/\mathbb{Q}$ has projective dihedral image and congruence primes for the newform associated to $E/\mathbb{Q}$.

## 1 Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. Denote by $\overline{\rho}_{E/\mathbb{Q},\ell}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ its mod $\ell$ representation, *i.e.* the representation obtained by the action of the absolute Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}$ on the $\ell$-torsion points of $E/\mathbb{Q}$ for $\ell$ prime. Let $S_{E/\mathbb{Q}} = \{\ell \text{ prime} \mid \overline{\rho}_{E/\mathbb{Q},\ell} \text{ is not surjective}\}$.

***Theorem 1.1*** **(Serre, [13])** *The set $S_{E/\mathbb{Q}}$ is finite if $E/\mathbb{Q}$ does not have complex multiplication.*

In the same paper [13], the following question was asked.

***Question 1.2*** *Is $S_{\mathbb{Q}} = \bigcup_{E/\mathbb{Q}} S_{E/\mathbb{Q}}$ finite as $E/\mathbb{Q}$ runs through elliptic curves without complex multiplication?*

This question is usually analyzed according to the nature of the image of $\overline{\rho}_{E/\mathbb{Q},\ell}$. If $\overline{\rho}_{E/\mathbb{Q},\ell}$ is not surjective, then by a classification of the subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ we have that $\operatorname{im} \overline{\rho}_{E/\mathbb{Q},\ell}$ is contained the normalizer $N'$ or $N$ of a non-split or split Cartan subgroup, a Borel subgroup $B$, or a subgroup $D$ with projective image $S_4$. The former three subgroups can be conjugated into one of the following standard forms (under the assumption $\ell$ is odd in case of $N'$), respectively,

$$N' = \left\{ \begin{pmatrix} \alpha & \lambda\beta \\ \beta & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & \lambda\beta \\ -\beta & -\alpha \end{pmatrix} \;\middle|\; \alpha, \beta \in \mathbb{F}_\ell, (\alpha, \beta) \neq (0,0) \right\}$$

$$N = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \begin{pmatrix} 0 & b \\ a & 0 \end{pmatrix} \;\middle|\; a, b \in \mathbb{F}_\ell^\times \right\}$$

Received by the editors October 24, 2000; revised March 15, 2001.
This research was supported by CICMA (1998-99) and MPIM (2000).
AMS subject classification: Primary: 11G05; secondary: 11F80.
Keywords: torsion points of elliptic curves, Galois representations, congruence primes, Serre tori, grossencharacters, non-split Cartan.




https://doi.org/10.4153/CMB-2002-036-3 Published online by Cambridge University Press

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \,\middle|\, a, d \in \mathbb{F}_\ell^\times, b \in \mathbb{F}_\ell \right\},$$

where $\lambda$ is a non-square in $\mathbb{F}_\ell^\times$.

Let $S^H_{E/\mathbb{Q}} = \{\ell \text{ prime} \mid \operatorname{im}(\overline{\rho}_{E/\mathbb{Q},\ell}) \subset \text{a conjugate of } H\}$. For $H$ being conjugate to one of $N'$, $N$, $B$, $D$, one can ask whether $S^H_{\mathbb{Q}} = \bigcup_{E/\mathbb{Q}} S^H_{E/\mathbb{Q}}$ is finite as $E/\mathbb{Q}$ runs through elliptic curves without complex multiplication.

Mazur's [6] results on rational isogenies of prime degree show that

$$S^B_{\mathbb{Q}} \subset \{p \text{ prime} \mid p \leq 37\}.$$

Momose shows [9] that an $E/\mathbb{Q}$ with $\operatorname{im}(\overline{\rho}_{E/\mathbb{Q},\ell})$ contained in a conjugate of $N$ has potentially good reduction at all odd primes if $\ell > 13$. These results rely on studying the associated modular curves and bounding their $\mathbb{Q}$-rational points via the arithmetic and geometry of their jacobians. Finally, Serre shows that $S^D_{\mathbb{Q}} \subset \{p \text{ prime} \mid p \leq 13\}$ using local methods (*cf.* [6] p. 36).

The case of $N'$ is the most difficult to study using jacobians of modular curves because the jacobians in question do not have a non-trivial quotient with finitely-many $\mathbb{Q}$-rational points.

In this paper, we investigate more carefully the sets $S^N_{E/\mathbb{Q}}$ and $S^{N'}_{E/\mathbb{Q}}$ for a fixed elliptic curve $E/\mathbb{Q}$. Under the assumption of modularity we will analyze these sets from the point of view of modular forms.

***Remark 1.3*** Breuil, Conrad, Diamond and Taylor have recently established the modularity of all elliptic curves over $\mathbb{Q}$ [1] so this assumption is no longer necessary.

We briefly recall one such connection implicit in work of Ribet [10] and Kraus [5]. Suppose $E/\mathbb{Q}$ is such that $\operatorname{im}(\overline{\rho}_{E/\mathbb{Q},\ell})$ is contained in $H$ where $H = N', N$ and $\ell$ is odd. Let $C'$ and $C$ denote the split and non-split Cartan subgroups which are normalized by $N'$ and $N$, respectively.

Let $\epsilon_{E/\mathbb{Q},\ell}$ be the character obtained by composing $\overline{\rho}_{E/\mathbb{Q},\ell}$ with the map to the quotients $N/C \cong N'/C' \cong \{\pm 1\}$. The character $\epsilon_{E/\mathbb{Q},\ell}$ is non-trivial in the case $H = N'$ as complex conjugation cannot be sent to an element in $C'$ under $\overline{\rho}_{E/\mathbb{Q},\ell}$. In the case $H = N$, we may assume without loss of generality that $\epsilon_{E/\mathbb{Q},\ell}$ is non-trivial or else we are back in the $H = B$ case. Thus, the character $\epsilon_{E/\mathbb{Q},\ell}$ cuts out a quadratic extension $K$ of $\mathbb{Q}$ which is imaginary in the case $H = N'$.

The representation $\overline{\rho}_{E/\mathbb{Q},\ell} \cong \operatorname{Ind}^{\mathbb{Q}}_K \chi$ is induced from a character $\overline{\chi}\colon G_K \to \mathbb{F}^\times$, where $\mathbb{F} = \mathbb{F}_{\ell^2}$ or $\mathbb{F}_\ell$ in the cases $H = N'$ or $N$, respectively. It thus has the property $\overline{\rho}_{E/\mathbb{Q},\ell} \otimes \epsilon_{E/\mathbb{Q},\ell} \cong \overline{\rho}_{E/\mathbb{Q},\ell}$. The following lemma can then be shown.

