Canad. Math. Bull. Vol. **48** (1), 2005 pp. 16–31

# On the Surjectivity of the Galois Representations Associated to Non-CM Elliptic Curves

Alina Carmen Cojocaru

*with an Appendix by Ernst Kani*

*Abstract.* Let $E$ be an elliptic curve defined over $\mathbb{Q}$, of conductor $N$ and without complex multiplication. For any positive integer $l$, let $\phi_l$ be the Galois representation associated to the $l$-division points of $E$. From a celebrated 1972 result of Serre we know that $\phi_l$ is surjective for any sufficiently large prime $l$. In this paper we find conditional and unconditional upper bounds in terms of $N$ for the primes $l$ for which $\phi_l$ is *not* surjective.

## 1 Introduction

Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. For primes $p$ of good reduction for $E$, that is, primes $p \nmid N$, let $E_p$ be the reduction of $E$ modulo $p$ and write

$$|E_p(\mathbb{F}_p)| = p + 1 - a_p$$

for the number of $\mathbb{F}_p$-rational points of $E_p$. We know from Hasse's inequality that

$$|a_p| \leq 2\sqrt{p}. \tag{1}$$

For a positive integer $k$, let $E[k]$ denote the group of complex points on $E$ whose order divides $k$, called *the group of $k$-division points of $E$*, and let $L_k = \mathbb{Q}(E[k])$ be the field obtained by adjoining to $\mathbb{Q}$ the $x$- and $y$-coordinates of the points in $E[k]$, called *the $k$-division field of $E$*. We know that $E[k]$ is isomorphic to $\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ and that $L_k/\mathbb{Q}$ is a finite Galois extension which is unramified outside $kN$ (see [Si86]).

There has been great interest in determining the size of the degree $[L_k : \mathbb{Q}]$ of the extensions $L_k/\mathbb{Q}$. For example, this problem has applications in the study of certain diophantine equations (see [Mer]) or in the study of the curve $E_p$ as $p$ varies (see [Co]).

A natural way of finding upper bounds for $[L_k : \mathbb{Q}]$ is by observing that the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$, acts on the $k$-division points $E[k]$ for any $k$. This allows us to define a representation

$$\phi_k \colon \mathrm{Gal}(L_k/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z}),$$

Received by the editors March 11, 2003.
AMS subject classification: Primary 11G05; secondary 11N36, 11R45.

called *the Galois representation associated to* $E[k]$. It is easy to see that $\phi_k$ is injective. Therefore for any $k$ we have

$$[L_k : \mathbb{Q}] \leq |\operatorname{GL}_2(\mathbb{Z}/k\mathbb{Z})| = k^4 \prod_{\substack{l|k \\ l \text{ prime}}} \left(1 - l^{-2}\right)\left(1 - l^{-4}\right).$$

Determining the size of the image of $\phi_k$ is a much more challenging question. By classical results in the theory of complex multiplication, we know that if $E$ has complex multiplication (denoted CM), then

$$\phi(k)^2 \ll [L_k : \mathbb{Q}] \ll k^2$$

for any $k > 2$, where $\phi(\,\cdot\,)$ denotes the Euler function. Thus $\phi_k$ cannot be surjective in this case. In big contrast, if $E$ does not have complex multiplication (denoted non-CM), a celebrated result of J.-P. Serre [Se72] asserts that there exists a finite set of primes $S_E$ such that $\phi_l$ is surjective for any prime $l \notin S_E$. Moreover, if we define

$$A(E) := 2 \cdot 3 \cdot 5 \cdot \prod_{l \in S_E} l,$$

we can deduce that $\phi_k$ is surjective for any positive integer $k$ coprime to $A(E)$ (see the Appendix of this paper). We will refer to $A(E)$ as *Serre's constant associated to* $E$.

Now a natural question to ask is how large the prime divisors of $A(E)$ can be. In his 1972 paper, and also later in a 1981 paper, J.-P. Serre asked if $A(E)$ is an absolute constant for any non-CM elliptic curve $E$ defined over $\mathbb{Q}$ (see [Se72, p. 299] and [Se81, p. 199]). In 1978 [Maz], B. Mazur showed that $A(E)$ is indeed an absolute constant if $E$ is a semistable elliptic curve, that is, if the conductor $N$ of $E$ is square-free.

In this paper we consider the more modest problem of finding upper bounds for the prime divisors of $A(E)$ in terms of the conductor $N$ of $E$.