***Lemma 1.4*** *Let $E/\mathbb{Q}$ be a modular elliptic curve whose associated newform is $f \in S_2\big(\Gamma_0(N_E)\big)$. Suppose $\operatorname{im}(\overline{\rho}_{E/\mathbb{Q},\ell}) \subset H$ with $H = N', N$ and $\ell$ is odd. Let $E'$ be the twist of $E$ by $\epsilon_{E/\mathbb{Q},\ell}$, and let $f'$ be the corresponding twist of $f \in S_2\big(\Gamma_0(N_E)\big)$. Then $N_{E'} = N_E$ and $f' \in S_2\big(\Gamma_0(N_E)\big)$ is a newform.*

**Proof** Kraus shows in [5] that the type of reduction (good, multiplicative, additive) of $E$ and $E'$ are the same, *i.e.* the tame exponents $\epsilon_p$ of $E$ and $E'$ are the same. On the other hand, the wild exponent $\delta_p$ of $E$ depends only on the restriction of $\overline{\rho}_{E/\mathbb{Q},\ell}$ and $\overline{\rho}_{E',\ell} = \overline{\rho}_{E/\mathbb{Q},\ell} \otimes \epsilon_{E/\mathbb{Q},\ell}$ to the wild inertia group at $p$. For $p \geq 3$, the restrictions are the same as $\epsilon_{E/\mathbb{Q},\ell}$ is trivial on the wild inertia at $p$. For $p = 2$, the restrictions still have the same image. ∎

We say that two eigenforms $f, g \in S_2\big(\Gamma_0(N)\big)$ are *congruent modulo* $\lambda$ if $a_p(f) \equiv a_p(g) \pmod{\lambda}$ for $p \nmid \ell N$ where $\lambda$ is a prime above $\ell$ of $\mathbb{Q}\big(a_p(f), a_p(g)\big)$. We say that $\ell$ is a *congruence prime* for newform $f \in S_2\big(\Gamma_0(N)\big)$, if there exists an eigenform $g$ in the (Petersson) orthogonal complement of $f$ such that $g$ is congruent to $f$ modulo $\lambda$ above $\ell$.

The property that $\rho_{E'/\mathbb{Q},\ell} \cong \overline{\rho}_{E/\mathbb{Q},\ell} \otimes \epsilon_{E/\mathbb{Q},\ell} \cong \overline{\rho}_{E/\mathbb{Q},\ell}$ implies the two newforms $f, f'$ are congruent modulo $\ell$. Thus the following proposition holds.

***Proposition 1.5*** *Let $E/\mathbb{Q}$ be a modular elliptic curve whose associated newform is $f \in S_2\big(\Gamma_0(N_E)\big)$. Suppose $\ell$ is odd and $\mathrm{im}(\overline{\rho}_{E/\mathbb{Q},\ell})$ is contained in $N'$, or $N$ but not $C$. Then $\ell$ is a congruence prime for $f$.*

In this paper, we will show that there are additional congruences between $f$ and CM-forms in the case $N'$ and discuss how the character of these CM-forms can be controlled under certain hypotheses.

***Theorem 1.6*** *Let $E/\mathbb{Q}$ be a modular elliptic curve whose associated newform is $f \in S_2\big(\Gamma_0(N_E)\big)$. Suppose $\mathrm{im}(\overline{\rho}_{E/\mathbb{Q},\ell}) \subset N'$ for $3 < \ell \nmid N_E$. Then there exists a newform $g \in S_2\big(\Gamma_1(M)\big)$ which is induced from a grossencharacter on $K$ and is congruent to $f$ modulo $\lambda$ a prime above $\ell$ where $M|N_E$ is the Artin conductor of $\overline{\rho}_{E/\mathbb{Q},\ell}$.*

***Theorem 1.7*** *Let $E/\mathbb{Q}$ be a modular elliptic curve whose associated newform is $f \in S_2\big(\Gamma_0(N_E)\big)$ and $16 \nmid N_E$. Suppose $\mathrm{im}(\overline{\rho}_{E/\mathbb{Q},\ell}) \subset N'$ for $3 < \ell \nmid N_E$. Then there exists a newform $g \in S_2\big(\Gamma_0(M)\big)$ which is induced from a grossencharacter on $K$ and is congruent to $f$ modulo $\lambda$ a prime above $\ell$ where $M|N_E$ is the Artin conductor of $\overline{\rho}_{E/\mathbb{Q},\ell}$.*

I would like to thank F. Momose for mentioning to me the connection between elliptic curves with $\mathrm{im}(\overline{\rho}_{E/\mathbb{Q},\ell}) \subset N'$ and grossencharacters on imaginary quadratic fields (*cf.* also the paper [8] from which the case of prime power $N_E$ in Theorem 1.7 follows).

## 2 Congruences with CM-forms

### 2.1 Algebraic characters

Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and an algebraic closure $\overline{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$. Let $K \subset \overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_\ell$ be a number field and denote by $D_K$ the set of embeddings of $K$ into $\overline{\mathbb{Q}}$.

Let $T/\mathbb{Q} = \mathrm{Res}^K_{\mathbb{Q}}(\mathbb{G}_m/K)$ be the restriction of scalars of $\mathbb{G}_m/K$ to $\mathbb{Q}$. This is a commutative algebraic group over $\mathbb{Q}$, isomorphic over $\overline{\mathbb{Q}}$ to $\mathbb{G}_m^{[K:\mathbb{Q}]}$, with the following properties.

https://doi.org/10.4153/CMB-2002-036-3 Published online by Cambridge University Press

1. $T(\mathbb{Q}) = K^\times$ and $T(\mathbb{Q}_\ell) = (K \otimes \mathbb{Q}_\ell)^\times = \prod_{v|\ell} K_v$

2. For all $\sigma \in D_K$, there is an algebraic character $[\sigma]\colon T/\overline{\mathbb{Q}} \to \mathrm{GL}_1/\overline{\mathbb{Q}}$ such that the composition

$$K^\times = T(\mathbb{Q}) \subset T(\overline{\mathbb{Q}}) \xrightarrow{[\sigma]} \mathrm{GL}_1(\overline{\mathbb{Q}}) = \overline{\mathbb{Q}}^\times$$

is given by the embedding $\sigma$.

3. Every algebraic homormorphism $f\colon T/\overline{\mathbb{Q}} \to \mathrm{GL}_1/\overline{\mathbb{Q}}$ is of the form $f = \prod_{\sigma\in D_K}[\sigma]^{n(\sigma)}$ where $n(\sigma) \in \mathbb{Z}$. The element $\sum_{\sigma\in D_K} n(\sigma)\sigma \in \mathbb{Z}[D_K]$ is called the *weight* of $f$ and completely determines $f$. Given a weight $k \in \mathbb{Z}[D_K]$, let $[k]$ denote the algebraic homomorphism determined by $k$.

## 2.2 Grossencharacters of Type $A_0$

Let $K \subset \overline{\mathbb{Q}}$ be a number field. For a place $v$ of $K$, let $K_v$ be the completion of $K$ at $v$, $\pi_v$ a uniformizer of $K_v$, and $\mathcal{O}_v$ the ring of integers of $K_v$ in the case $v$ is a finite place. Let $J_K$ be the idèles of $K$ and $C_K = J_K/K^\times$ the idèle class group. For a modulus $\mathfrak{m}$ of $K$ let $U_\mathfrak{m} = \prod_v U_{\mathfrak{m},v}$ where

$$U_{\mathfrak{m},v} = \begin{cases} \ker\bigl(\mathcal{O}_v^\times \to (\mathcal{O}_v/\mathfrak{m}\mathcal{O}_v)^\times\bigr) & \text{if } v \nmid \infty \\ \text{the connected component of } 1 & \text{if } v|\infty \end{cases}$$

Let $E_\mathfrak{m} = \ker(K^\times \to J_K/U_\mathfrak{m})$ denote the units congruent to 1 modulo $\mathfrak{m}$, and $C_\mathfrak{m} = C/U_\mathfrak{m}K^\times$ be the ray class group of modulus $\mathfrak{m}$.

Let $\chi\colon C_K \to \overline{\mathbb{Q}}_\ell{}^\times$ be a continuous character. This can be written in the form $\chi = \prod_v \chi_v$ where $\chi_v|_{\mathcal{O}_v^\times} = 1$ for all but finitely-many $v$. The homormorphism $\chi\colon C_K \to \overline{\mathbb{Q}}_\ell{}^x$ is said to be *locally algebraic of weight* $k \in \mathbb{Z}[D_K]$ if $\chi_\ell = \prod_{v|\ell}\chi_v$ coincides with the algebraic character $[-k]\colon \prod_{v|\ell} K_v = T(\overline{\mathbb{Q}}_\ell) \to \mathrm{GL}_1(\overline{\mathbb{Q}}_\ell) = \overline{\mathbb{Q}}_\ell{}^\times$ of weight $-k$ on the subgroup $\prod_{v|\ell} U_{\mathfrak{m},v}$. We say $\chi$ has *modulus* $\mathfrak{m}$ if $\chi_\ell$ coincides with $[-k]$ on $\prod_{v|\ell} U_{\mathfrak{m},v}$ and $\chi_v|_{U_{\mathfrak{m},v}} = 1$ for $v \nmid \ell$. The smallest modulus for $\chi$ is called the *conductor* of $\chi$.

When $\ell = \infty$, a locally algebraic character $\chi$ of modulus $\mathfrak{m}$ and weight $k$ coincides with the notion of a grossencharacter of type $A_0$ of modulus $\mathfrak{m}$ and weight $k$.

***Theorem 2.1*** **(Weil, [15])** *Let $\chi$ be a grossencharacter of type $A_0$. The extension $\mathbb{Q}\bigl(\chi(\pi_v) \mid v \nmid \infty\mathfrak{m}\bigr)$ is a finite extension of $\mathbb{Q}$ called the* field generated by *$\chi$.*

***Proposition 2.2*** *Let $k \in \mathbb{Z}[D_K]$ be a weight. There exists a non-trivial grossencharacter of type $A_0$ of weight $k$ and modulus $\mathfrak{m}$ if and only if $[k](E_\mathfrak{m}) = 1$. If this holds then there are $h_\mathfrak{m}$ such grossencharacters where $h_\mathfrak{m}$ is the order of the class group $C_\mathfrak{m}$.*

There is a natural grossencharacter of type $A_0$ of conductor $\mathcal{O}_K$ and weight $\sum_{\sigma\in D_K}\sigma$. This is given by

$$\omega_K\colon C_K \to \mathbb{R}^{>0} \subset \mathbb{C}^\times$$
$$x \mapsto \prod_v \|x_v\|$$

where $\|x_v\| = |x_v|^{[K_v:\mathbb{Q}_p]}$ and for $p$ finite, $|\pi_v| = 1/p^{1/e_v}$, and $e_v$ is the ramification index of $v|p$. The character $\omega_K$ is trivial on $K^\times$ by the product formula.

## 2.3 Fundamental Characters

For $v|\ell$ let $\overline{K_v}$ be a fixed algebraic closure of $K_v$. This fixes an algebraic closure $\overline{k_v}$ of the residue field $k_v$. Let $I_{K_v}$ denote the inertia subgroup of $G_{K_v}$ and $I_{K_v,t}$ its tame quotient.

A character $\overline{\chi}\colon I_{K_v,t} \to \overline{k_v}^\times$ is called a *tame character*. For all $q = \ell^n$, there is a tame character

$$\Theta_{q-1}\colon I_{K_v,t} \to \mathbb{F}_q^\times \subset \overline{k_v}^\times$$

called the *fundamental tame character of level n* which is surjective to $\mathbb{F}_q^\times$.

A tame character is said to have *level n* if its image is contained in $\mathbb{F}_q^\times \subset \overline{k_v}^\times$, $q = \ell^n$, but no smaller finite field. The fundamental tame character of level $n$ has the property that any character $\overline{\chi}$ of level $\leq n$ can be expressed as a power of $\Theta_{q-1}$.

Suppose $\overline{\chi}$ is a tame character of level $n$ and $\overline{\chi} = \Theta_{q-1}^a$ with $0 \leq a < q-1$. Because of the assumption that $\overline{\chi}$ has level $n$, not all possible $a$ arise. We may write the integer $a$ uniquely in the form $a = a_0 + a_1\ell + \cdots + a_{n-1}\ell^{n-1}$ where $0 \leq a_i \leq \ell - 1$ and hence $\overline{\chi} = \Theta_{q-1}^{a_0}\Theta_{q-1}^{\ell a_1}\cdots\Theta_{q-1}^{\ell^{n-1}a_{n-1}}$.

Let $\overline{\chi}\colon G_{K_v^{\mathrm{ab}}} \to \overline{k_v}^\times$ be a character and consider its restriction to $I_{K_v^{\mathrm{ab}}}$. This restriction factors to $I_{K_{v,t}^{\mathrm{ab}}}$ to yield a tame character $\overline{\chi}$ which we also denote by $\overline{\chi}$. The local class field homomorphism $r_v\colon K_v^\times \to G_{K_v^{\mathrm{ab}}}$ induces an isomorphism $k_v^\times \cong I_{K_{v,t}^{\mathrm{ab}}}$ so that the tame character $\overline{\chi}$ has level $\leq n$ where $q = \ell^n = \#k_v$. We denote by $\overline{\chi}|_{k_v^\times}$ the character on $k_v^\times$ obtained by precomposing the tame character $\overline{\chi}$ with the local class field homomorphism. Let $D_{K_v}$ denote the set of embeddings $\sigma_v\colon K_v \to \overline{K_v}$. For each such embedding $\sigma_v$, let $\overline{\sigma_v}\colon k_v \to \overline{k_v}$ denote the associated embedding of residue fields. We can therefore write the tame character in the form as above $\overline{\chi} = \prod_{\sigma_v\in D_{K_v}} \Theta_{q-1}^{\overline{\sigma_v}a(\sigma_v)}$ where $0 \leq a(\sigma_v) \leq \ell - 1$. The element $\sum_{\sigma_v\in D_{K_v}} a(\sigma_v)\sigma_v \in \mathbb{Z}[D_{K_v}]$ is called the *optimal weight* of $\overline{\chi}$ at $v$.

A calculation in [13] shows that the composition

$$k_v^\times \cong I_{K_v^{\mathrm{ab}}} \xrightarrow{\Theta_{q-1}} k_v^\times$$

corresponds with the character $x \mapsto x^{-1}$.

# 3 Adjustment to Optimal Level and Weight

***Proposition 3.1*** *Let $\mathbb{Q} \subset K \subset \overline{\mathbb{Q}}$ be an imaginary quadratic field whose set of embeddings to $\overline{\mathbb{Q}}$ is denoted by $D_K = \{1, \tau\}$. Let $\overline{\chi}\colon G_K \to \mathbb{F}_{\ell^2}^\times$ be a continuous character with Artin conductor $\mathfrak{m}$ and let $\widetilde{\chi}\colon C_K \to \mathbb{C}^\times$ be its Teichmüller lift considered as a continuous character of $C_K$. Suppose that*

1. *$\ell \geq 5$ is inert in $K$*

https://doi.org/10.4153/CMB-2002-036-3 Published online by Cambridge University Press

2. $\overline{\chi}|_{k_\ell^\times} = \overline{[1]}^{-1}$.