One approach to this problem was initiated by J.-P. Serre in 1981; we recall it in what follows. In [Se81, p. 197] Serre showed that if $l$ is a prime and if we let $G_l$ denote the image of $\phi_l$ in $\operatorname{GL}_2(\mathbb{Z}/l\mathbb{Z})$ and $PG_l$ the image of $G_l$ in the projective group $\operatorname{PGL}_2(\mathbb{Z}/l\mathbb{Z}) := \operatorname{GL}_2(\mathbb{Z}/l\mathbb{Z})/(\mathbb{Z}/l\mathbb{Z})^*$, then, in order to prove that $G_l = \operatorname{GL}_2(\mathbb{Z}/l\mathbb{Z})$, it suffices to show that:

- $PG_l$ is not contained in a Borel subgroup of $\operatorname{PGL}_2(\mathbb{Z}/l\mathbb{Z})$;
- $PG_l$ is not contained in a non-split Cartan subgroup of $\operatorname{PGL}_2(\mathbb{Z}/l\mathbb{Z})$;
- $PG_l$ is not isomorphic to the permutation groups $A_4, S_4$ or $A_5$;
- $PG_l$ is not contained in the normalizer $\mathcal{N}_l$ of a Cartan subgroup $C_l$ of $\operatorname{PGL}_2(\mathbb{Z}/l\mathbb{Z})$ such that $PG_l \nsubseteq C_l$.

(For the definitions of the Borel and Cartan subgroups of $\operatorname{PGL}_2(\mathbb{Z}/l\mathbb{Z})$ the reader may consult [Se72, Section 2, p. 278] or [La, Sections 1–2 of Ch. XI]). Serre showed that the first three situations above hold if $l \geq 19$ and $l \neq 37$ (see [Se81, Lemmas 16–18]). If there exists a Cartan subgroup $C_l$ of $\operatorname{PGL}_2(\mathbb{Z}/l\mathbb{Z})$ such that $PG_l$ is contained in the

normalizer $\mathcal{N}_l$ of $C_l$ in $\mathrm{PGL}_2(\mathbb{Z}/l\mathbb{Z})$ and is not contained in $C_l$, then we identify $\mathcal{N}_l/C_l$ with the group $\{\pm 1\}$ and we let $\epsilon_l$ be the composition

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow G_l \longrightarrow \frac{\mathcal{N}_l}{C_l} \longrightarrow \{\pm 1\}.$$

We see that $\epsilon_l$ is a quadratic character of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$, which we identify with a Dirichlet character. Serre [Se72, p. 317] showed that

(2) $\epsilon_l$ is unramified at the primes $p$ which do not divide $N$,

and

(3) $a_p \equiv 0 (\mathrm{mod}\, l)$ for any prime $p \nmid N$ such that $\epsilon_l(p) = -1$.

In other words, if $l$ is a prime divisor of $A(E)$, then either $l \mid 37 \prod_{q \leq 19, q \text{ prime}} q$ or (3) holds.

Now let $p_0$ be the smallest prime $p$ of good reduction for $E$ such that $\epsilon_l(p) = -1$ and $a_p \neq 0$. Serre proved that if we assume GRH for the Dedekind zeta functions of the division fields of $E$, there exists a positive absolute constant $c_0$ such that

(4) $$p_0 \leq c_0 (\log N)^2 (\log\log(2N))^6$$

(see [Se81, proof of Lemma 19]). By (1) and (4) we then get the estimate

$$\begin{aligned} A(E) &\leq 37 \Bigg( \prod_{\substack{q \leq 19 \\ q \text{ prime}}} q \Bigg) \prod_{\substack{l \mid a_{p_0} \\ 1 \text{ prime} \\ (l, 37 \prod_{q \leq 19} q) = 1}} l \\ &\leq 37 \Bigg( \prod_{\substack{q \leq 19 \\ q \text{ prime}}} q \Bigg) |a_{p_0}| \leq c_1 (\log N)(\log\log(2N))^3 \end{aligned}$$

for some positive absolute constant $c_1$. We record this result as:

***Theorem 1*** *Let $E$ be a non-CM elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $A(E)$ be Serre's constant associated to $E$. If we assume GRH for the Dedekind zeta functions of the division fields of $E$, there exists a positive absolute constant $c_1$ such that*

$$A(E) \leq c_1 (\log N)(\log\log(2N))^3.$$

Another approach to the problem of finding upper bounds for the prime divisors of $A(E)$ is due to D. W. Masser and G. Wüstholz (see [MaWü, p. 247]) who showed that there exist absolute positive constants $c_2$ and $\gamma$, with $\gamma$ effective, such that $\phi_l$ is surjective for any prime $l$ satisfying

(5) $$l > c_2 \, \mathrm{h}(E)^{\gamma},$$

where $h(E)$ denotes the Faltings height of $E$ (for a definition, we refer the reader to [Si84, p. 254]). We will refer to $\gamma$ as *the Masser-Wüstholz constant*.