*Then there exists a grossencharacter $\chi$ of type $A_0$ with conductor $\mathfrak{m}$ and weight 1 and a prime $\lambda$ above $\ell$ in the field generated by $\widetilde{\chi}$ and $\chi$ such that $\widetilde{\chi}(\pi_v) \equiv \chi(\pi_v) \pmod{\lambda}$ for all $v \nmid \infty\ell\mathfrak{m}$.*

**Proof** By the global class field homomorphism $r_K\colon C_K \to G_{K^{\mathrm{ab}}}$ we may regard both $\overline{\chi}$ and $\widetilde{\chi}$ as continuous characters of $C_K$ and can write $\overline{\chi} = \prod_v \overline{\chi}_v$ and $\widetilde{\chi} = \prod_v \widetilde{\chi}_v$ where $\overline{\chi}_v$ and $\widetilde{\chi}_v$ are characters of $K_v^\times$. By comparing $\overline{\chi}_v$ and $\widetilde{\chi}_v$ place by place we see that $\widetilde{\chi}$ has conductor $\mathfrak{m}\ell$ and weight 0.

Let $u \in E_\mathfrak{m} = K^\times \cap U_\mathfrak{m}$. Since $\overline{\chi}$ is trivial on $K^\times$, $\overline{\chi}(u) = 1$. On the other hand, we also have $\overline{\chi}|_{k_\ell^\times}(u) = \overline{[1]}^{-1}(u) = \overline{u}^{-1}$ and $\overline{\chi}|_{U_{\mathfrak{m},v}}(u) = 1$ for $v \neq \ell$. Thus, we have that $u \equiv 1 \pmod{\ell}$. As $K$ is imaginary quadratic and $\ell \geq 5$, this implies $u = 1$.

Since $E_\mathfrak{m}$ is trivial, there exists a grossencharacter $\phi$ of type $A_0$ with modulus $\mathfrak{m}$ and weight 1. Write $\phi = \prod_v \phi_v$. As $\phi$ has weight 1, $\phi_\infty(z) = \overline{z}$. Let $\delta\colon J_K \to \overline{\mathbb{Q}_\ell}^\times$, $\delta = \prod_v \delta_v$ be defined as follows. For $v \nmid \infty\ell$, let $\delta_v = \phi_v$, and define $\delta_\infty = 1$, $\delta_\ell = \phi_v[1]^{-1}$. By construction, $\delta$ factors to a character of $C_K$. Let $\overline{\delta}\colon C_K \to \overline{\mathbb{F}_\ell}^\times$ be the reduction of $\delta$ modulo a prime $\lambda'$ above $\ell$ of the field generated by $\delta$ (which is the same as the field generated by $\delta$), and let $\widetilde{\delta}\colon C_K \to \mathbb{C}^\times$ be the Teichmüller lift of $\overline{\delta}$.

The desired grossencharacter of type $A_0$ is then $\chi = \widetilde{\chi}\widetilde{\delta}^{-1}\phi$. The weight of $\chi$ is 1 and it evidently has modulus $\mathfrak{m}\ell$. In fact, $\chi$ has conductor $\mathfrak{m}$. Since $\chi_\ell = \widetilde{\chi}_\ell\widetilde{\delta}_\ell^{-1}\phi_\ell = \widetilde{[1]}^{-1}\widetilde{[1]}\widetilde{\phi_\ell}^{-1}\phi_\ell$ we see that $\chi_\ell$ is trivial on $\mathcal{O}_\ell^\times$. Thus, $\chi$ has modulus $\mathfrak{m}$. To see that $\chi$ has conductor precisely $\mathfrak{m}$, consider the character $\chi\colon C_K \to \overline{\mathbb{Q}_\ell}^\times$ given by $\chi = \widetilde{\chi}\widetilde{\delta}^{-1}\delta$ which has the same conductor as $\chi$. Since $\chi$ reduces modulo $\lambda$ to $\overline{\chi}$ having Artin conductor $\mathfrak{m}$, it follows that $\mathfrak{m}$ divides the Artin conductor of $\chi$ as the Artin conductor can only decrease under reduction modulo $\lambda$.

For $v \nmid \infty\ell\mathfrak{m}$, $\chi(\pi_v) = \widetilde{\chi}_v(\pi_v)\widetilde{\delta}_v^{-1}(\pi_v)\phi_v(\pi_v) = \widetilde{\chi}_v(\pi_v)\widetilde{\phi_v}^{-1}(\pi_v)\phi_v(\pi_v) \equiv \widetilde{\chi}_v(\pi_v) \pmod{\lambda}$ where $\lambda$ is a prime of the field generated by $\widetilde{\chi}$ and $\widetilde{\delta}$ above $\lambda'$. ■

## 4 Proof of Theorem 1.6

Let $E/\mathbb{Q}$ be a modular elliptic curve whose associated newform is $f \in S_2\big(\Gamma_0(N_E)\big)$. Suppose $\operatorname{im}(\overline{\rho}_{E/\mathbb{Q},\ell}) \subset N'$ for $3 < \ell \nmid N_E$. Then $\overline{\rho}_{E/\mathbb{Q},\ell} \cong \operatorname{Ind}_K^\mathbb{Q} \overline{\chi}$ is induced from a character $\overline{\chi}\colon G_K \to \mathbb{F}_{\ell^2}^\times$ on the imaginary quadratic field $K$ associated to such a $\overline{\rho}_{E/\mathbb{Q},\ell}$. Since $\ell \nmid N_E$, the argument in [13] p. 317 shows that $\ell$ is inert in $K$.

Let us briefly recall the definition of the Serre's *optimal weight* attached to this particular $\overline{\rho}_{E/\mathbb{Q},\ell}$ [14]. Identifying $G_{\mathbb{Q}_\ell}$ with a decomposition subgroup at $\ell$ of $G_\mathbb{Q}$, the restriction of $\overline{\rho}_{E/\mathbb{Q},\ell}$ to $I_{\mathbb{Q}_\ell}$ factors through its tame quotient $I_{\mathbb{Q}_\ell,t}$ and is semi-simple. Since $\ell$ is unramified in $K$, $I_{\mathbb{Q}_\ell} \subset G_K$ so that

$$\overline{\rho}_{E/\mathbb{Q},\ell}|_{I_{\mathbb{Q}_\ell}} \cong \begin{pmatrix} \overline{\chi} & 0 \\ 0 & \overline{\chi}' \end{pmatrix}$$

where $\overline{\chi}'(g) = \overline{\chi}(\tau^{-1}g\tau)$.

Both $\overline{\chi}$ and $\overline{\chi}'$ are tame characters of level 2 so that $\overline{\chi}^{\ell} = \overline{\chi}'$. Write $\overline{\chi} = \Theta_{q-1}^{a_0+\ell a_1}$ where $q = \ell^2 = \#k_v^{\times}$ and $0 \le a_0, a_1 \le \ell - 1$. Since $\overline{\rho}_{E/\mathbb{Q},\ell}$ is induced from either $\overline{\chi}$ or $\overline{\chi}'$, up to switching $\overline{\chi}'$ for $\overline{\chi}$ we may assume $a > b$. The optimal weight is defined as $k = 1 + a_0 + \ell a_1$. Since $\ell \nmid N_E$, Proposition 4 of [14] implies that $k = 2$ and so $a_0 = 1$, $a_1 = 0$ in our situation. Thus, we see that $\overline{\chi}|_{k_v^{\times}} = \overline{[1]}^{-1}$.