In this paper we will first derive an unconditional upper bound for $A(E)$. After obtaining this estimate, we discovered that A. Kraus had already obtained a similar result a few years earlier (see [Kr]). The proof we give is conceptually the same as the one by Kraus but much simpler in that it is essentially self-contained; for example, Kraus uses certain theorems of Deligne [De] without proof. We will also derive a conditional upper bound for the prime divisors of $A(E)$ based on a different hypothesis than GRH.

Before stating the precise results that we are proving in this paper, let us point out that one of the key facts used in our proofs is the modularity of elliptic curves defined over $\mathbb{Q}$, a long-standing conjecture formulated by Shimura and Taniyama, eventually proven by Wiles, Taylor, and Wiles and Breuil, Conrad, Diamond, and Taylor. One formulation of this conjecture is that for any elliptic curve $E$ defined over $\mathbb{Q}$ and of conductor $N$, there exists a non-trivial surjective morphism

$$\phi\colon X_0(N) \longrightarrow E,$$

defined over $\mathbb{Q}$, called *a modular parametrization of E*. Here $X_0(N)$ is the modular curve obtained by the action of the complex upper-half plane on the matrix subgroup of $\mathrm{SL}_2(\mathbb{Z})$ composed of elements whose left lower entry is 0 modulo $N$.

The main results of our paper are as follows.

***Theorem 2*** *Let $E$ be a non-CM elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Then, for any prime $l$ satisfying the inequality*

$$l \geq \frac{4\sqrt{6}}{3} N \prod_{\substack{p|N \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right)^{1/2} + 1,$$

*the Galois representation $\phi_l$ associated to $E$ is surjective. Moreover,*

$$A(E) \ll N(\log\log N)^{1/2},$$

*where the implied $\ll$-constant is absolute.*

***Theorem 3*** *Let $E$ be a non-CM elliptic curve defined over $\mathbb{Q}$ and of conductor $N$. Let $\phi$ be a modular parametrization for $E$ of minimal degree $\deg\phi$. Assuming the degree conjecture for $\phi$, that is, assuming that for any $\varepsilon > 0$,*

$$\deg\phi = \mathrm{O}_\varepsilon\left(N^{2+\varepsilon}\right),$$

*there exists an absolute positive constant $c_3$ such that, for any prime $l$ satisfying the inequality*

$$l \geq c_3(\log N)^\gamma,$$

*with $\gamma$ denoting the Masser-Wüstholz constant, the Galois representation $\phi_l$ associated to $E$ is surjective.*

## 2 Preliminaries

In this section we review the properties of modular forms that will be needed for proving the two results of the paper. For more details we refer the reader to [La].

Let $k, N$ be positive integers and let

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 (\mathrm{mod}\, N) \right\}.$$

Also, let $\mathrm{M}_k(\Gamma_0(N))$ and $\mathrm{S}_k(\Gamma_0(N))$ be the complex vector spaces of modular forms and cusp forms of weight $k$ on $\Gamma_0(N)$, respectively.

On the space $\mathrm{S}_k(\Gamma_0(N))$ we can define an inner product, called *the Petersson inner product*. We can also define certain linear transformations on $\mathrm{M}_k(\Gamma_0(N))$ and $\mathrm{S}_k(\Gamma_0(N))$, called *Hecke operators*. A cusp form $f$ which is an eigenform for all the Hecke operators is called *an eigenform*; if its first Fourier coefficient $a_1(f)$ is 1, then it is called a *normalized* form. A nice property of an eigenform $f$ is that its Fourier coefficients $a_n(f)$ are multiplicative in $n$. Moreover, for any prime $q \nmid N$ and any positive integer $t$, the Fourier coefficients $a_{q^t}(f)$ satisfy the recurrence relations

$$a_{q^t}(f)a_q(f) = a_{q^{t+1}}(f) + q^{k-1}a_{q^{t-1}}. \tag{6}$$

A natural question to ask is: when are two modular forms equal? We have the following answer:

***Proposition 2.1*** *Let $f$ and $f'$ be two distinct modular forms of weight $k$ and levels $N$ and $N'$, respectively. Let $M := \mathrm{lcm}(N, N')$. Then there exists a positive integer $n$ such that*

$$n \leq \frac{k}{12} M \prod_{\substack{p \mid M \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right) + 1$$