Let $\widetilde{\chi}$ be the Teichmüller lift of $\overline{\chi}$. By Proposition 3.1, there exists a grossencharacter $\chi$ of type $A_0$ with conductor $\mathfrak{m}$ and weight 1 such that $\chi(\pi_v) \equiv \widetilde{\chi}(\pi_v) \pmod{\lambda}$ where $\lambda$ is a prime above $\ell$ of the field generated by $\widetilde{\chi}$ and $\chi$.

Let $I(\mathfrak{m})$ denote the group of fractional ideals of $K$ prime to $\mathfrak{m}$. For an ideal $\mathfrak{a} \in I(\mathfrak{m})$ denote by $[\mathfrak{a}]$ the idèle $\prod_{v \nmid \infty\mathfrak{m}} \pi_v^{e_v}$ associated to the ideal $\mathfrak{a} = \prod_{v\nmid\infty\mathfrak{m}} \mathfrak{p}_v^{e_v}$, where $\mathfrak{p}_v$ is the prime of $K$ associated to the finite place $v$, and $\pi_v$ is any choice of uniformizer for $K_v$.

***Theorem 4.1* (Hecke)** *Let $K \subset \overline{\mathbb{Q}}$ be an imaginary quadratic field with discriminant $d_K$ and let $D_K = \{1, \tau\}$ denote its embeddings into $\overline{\mathbb{Q}}$. Let $\chi$ be a grossencharacter of type $A_0$ on $K$ with conductor $\mathfrak{m}$ and weight $k = u \cdot 1 \in \mathbb{Z}[D_K]$, $u > 0$. Consider $g(z) = \sum_{\mathfrak{a}\in I(\mathfrak{m})} \chi([\mathfrak{a}])q(z)^{N_K(\mathfrak{a})}$ where $q(z) = e^{2\pi i z}$. Then $g$ is a newform on $S_{u+1}\big(\Gamma_0(M), \xi\big)$ where $M = N_K(\mathfrak{m})|d_K|$ and $\xi\colon (\mathbb{Z}/M\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$ is defined by $\xi = \epsilon_K \frac{\chi\circ\mathrm{Ver}}{\omega_{\mathbb{Q}}^{u}}$. Here $\epsilon_K\colon C_{\mathbb{Q}} \to \{\pm 1\}$ is the character defining $K$ and $\mathrm{Ver}\colon C_{\mathbb{Q}} \to C_K$ is the Verlagerung map.*

**Proof** *cf.* Theorem 4.8.2 [7] (but note Miyake normalizes his grossencharacters so they are unitary) ∎

Let $g(z) = \sum_{\mathfrak{a}\in I(\mathfrak{m})} \chi([\mathfrak{a}])q(z)^{N_K(\mathfrak{a})} \in S_2\big(\Gamma_1(M)\big)$ be the newform constructed from $\chi$ as in the theorem above. Let $p \nmid \ell M$ be a prime and $\mathrm{Fr}_p \in G_{\mathbb{Q}}$ a Frobenius element at $p$. If $p$ is inert in $K$, then $\mathrm{Fr}_p \notin G_K$ so that $a_p(f) \equiv \mathrm{tr}\,\overline{\rho}_{E/\mathbb{Q},\ell}(\mathrm{Fr}_p) \equiv \mathrm{tr}(\mathrm{Ind}_K^{\mathbb{Q}}\overline{\chi})(\mathrm{Fr}_p) \equiv 0 = a_p(g) \pmod{\lambda}$. If $p$ is split in $K$ with $v_i|p$ being the two places above $p$, then $\mathrm{Fr}_p \in G_K$ so that $a_p(f) \equiv \mathrm{tr}\,\overline{\rho}_{E/\mathbb{Q},\ell}(\mathrm{Fr}_p) \equiv \mathrm{tr}(\mathrm{Ind}_K^{\mathbb{Q}}\overline{\chi})(\mathrm{Fr}_p) \equiv \overline{\chi}(\mathrm{Fr}_p) + \overline{\chi}(\tau\,\mathrm{Fr}_p\,\tau^{-1}) \equiv \overline{\chi}(\pi_{v_1}) + \overline{\chi}(\pi_{v_2}) \equiv \chi(\pi_{v_1}) + \chi(\pi_{v_2}) = a_p(g) \pmod{\lambda}$. Thus, $a_p(f) \equiv a_p(g) \pmod{\lambda}$ for $p \nmid \ell M$.

***Lemma 4.2*** *Let $\ell$ be a prime which is inert in an imaginary quadratic field $K \subset \overline{\mathbb{Q}}$ with its set of embeddings denoted by $D_K = \{1, \tau\}$. Let $\overline{\chi}\colon G_K \to \mathbb{F}_{\ell^2}^{\times}$ be a character with Artin conductor $\mathfrak{m}(\overline{\chi})$ prime to $\ell$ and suppose $\overline{\rho} = \mathrm{Ind}_K^{\mathbb{Q}}\overline{\chi}$ is irreducible. If we denote by $N(\overline{\rho})$ the Artin conductor of $\overline{\rho}$, then*

$$N(\overline{\rho}) = (d_K)N_K\big(\mathfrak{m}(\overline{\chi})\big).$$

**Proof** Let $\widetilde{\chi}\colon G_K \to L^{\times} \subset \mathbb{C}^{\times}$, $L = \mathbb{Q}(\zeta_n)$, $n = \ell^2 - 1$ be the Teichmüller lift of $\overline{\chi}$, and let $\widetilde{\rho} = \mathrm{Ind}_K^{\mathbb{Q}}\widetilde{\chi}$. By [12] VI.3 Proposition 6, $N(\widetilde{\rho}) = (d_K)N_K\big(\mathfrak{m}(\widetilde{\chi})\big) = (d_K)\ell^2 N_K\mathfrak{m}(\overline{\chi})$.

Let us compare $N(\overline{\rho}) = \prod_{p \neq \ell} p^{\overline{e}_p}$ and $N(\widetilde{\rho}) = \prod_{p \neq \ell} p^{\widetilde{e}_p}$ (as $\ell \nmid N(\widetilde{\rho})$). The quantities $\overline{e}_p$ and $\widetilde{e}_p$ are defined as

$$\overline{e}_p = \sum_{i=0}^{\infty} \frac{\#\overline{\rho}(G_{p,i})}{\#\overline{\rho}(G_{p,0})}(2 - \dim \overline{\rho}^{G_{p,i}})$$

$$\widetilde{e}_p = \sum_{i=0}^{\infty} \frac{\#\widetilde{\rho}(G_{p,i})}{\#\widetilde{\rho}(G_{p,0})}(2 - \dim \widetilde{\rho}^{G_{p,i}})$$

where $G_{p,i}$ denotes the $i$-th ramification group of a decomposition group at $p$, indexed so that $G_{p,0}$ is the inertia subgroup at $p$.

Our aim is to show that $N(\overline{\rho})$ is the prime to $\ell$-part of $N(\widetilde{\rho})$ and hence equal to $N(\widetilde{\rho}) = (d_K)N_K\big(\mathfrak{m}(\overline{\chi})\big)$. It suffices from the definitions of $\overline{e}_p$ and $\widetilde{e}_p$ to show that $\dim \overline{\rho}^H = \dim \widetilde{\rho}^H$ for any given subgroup $H$ of $G_{\mathbb{Q}}$. Let $\widetilde{V} = L \oplus L\tau$ be the representation space of $\widetilde{\rho}$ and let $\Lambda = \mathcal{O}_L \oplus \mathcal{O}_L\tau$ be the natural $G_{\mathbb{Q}}$-invariant lattice lying inside $\widetilde{V}$. For any prime $\lambda$ above $\ell$ of $L$, the $\mathbb{F}_{\ell^2}$-vector space $\Lambda/\lambda\Lambda$ is isomorphic to $\overline{\rho}$.