*and*

$$a_n(f) \neq a_n(f'),$$

*where $a_n(f)$ and $a_n(f')$ are the $n$-th Fourier coefficients of $f$ and $f'$.*

**Proof** The following argument was given in [RM97]. We consider the function

$$\phi := \frac{(f - f')^{12}}{\Delta^k},$$

where $\Delta$ is the classical delta function defined by

$$\Delta(z) := e^{2\pi i z} \prod_{n=1}^{\infty} \left(1 - e^{2\pi i n z}\right)^{24}.$$

We recall that $\Delta$ is a cusp form of weight 12 on $\mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(1)$, which is nonzero on the complex upper-half plane and has a simple zero at infinity. Then $\phi$ is a meromorphic function on $X_0(M)$, for which we have

$$\begin{aligned} 12m_0 - k \leq & \text{ number of zeroes of } \phi \\ = & \text{ number of poles of } \phi \\ \leq & k([\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(M)] - 1) \\ = & k\Big(M \prod_{\substack{p|M \\ p \text{ prime}}} \Big(1 + \frac{1}{p}\Big) - 1\Big), \end{aligned}$$

with $m_0$ denoting the order of the zero at infinity of $f - f'$. Thus

$$m_0 \leq \frac{k}{12} M \prod_{\substack{p|M \\ p \text{ prime}}} \Big(1 + \frac{1}{p}\Big).$$

This completes the proof of the proposition. ∎

Another natural question to ask is how to generate new modular forms from a given modular form. One way of answering this question is to associate to a given $f \in \mathrm{M}_k(\Gamma_0(N))$ and a primitive Dirichlet character $\chi$ a function $\tilde{f}$ defined by

$$\tilde{f}(z) := \sum_{n=0}^{\infty} \chi(n) a_n(f) e^{2\pi i n z},$$

called *the twist of $f$ by $\chi$*, where

$$f(z) = \sum_{n=0}^{\infty} a_n(f) e^{2\pi i n z}$$

is the Fourier expansion of $f$. We have the following useful properties (for a proof, see [Iw, p. 124]):

***Proposition 2.2*** *The twist $\tilde{f}$ of a modular form $f \in \mathrm{M}_k(\Gamma_0(N))$ by a quadratic character $\chi$ of conductor $r$ is a modular form in $\mathrm{M}_k(\Gamma_0(M))$, where $M = \mathrm{lcm}(N, r^2)$. Moreover, if $f$ is a cusp form, so is $\tilde{f}$.*

We can also generate new modular forms by remarking that if $N'|N$, then a cusp form $f \in \mathrm{S}_k(\Gamma_0(N'))$ can be viewed as an element of $\mathrm{S}_k(\Gamma_0(N))$. More generally, if $\delta | \frac{N}{N'}$, we have that $f(\delta z) \in S_k(\Gamma_0(N))$. The $\mathbb{C}$-span of

$$\bigcup_{\substack{N'|N \\ N' \neq N}} \bigcup_{\delta | \frac{N}{N'}} \{f(\delta z) : f \in S_k(\Gamma_0(N'))\}$$

is called the space of *oldforms* on $\Gamma_0(N)$. The eigenforms in the orthogonal complement (under the Petersson inner product) of the space of oldforms in $S_k(\Gamma_0(N))$ are called *newforms*.

We conclude our review with a few words on the modularity of the elliptic curves defined over $\mathbb{Q}$. The famous Shimura-Taniyama conjecture, now known to be true (see [BCDT]), gives a one-to-one correspondence between isogeny classes of elliptic curves defined over $\mathbb{Q}$ and of conductor $N$, and normalized newforms in $S_2(\Gamma_0(N))$ with integer Fourier coefficients. An equivalent formulation is as follows:

***Theorem 2.3*** (Shimura-Taniyama Conjecture) *For every elliptic curve $E$ defined over $\mathbb{Q}$ and of conductor $N$ there exists a surjective non-trivial morphism $\phi\colon X_0(N) \longrightarrow E$, defined over $\mathbb{Q}$.*

Regarding the size of the degree of $\phi$ we have the following conjecture, unsolved for the moment, formulated by G. Frey:

***Conjecture 2.4*** (Degree Conjecture) *Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and of conductor $N$, and let $\phi$ be a modular parametrization of $E$ of minimal degree. Then, for any $\varepsilon > 0$, we have* $\deg \phi = O_\varepsilon\left(N^{2+\varepsilon}\right)$. *Here, the $O_\varepsilon$-constant depends only on $\varepsilon$.*

## 3 Proof of Theorem 2

As mentioned in the Introduction, Serre showed that if $l$ is a prime such that $l \geq 19$ and $l \neq 37$, then $PG_l$ cannot be contained in a Borel subgroup or a Cartan subgroup of $\mathrm{PGL}_2(\mathbb{Z}/l\mathbb{Z})$, nor can it be isomorphic to the permutation groups $A_4, S_4$ or $A_5$. In what follows we will show that if

$$l \geq \frac{4\sqrt{6}}{3} N \prod_{\substack{p|N \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right)^{1/2} + 1,$$

then $PG_l$ cannot be contained in the normalizer of a Cartan subgroup $C_l$ of $\mathrm{PGL}_2(\mathbb{Z}/l\mathbb{Z})$ such that $PG_l \nsubseteq C_l$. This will imply that $\phi_l$ is surjective.

Let us suppose that there exists a Cartan subgroup $C_l$ of $\mathrm{PGL}_2(\mathbb{Z}/l\mathbb{Z})$ such that $PG_l$ is contained in the normalizer $\mathcal{N}_l$ of $C_l$ in $\mathrm{PGL}_2(\mathbb{Z}/l\mathbb{Z})$ and is not contained in $C_l$. As explained in the Introduction, this implies the existence of a Dirichlet quadratic character $\epsilon_l$ satisfying (2) and (3). We also note that since $\epsilon_l$ is a quadratic character, property (2) implies that the conductor $D$ of $\epsilon_l$ is of the form $D_0$ or $4D_0$ for some square-free integer $D_0$ such that $D_0|N$.

We follow Serre's idea of estimating $l$, that is, we first look for a prime $q$ of good reduction for $E$ for which $a_q \neq 0$ and $\epsilon_l(q) = -1$, and then we look for a non-trivial upper bound for $q$. By (3) and Hasse's bound (1) we obtain that $l \leq 2\sqrt{q}$. Hence the upper bound for $q$ will give us an upper bound for $l$.

Let $E'$ be the elliptic curve defined over $\mathbb{Q}$ and obtained by taking the twist of $E$ with respect to $\epsilon_l$. We denote its conductor by $N'$. Let $f$ and $f'$ be the weight 2 normalized newforms with integer Fourier coefficients, of levels $N$ and $N'$, respectively,

associated to $E$ and $E'$ via the Shimura-Taniyama Conjecture. Proposition 2.2 gives us that $N' | \operatorname{lcm}(N, D^2)$. Thus the primes of bad reduction for $E'$ are divisors of $2N$, and so

$$a'_p = \epsilon_l(p) a_p \text{ for any prime } p \nmid 2N, \tag{7}$$

where $p + 1 - a'_p$ denotes the number of $\mathbb{F}_p$-rational points of the reduction of $E'$ modulo $p$.

We want to prove that there exists a prime $q$ which does not divide $N$ and which satisfies

$$a_q \neq a'_q, \tag{8}$$

$$\epsilon_l(q) = -1, \tag{9}$$

$$q \leq \frac{8}{3} N^2 \prod_{\substack{p|N \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right) + 1. \tag{10}$$

To do this, we first observe that $f \neq f'$, since $E$ is a non-CM elliptic curve. Indeed, if we assume that $f = f'$, then by the definition of $f'$ we must have $a_p = 0$ for any prime $p$ such that $\epsilon_l(p) = -1$. But, on one hand, by Dirichlet's theorem, the number of primes $p \leq x$ for which $\epsilon_l(p) = -1$ is asymptotically equal to $\frac{x}{2 \log x}$. On the other hand, the number of primes $p \leq x$ for which $a_p = 0$ is, in the case of a non-CM elliptic curve, $o(\frac{x}{\log x})$ (see [Se81, Corollary 2]). Thus we are led to a contradiction.

Now we twist $f$ and $f'$ by a quadratic character which is zero only at the primes dividing $N$, and obtain cusp forms

$$\tilde{f}, \tilde{f}' \in S_2(\Gamma_0(M))$$

with $M | 16N^2$ (see Proposition 2.2) and such that $\tilde{f}, \tilde{f}'$ vanish at all the primes of bad reduction for $E$. By the same argument as the one used for showing that $f \neq f'$, we have $\tilde{f} \neq \tilde{f}'$. By Proposition 2.1 this last assertion implies that there exists a positive integer $n$ such that

$$n \leq \frac{1}{6} M \prod_{\substack{p|M \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right) + 1 \tag{11}$$

and

$$a_n(\tilde{f}) \neq a_n(\tilde{f}'), \tag{12}$$

where $a_n(\tilde{f})$ and $a_n(\tilde{f})$ are the $n$-th Fourier coefficients of $\tilde{f}$ and $\tilde{f}'$, respectively. In particular, (12) tells us that we must have $(n, N) = 1$.