If $H$ is a given subgroup of $G_{\mathbb{Q}}$, then we see from the description of $\overline{\rho}$ as a reduction of $\widetilde{\rho}$ that $\dim \widetilde{\rho}^H \leq \dim \overline{\rho}^H$. To show equality, we first show that given a non-zero $\overline{v} \in \overline{V}^H$ it is possible to find a lift $\widetilde{v} \in \Lambda^H$, *i.e.* $\widetilde{v} \in \Lambda^H$, $\widetilde{v} \equiv \overline{v} \pmod{\lambda\Lambda}$. To do this write $\overline{v} = \overline{x} + \overline{y}\tau$ and let $H_1 = H \cap G_K$ and $H_2 = H \cap \tau G_K$.

Suppose both $\overline{x}, \overline{y} \neq 0$. For every $h \in H_1$, $\overline{\rho}(h)(\overline{v}) = \overline{\chi}(h)\overline{x} + \overline{\chi}'(h)\overline{y}\tau = \overline{x} + \overline{y}\tau = \overline{v}$. It follows that $\overline{\chi}(h) = \overline{\chi}'(h) = 1$ for all $h \in H_1$, and hence $\widetilde{\rho}(h) = 1$ for all $h \in H_1$ so that any lift of $\overline{v}$ is invariant under $h \in H_1$. For every $h = \tau\sigma \in H_2$, $\overline{\rho}(h)(\overline{v}) = \overline{\chi}(\sigma)\overline{y} + \overline{\chi}'(\sigma)\overline{x}\tau = \overline{x} + \overline{y}\tau = \overline{v}$. Thus, $\overline{\chi}(\sigma)\overline{y} = \overline{x}$ and $\overline{\chi}'(\sigma)\overline{x} = \overline{y}$ for all $h = \tau\sigma \in H_2$. Note this implies that $\overline{\chi}(\sigma)$, $\overline{\chi}'(\sigma)$, $\widetilde{\chi}(\sigma)$, $\widetilde{\chi}'(\sigma)$ are constant as $h = \tau\sigma$ varies in $H_2$. Let $\widetilde{y} \in \mathcal{O}_L$ be any lift of $\overline{y}$. Define $\widetilde{x} = \widetilde{\chi}(\sigma)\widetilde{y}$ and $\widetilde{v} = \widetilde{x} + \widetilde{y}\tau$. Then also $\widetilde{\chi}'(\sigma)\widetilde{x} = \widetilde{y}$, and hence $\widetilde{\rho}(h)(\widetilde{v}) = \widetilde{v}$ for all $h \in H_2$.

Suppose one of $\overline{x}, \overline{y} = 0$. If there exists an element $h = \tau\sigma \in H_2$, then arguing as above, we have that $\overline{\chi}(\sigma)\overline{y} = \overline{x}$ and $\overline{\chi}'(\sigma)\overline{x} = \overline{y}$. But then implies both $\overline{x}, \overline{y} = 0$ contradicting $\overline{v} \neq 0$. Hence, we must have $H \subset G_K$. Again, arguing as above, we see there is a lift $\widetilde{v}$ of $\overline{v}$ in $\Lambda^H$.

The equality $\dim \overline{\rho}^H = \dim \widetilde{\rho}^H$ now follows by picking a lift as above for each element of a basis of $\overline{V}^H$ to form a basis for $\widetilde{V}^H$ of the same size. ∎

From the above lemma, it follows that $M = N_K(\mathfrak{m})|d_K|$ is the Artin conductor of $\overline{\rho}_{E/\mathbb{Q},\ell}$ which divides $N_E$.

## 5 Proof of Theorem 1.7

In this section, we show that the grossencharacter $\chi$ used to prove Theorem 1.6 can adjusted (in certain situations) so that it has the additional property that the character $\xi\colon (\mathbb{Z}/M\mathbb{Z})^\times \to \mathbb{C}^\times$ of the associated newform $g(z) = \sum_{\mathfrak{a} \in I(\mathfrak{m})} \chi([\mathfrak{a}])q(z)^{N_K(\mathfrak{a})}$ is trivial.

The Verlagerung map $\mathrm{Ver}\colon C_{\mathbb{Q}} \to C_K$ is defined by $\mathrm{Ver} = \prod_p \mathrm{Ver}_p$, where $\mathrm{Ver}_p$ is the natural map $\mathbb{Q}_p^\times \to (K \otimes \mathbb{Q}_p)^\times$ (here $p = \infty$ is included). By Theorem 4.1, the character $\xi$ is given by the formula $\xi = \epsilon_K \frac{\chi\circ\mathrm{Ver}}{\omega_{\mathbb{Q}}^u}$. If $\chi$ is a grossencharacter on $K$ of weight $k = a_0 + a_1\tau$ and modulus $\mathfrak{m}$, then $\chi \circ \mathrm{Ver}$ is a grossencharacter on $\mathbb{Q}$ of weight $a_0 + a_1$ and modulus $N_K(\mathfrak{m})$. Thus, the expression for $\xi$ is indeed a grossencharacter of $\mathbb{Q}$ of weight 0 and modulus $M$ and hence factors to $C_{\mathbb{Q},M} \cong (\mathbb{Z}/M\mathbb{Z})^\times$.

***Proposition 5.1*** *Let $H \subset G$ be finite abelian groups. Let $v$ be the unique valuation of $\overline{\mathbb{Q}}_\ell$ extending that of $\mathbb{Q}_\ell$. Suppose $f\colon H \to \overline{\mathbb{Q}_\ell}^\times$ is a character such that such that $v\big(f(h) - 1\big) > 0$ for all $h \in H$. Then there exists a character $f'\colon G \to \overline{\mathbb{Q}_\ell}^\times$ extending $f$ such that $v\big(f'(g) - 1\big) > 0$ for all $g \in G$.*

**Proof** The main idea of the proof is to mimic the proof of Baer's criterion (*cf.* [3]). We shall write the abelian groups $H \subset G$ additively. The first step is to show the following intermediate result.

Let $f\colon m\mathbb{Z} \to \overline{\mathbb{Q}_\ell}^\times$ be a homomorphism such that $f(m)$ is a root of unity and $v\big(f(m) - 1\big) > 0$. Then there exists a homomorphism $\overline{f}\colon \mathbb{Z} \to \overline{\mathbb{Q}_\ell}^\times$ extending $f$ such that $\overline{f}(1)$ is a root of unity and $v\big(\overline{f}(1) - 1\big) > 0$. To show that $\overline{f}$ exists, choose a root of unity $x \in \overline{\mathbb{Q}_\ell}^x$ such that $x^m = f(m)$. Let $L = \mathbb{Q}_\ell(x)$, with $\lambda|\ell$ the unique primes of $L$, $\mathbb{Q}_\ell$ corresponding to the restrictions of $v$ to these fields. Let $\bar{x}$ be the reduction of $x$ modulo $\lambda$ and let $\widetilde{x}$ denote the Teichmüller lift of this reduction to $\overline{\mathbb{Q}_\ell}^\times$. Since $x^m = f(m) \equiv 1 \pmod{\lambda}$, we see that $\widetilde{x}^m = 1$, so $\widetilde{x}$ is an $m$-th root of unity in $\overline{\mathbb{Q}}_\ell$. Now, $(x/\widetilde{x})^m$ is also equal to $f(m)$ but $x/\widetilde{x}$ is congruent to 1 modulo $\lambda$. We define $\overline{f}$ by $\overline{f}(1) = x/\widetilde{x}$.