Using (11) and that $\tilde{f}$ and $\tilde{f}'$ are twists of $f$ and $f'$ by a quadratic character vanishing at the primes of bad reduction for $E$, we obtain that

$$a_n(f) \neq a_n(f')$$

for some

$$n \leq \frac{1}{6}M \prod_{\substack{p|M \\ p \text{ prime}}} \left(1+\frac{1}{p}\right) + 1 \leq \frac{8}{3}N^2 \prod_{\substack{p|N \\ p \text{ prime}}} \left(1+\frac{1}{p}\right) + 1$$

with $(n, N) = 1$. Here, $a_n(f)$ and $a_n(f')$ denote the $n$-th Fourier coefficients of $f$ and $f'$.

Since $f$ and $f'$ are normalized newforms, the coefficients $a_n(f)$ and $a_n(f')$ are multiplicative in $n$, hence there exists a prime $q|n$ such that

$$a_{q^\alpha}(f) \neq a_{q^\alpha}(f'),$$

with the power $\alpha$ such that $q^\alpha \| n$. Moreover, the recurrence relations (6) for $a_{q^t}(f)$ and their analogues for $a_{q^t}(f')$, where $t$ is an arbitrary positive integer, give us that

$$a_q = a_q(f) \neq a_q(f') = a'_q. \tag{13}$$

Now we want to show that $\epsilon_l(q) = -1$. Let us suppose that $\epsilon_l(q) \neq -1$. We notice that $\epsilon_l(q) \neq 0$, since $\epsilon_l$ is unramified at the primes of good reduction for $E$ and $q$ is such a prime. Then we must have $\epsilon_l(q) = 1$, which implies

$$a'_q = \epsilon_l(q) a_q = a_q,$$

a contradiction with (13).

We have therefore proven that there exists a prime $q$ of good reduction for $E$ satisfying conditions (8), (9), (10). By (8) we deduce that $a_q \neq 0$, and by (10) and (3) we deduce that $l|a_q$. Using Hasse's bound and (10) we obtain

$$l < \frac{4\sqrt{6}}{3}N \prod_{\substack{p|N \\ p \text{ prime}}} \left(1+\frac{1}{p}\right)^{1/2} + 1,$$

which completes the proof of the first part of Theorem 2.

Let us remark that

$$A(E) \leq 37\Big(\prod_{\substack{p \leq 19 \\ p \text{ prime}}} p\Big)\,|a_q| \ll q^{1/2}, \tag{14}$$

where $q$ is the prime satisfying (8)–(10). We also recall from elementary number theory that

$$\prod_{\substack{p|N \\ p \text{ prime}}} \left(1+\frac{1}{p}\right) \ll \log\log N. \tag{15}$$

Combining (10), (14) and (15) gives the second assertion of Theorem 2. This completes the proof.

## 4 Proof of Theorem 3

We recalled in the Introduction that for any prime $l$ such that $l > c_2\, \mathrm{h}(E)^{\gamma}$, with $\mathrm{h}(E)$ denoting the Faltings height of $E$ and with $c_2$ and $\gamma$ as in (5), the representation $\phi_l$ is surjective.

Now we want to relate $\mathrm{h}(E)$ to the conductor $N$ of the elliptic curve $E$. To do so, we let $f \in \mathrm{S}_2(\Gamma_0(N))$ be the normalized newform associated to $E$ and $\phi\colon X_0(N) \longrightarrow E$ be a minimal modular parametrization of $E$ given by Theorem 2.3. As shown in [RM99, pp. 181–182], we have that

$$2\,\mathrm{h}(E) + \log\langle f, f\rangle = \log \deg \phi + \mathrm{O}(1),$$

and that for any $\varepsilon > 0$ and $N$ sufficiently large,

$$(1-\varepsilon)\log N < \log\langle f, f\rangle < (1+\varepsilon)\log N.$$

Here, $\langle \cdot\,, \cdot \rangle$ denotes the Petersson inner product and $\deg\phi$ denotes the degree of $\phi$. We obtain

$$(1-\varepsilon)\log N + 2\,\mathrm{h}(E) < \log\deg\phi + \mathrm{O}(1) < (1+\varepsilon)\log N + 2\,\mathrm{h}(E).$$

By the degree conjecture for $E$, $\deg\phi = \mathrm{O}_{\varepsilon}(N^{2+\varepsilon})$, hence

$$\mathrm{h}(E) \ll \log N, \tag{16}$$

where the implied constant is absolute. We use (16) in (5) and deduce that there exists an absolute positive constant $c_3$ such that, for any prime $l$ satisfying

$$l > c_3(\log N)^{\gamma}\,(\geq c_2\,\mathrm{h}(E)^{\gamma})\,,$$

the representation $\phi_l$ is surjective. This completes the proof of Theorem 3.

## 5 Final Remarks

The bound provided by Theorem 3 is weaker than the bound (4) obtained by Serre by assuming GRH, since the Masser-Wüstholz constant $\gamma$, even though effective, is not yet determined (see [MaWü, p. 248]). On the other hand, the hypothesis of Theorem 3 is different, as illustrated in [RM99], where it is shown that the ABC conjecture is equivalent to the degree conjecture for Frey curves.[1] It will be interesting to find the value of the Masser-Wüstholz constant $\gamma$, and consequently, to find the precise estimate $A(E) \ll N^b$ provided by Theorem 3. As shown in Theorem 2, we have $A(E) \ll_{\varepsilon} N^{1+\varepsilon}$ for any small positive $\varepsilon$. Currently, this is the best (unconditional) estimate for $A(E)$. We hope to address the problem of showing that $A(E) \ll N^b$ for some $b < 1$ in future research.

**Acknowledgements** The results of this paper were obtained in the fall of 2001, while I was a graduate student at Queen's University in Kingston. I wish to thank Prof. M. Ram Murty for valuable discussions on these results and for encouraging me to write the paper. Also, I wish to thank Prof. Ernst Kani for useful discussions on the constant $A(E)$.

[1] Using the "unconditional ABC" proven in [StYu], we obtain that for a non-CM Frey curve $E$ of conductor $N$, $\phi_l$ is surjective for any prime $l \gg N^{\gamma/3}(\log N)^3$.

## Appendix: The Surjectivity of mod $m$ Galois Representations

### *by* Ernst Kani

The aim of this appendix is to prove the following result.

***Theorem 1*** *If $E$ is an elliptic curve defined over $\mathbb{Q}$ and $m$ is any integer with $(m, 30) = 1$, then the Galois representation*

$$\overline{\rho}_{E,m}\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

*is surjective if and only if the Galois representations $\overline{\rho}_{E,p}$ are surjective for every prime $p|m$. In particular, if $E$ is a non-CM elliptic curve and $A(E)$ is Serre's constant associated to $E$ (see the definition in Section 1 of the paper), then $\overline{\rho}_{E,m}$ is surjective for every integer $m$ with $(m, A(E)) = 1$.*

This theorem is essentially due to Serre and can be deduced from the Main Lemma in his book [Se68, p. IV-19]. However, since this fact does not seem to be widely known and since there is a small gap in his argument (similar to the gap which is mentioned in his Collected Papers [Se85, p. 715]), it seems useful to present the following (modified) proof.

As in Serre's book, the above assertion can be deduced from a purely group-theoretical statement about subgroups of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, which is perhaps also of independent interest. To state this result, we use the following notation introduced in Serre [Se68, p. IV-25]

***Notation*** For any finite group $G$, let $\mathrm{Occ}(G)$ denote the set of isomorphism classes of non-abelian finite simple groups which occur as a composition factor of some subgroup $H \leq G$. Let $p$ and $q$ denote rational primes.

***Theorem 2*** *Let $G$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ where $(m, 30) = 1$. Then:*

(a) *$G = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ if and only if $G \geq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ and $\phi(m)|[G : G']$.*
(b) *$G \geq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ if and only $\mathrm{PSL}_2(p) \in \mathrm{Occ}(G)$ for all primes $p|m$ (here, $\mathrm{PSL}_2(p) := \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/(\pm 1)$).*

In order to prove this theorem, we first recall some basic facts about the matrix groups $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$.