Let $f\colon H \to \overline{\mathbb{Q}_\ell}^\times$ be given such that $v\big(f(h) - 1\big) > 0$ for all $h \in H$. There exists a maximal extension $\overline{f}\colon \overline{H} \to \overline{\mathbb{Q}_\ell}^\times$ extending $f\colon H \to \overline{\mathbb{Q}_\ell}^\times$ such that $v\big(\overline{f}(\overline{h}) - 1\big) > 0$ for all $\overline{h} \in \overline{H}$. If $\overline{H} = G$, then we are done. If $\overline{H}$ is strictly contained in $G$, then let $a \in G$ such that $a \notin \overline{H}$. Consider the ideal $\mathfrak{a} = \{r \in \mathbb{Z} : ra \in \overline{H}\}$ of $\mathbb{Z}$. We define a homomorphism $f_0\colon \mathfrak{a} \to \overline{\mathbb{Q}_\ell}^\times$ by $f_0(r) = \overline{f}(ra)$. By the intermediate result above, there is an extension $\overline{f}_0\colon \mathbb{Z} \to \overline{\mathbb{Q}_\ell}^\times$ such that $v\big(\overline{f}_0(1) - 1\big) > 0$. Let $u = \overline{f}_0(1)$. We now define $f'(x + ra) = \overline{f}(x) \cdot u^r$, where $x \in \overline{H}$, and $r \in \mathbb{Z}$. This is well-defined since if $x + ra = 0$, then $r \in \mathfrak{a}$, and hence $\overline{f}(x) \cdot u^r = \overline{f}(x) \cdot \overline{f}(ra) = \overline{f}(x + ra) = 0$. Now, $f'$ extends $\overline{f}$ to $H' = \langle \overline{H}, a\rangle$ still keeping the property $v\big(f'(h') - 1\big) > 0$ for all $h' \in H'$, contradicting the maximality of $\overline{f}$. ∎

Let $\overline{\mathrm{Ver}}\colon C_{\mathbb{Q},M} \to C_{K,\mathfrak{m}}$ be the homomorphism induced by Ver on ray class groups.

***Corollary 5.2*** *Let $\xi\colon C_{\mathbb{Q},M} \to \mathbb{C}^\times$ be a character such that $\xi$ is trivial on the kernel of $\overline{\mathrm{Ver}}$ and $\xi \equiv 1 \pmod{\lambda}$ for $\lambda$ a prime above $\ell$ of the field generated by $\xi$. Then there exists a character $\psi\colon C_{\mathbb{Q},\mathfrak{m}} \to \mathbb{C}^\times$ such that $\psi \circ \overline{\mathrm{Ver}} = \xi$ and $\psi \equiv 1 \pmod{\lambda}$.*

Let $\chi$ be as in the proof of Theorem 1.6 and let $\xi = \epsilon_K \frac{\chi\circ\mathrm{Ver}}{\omega_{\mathbb{Q}}}$. Assume $\xi^{-1}$ satisfies the requirements of the corollary above and let $\psi$ be the character extending the character $\xi^{-1}$ from the corollary. The character $\chi' = \chi\psi$ also satisfies the requirements

https://doi.org/10.4153/CMB-2002-036-3 Published online by Cambridge University Press

for Theorem 1.6, but now the character of the associated newform $g'$ becomes

$$\xi' = \epsilon_K \frac{\chi\psi \circ \mathrm{Ver}}{\omega_{\mathbb{Q}}} = \epsilon_K \frac{\chi \circ \mathrm{Ver}}{\omega_{\mathbb{Q}}} \psi \circ \mathrm{Ver} = \xi\xi^{-1} = 1.$$

Since $\overline{\rho}_{f,\ell} \cong \overline{\rho}_{g,\lambda} \pmod{\lambda}$, it follows that $\xi \equiv 1 \pmod{\lambda}$ as the character of $f$ is trivial. Thus, to prove Theorem 1.7, we need only verify that $\xi$ is trivial on the kernel of $\overline{\mathrm{Ver}}$.

Let $\pi_N \colon C_{\mathbb{Q}} \to C_{\mathbb{Q},M}$ denote the quotient map. Let $x \in C_{\mathbb{Q}}$ such that $\overline{\mathrm{Ver}}\big(\pi_N(x)\big) = 1$. This means that $\mathrm{Ver}(x) = u \cdot k \in U_{K,\mathfrak{m}} \cdot K^{\times}$. Now, $\chi(u \cdot k) = \chi(u) = \chi_\infty(u_\infty) = u_\infty$. On the other hand, $\omega_{\mathbb{Q}} = \omega_K^{1/2}$ and $\omega_K(u \cdot k) = \omega_{\mathbb{Q}}(u) = \omega_{K,\infty}(u_\infty) = u_\infty^2$. Hence, $\frac{\chi \circ \mathrm{Ver}}{\omega_{\mathbb{Q}}}$ considered as a character of $C_{\mathbb{Q},M}$ is trivial on the kernel of $\overline{\mathrm{Ver}}$.

Thus, it remains to show that $\epsilon_K$ is trivial on the kernel of $\overline{\mathrm{Ver}}$. The class group $C_{\mathbb{Q},M} \cong (\mathbb{Z}/M\mathbb{Z})^{\times}$. Given an element $g \in C_{\mathbb{Q},M}$, there exist infinitely many primes $q$ such that $\overline{q} = g \pmod{M}$ by the Cheboterov density theorem. The character $\epsilon_K$ considered as a character of $C_{\mathbb{Q},M}$ can then be described by $q \mapsto (\frac{d_K}{q})$. Let $g \in C_{\mathbb{Q},M}$ be such that $\overline{\mathrm{Ver}}(g) = 1$ and let us represent $g = \overline{q}$ for an odd prime $q$. The property $\overline{\mathrm{Ver}}(\overline{q}) = 1$ implies that $q \equiv 1 \pmod{p}$ for every prime $p | N_K(\mathfrak{m})$.

Assume now that $2 \nmid d_K$ so that $d_K \equiv 1 \pmod{4}$ is square-free. From [13] Section 5.8, we deduce that

1. The character $\epsilon_K = \epsilon_{E/\mathbb{Q},\ell}$ is unramified outside $p | N_E$ because of the condition $3 < \ell \nmid N_E$.
2. Furthermore, if $p \nmid d_K$, then $p^2 | N_E$.

Thus, since $d_K$ is square-free, it follows that if $p | d_K$, then $p | N_E / d_K$. But then $p | N_K(\mathfrak{m})$ as only semi-stable primes can be stripped from $N_E$ (*cf.* [14] Section 4.6). Thus, we have

$$\epsilon_K(q) = \left(\frac{d_K}{q}\right) = (-1)^{\frac{q-1}{2}\frac{d_K-1}{2}} \left(\frac{q}{d_K}\right) = 1$$

as $d_K \equiv 1 \pmod{4}$ and $q \equiv 1 \pmod{p}$ for each $p | N_K(\mathfrak{m})$. Given the following lemma, Theorem 1.7 is now proved.

***Lemma 5.3*** *Let $E/\mathbb{Q}$ be an elliptic curve with conductor $N_E$ and suppose* $\mathrm{im}(\overline{\rho}_{E/\mathbb{Q},\ell}) \subset$ *$N'$ for $\ell$ odd. Let $K$ be the imaginary quadratic field associated to such $\overline{\rho}_{E/\mathbb{Q},\ell}$. If $16 \nmid N_E$ then $2 \nmid d_K$.*

**Proof** Let $\Phi_2 = \overline{\rho}_{E/\mathbb{Q},\ell}(I_2)$ be the image of inertia at 2. Then $\Phi_2$ can be considered as a subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$ with order restricted to 1, 2, 3, 4, 6, 8, 24 [13]. If $\#\Phi_2 = 1, 2, 3, 6$, then under the assumption $\ell$ odd, we have that $2 \nmid d_K$ by [13] Section 5.8. In fact, if $\#\Phi_2 = 24$, then $2 \nmid d_K$ as $\mathrm{SL}_2(\mathbb{F}_3)$ cannot be embedded into the normalizer of a non-split Cartan subgroup $N'$.

If $\#\Phi_2 = 4$ and $2 | d_K$ then $\#\overline{\rho}_{E/\mathbb{Q},\ell}(G_{2,0}) = \#\overline{\rho}_{E/\mathbb{Q},\ell}(G_{2,1}) = 4$ which implies the Artin exponent $\overline{e}_p$ of $\overline{\rho}_{E/\mathbb{Q},\ell}$ is $\geq 4$. Similarly, if $\#\Phi_2 = 8$, then also $e_p \geq 4$. ■

## 6 Conclusions

It is known that $S_{\mathbb{Q}}^{N'}$ contains the primes 2, 3, 5, 7, 11. For instance, the modular curves $X(\ell)/N'$ (which classify up to twist those $E/\mathbb{Q}$ with $\ell \in S_{E/\mathbb{Q}}^{N'}$) are isomorphic to $\mathbb{P}^1/\mathbb{Q}$ in the cases $\ell = 3, 5, 7$. It is possible to give explicit equations for such elliptic curves [2]. On the other hand, $X(11)/N'$ is the elliptic curve $121D$ which has rank 1 so there are infinitely-many $E/\mathbb{Q}$ (non-isomorphic over $\overline{\mathbb{Q}}$) with $11 \in S_{E/\mathbb{Q}}^{N'}$. Explicit examples of such elliptic curves seem to be unknown however.

A naive search among elliptic curves $E/\mathbb{Q}$ with integral $j$-invariant having absolute value less than 800, 000 only give rise to the primes 2, 3, 5 in $S_{\mathbb{Q}}^{N'} \cup S_{\mathbb{Q}}^{N}$. It would be interesting to gather further computational data regarding the sets $S_{\mathbb{Q}}^{N}$ and $S_{\mathbb{Q}}^{N'}$ especially in relation to congruence primes. For instance, the following is an example illustrating the theorems shown in this paper.

Consider the elliptic curve $4176N = E/\mathbb{Q} : y^2 = x^3 - 3105x + 139239$ from Cremona's tables [4]. Its discriminant, $j$-invariant, and conductor are $\Delta = -2^4 3^9 29^5$, $j = -10512288000/20511149 = 2^8 3^3 5^3 23^3/29^5$, and $N = 4176 = 2^4 3^2 29$, respectively. Because the $j$-invariant is of the form $125\frac{t(2t+1)^3(2t^2+7t+8)^3}{(t^2+t-1)^5}$ for $t = -4/5$, the explicit parametrization of $X(5)/N'$ in [2] implies that $5 \in S_{E/\mathbb{Q}}^{N'}$. Since $E/\mathbb{Q}$ is semistable at 29 and the exponent of 29 in $\Delta$ is divisible by 5, by Ribet's theorem [11], $\overline{\rho}_\ell$ is modular of level $144 = 2^4 3^2$. Indeed, there is a newform $g$ at level 144 which is congruent modulo 5 to the newform $f$ at level $4176 = 144 \cdot 29$ attached to $E/\mathbb{Q}$. The first few fourier coefficients $a_p$ for $p$ prime are given below (for $p$ dividing the level, the signs of the action of the Atkin-Lehner involution $W_p$ are given).

$$a_p(g) = [-, +, 0, 4, 0, 2, 0, -8, 0, 0, 4, -10, 0, -8, 0, 0, \dots$$
$$a_p(f) = [-, +, 0, -1, -5, -3, 5, 2, 0, +, -6, 10, 10, 2, \dots$$

The newform $g$ corresponds to the isogeny class of elliptic curves $144A$ which have complex multiplication by $\sqrt{-3}$, so $g$ is induced from a grossencharacter on the imaginary quadratic field $\mathbb{Q}(\sqrt{-3})$.

## 7 Acknowledgements

I would like to thank CICMA, MPIM, and MSRI for their support and hospitality during my stay there 1998–99, January–August 2000, and October–December 2000 respectively.

## References

[1] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over Q: wild 3-adic exercises.* J. Amer. Math. Soc., to appear.

[2] I. Chen, *On Siegel's modular curve of level* 5 *and the class number one problem.* J. Number Theory (2) **74**(1999).

[3] P. M. Cohn, *Algebra, Volume 2.* John Wiley & Sons, second edition, 1982.

[4] J. E. Cremona, *Algorithms for modular elliptic curves.* Cambridge University Press, second edition, 1997.

[5] A. Kraus, *Une remarque sur les points de torsion des courbes elliptiques*. C. R. Acad. Sci. Paris Série I Math. **321**(1995), 1143–1146.
[6] B. Mazur, *Rational isogenies of prime degree*. Invent. Math. **44**(1978), 129–162.
[7] T. Miyake, *Modular Forms*. Springer-Verlag, 1989.
[8] F. Momose, *Galois action on some ideal section points of the abelian variety associated with a modular form and its application*. Nagoya Math. J. **91**(1983), 19–36.
[9] ______, *Rational points on the modular curves* $X_{\mathrm{split}}(p)$. Compositio Math. **52**(1984), 115–137.
[10] K. Ribet, *On* $\ell$*-adic representations attached to modular forms*. Invent. Math. **28**(1975), 245–275.
[11] ______, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ *arising from modular forms*. Invent. Math. **100**(1990), 431–476.
[12] J. P. Serre, *Corps locaux*. Number VIII in Publications de l'Université de Nancago, Hermann, Paris, deuxième edition, 1968.
[13] ______, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15**(1972), 259–331.
[14] ______, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Duke Math. J. (1) **54**(1987), 179–230.
[15] A. Weil, *On a certain type of characters of the idèle-class groups of an algebraic number-field*. In: Proceedings of the international symposium of algebraic number theory, Tokyo & Nikko, 1955, Tokyo, 1956, Science Council of Japan, 1–7.

*Max Planck Institut für Mathematik*
*Vivatsgasse 7, P.O. Box 7280*
*D-53072 Bonn,*
*Germany*
*e-mail: chen@mpim-bonn.mpg.de*

https://doi.org/10.4153/CMB-2002-036-3 Published online by Cambridge University Press