The following (well-known) facts can be found in [Hu, Theorems II.6.13; II.8.14]:

***Lemma 3*** *Let $p$ and $q$ be prime numbers. Then:*

(a) *$\mathrm{PSL}_2(p)$ is a simple group for any $p \geq 5$;*
(b) *$\mathrm{PSL}_2(p) \simeq \mathrm{PSL}_2(q)$ if and only if $p = q$;*
(c) *If $H$ is a proper subgroup of $\mathrm{PSL}_2(p)$, then $H$ is solvable or $H \simeq A_5$;*
(d) *$\mathrm{PSL}_2(p) \simeq A_5$ if and only if $p = 5$.*

Moreover, by Lemma 2 of [Se68, p. IV-23], we have

***Lemma 4*** *Let $H$ be a subgroup of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ such that $\pm H = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Then $H = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.*

***Corollary 5*** *If $p \geq 5$ is a prime, then the commutator subgroup $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})'$ of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ itself,* i.e., $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})' = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

**Proof** Since $\mathrm{PSL}_2(p)$ is non-abelian and simple (*cf.* Lemma 3(a)), we have

$$\mathrm{PSL}_2(p)' = \mathrm{PSL}_2(p)$$

and so $\pm\,\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})' = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Thus, the assertion follows from Lemma 4. ■

To extend the above result to $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ for an arbitrary integer $m$, let $d|m$ be a divisor of $m$ and consider the (surjective) group homomorphism

$$pr_d = pr_d^{(m)}\colon\ \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}),$$

which is induced by reduction modulo $d$. We then have:

***Lemma 6*** *Let $H$ be a subgroup of $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$, where $p \geq 5$ is a prime and $r$ is a positive integer. If $pr_p(H) = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, then $H = \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$.*

This result can be deduced from the proof of Lemma 3 of [Se68]. As pointed out in [Se68], the result is false for $p = 2$ and $p = 3$. The above lemma has the following consequences:

***Corollary 7*** *For any integer $m$ with $(m, 6) = 1$ we have that the commutator subgroup $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})'$ is $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$.*

**Proof** Since $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) = \prod_{p^r||m} \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$, it is enough to verify this for a prime power $m = p^r$ with $p \geq 5$. In that case we can apply Lemma 6 to $H = \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})'$ because by Corollary 5 we have $pr_p(H) = pr_p(\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z}))' = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})' = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Thus, by Lemma 6 we obtain that $H = \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$, as desired. ■

***Corollary 8*** *Let $m$ be a positive integer coprime to 6. If*

$$\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \leq H \leq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

*then $H' = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. In particular, $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})' = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$.*

**Proof** Since $H/\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \leq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ is abelian, we see that $H' \leq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. On the other hand, by Corollary 7 we also have that

$$\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})' \leq H',$$

and so $H' = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. ■

As we shall see below, part (a) of Theorem 2 follows readily from Corollary 8. We therefore turn now to preliminary preparations for part (b). Here we first note:

***Lemma 9*** *Let $G$ be a finite group. Then:*

(a) $\mathrm{Occ}(G) = \varnothing$ *if and only if $G$ is solvable.*
(b) *If $H$ is a normal subgroup of $G$, then* $\mathrm{Occ}(G) = \mathrm{Occ}(H) \cup \mathrm{Occ}(G/H)$.

**Proof** Let $\mathcal{N}(G)$ denote the set of isomorphism classes of non-abelian composition factors of $G$, so that $\mathrm{Occ}(G) = \bigcup_{H \leq G} \mathcal{N}(H)$.

(a) If $\mathrm{Occ}(G) = \varnothing$, then also $\widetilde{\mathcal{N}}(G) = \varnothing$, and so by [Hu, I.11.9] $G$ is solvable. Conversely, if $G$ is solvable, then so is any of its subgroups $H \leq G$, and hence by [Hu, I.11.9] again, we obtain that $\mathrm{Occ}(G) = \varnothing$.

(b) From the definition it follows that $\mathcal{N}(G) = \mathcal{N}(H) \cup \mathcal{N}(G/H)$, and so we see that $\mathrm{Occ}(G) \supseteq \mathrm{Occ}(H) \cup \mathrm{Occ}(G/H)$. For the reverse inclusion we let $K \leq G$. Then $H \cap K$ is a normal subgroup of $K$, and so $\mathcal{N}(K) = \mathcal{N}(H \cap K) \cup \mathcal{N}(K/(H \cap K)) = \mathcal{N}(H \cap K) \cup \mathcal{N}((HK)/K) \subseteq \mathrm{Occ}(H) \cup \mathrm{Occ}(G/H)$, which yields the other inclusion. ∎

We now use the above result to determine $\mathrm{Occ}(G)$ for our matrix groups.

***Lemma 10*** *If $m$ is a positive integer, then*

$$\mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})) = \mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})) = \bigcup_{p|m} \mathrm{Occ}(\mathrm{PSL}_2(p)). \tag{17}$$

*Moreover, if $p \geq 5$ is a prime, then*

$$\{\mathrm{PSL}_2(p)\} \subset \mathrm{Occ}(\mathrm{PSL}_2(p)) \subset \{\mathrm{PSL}_2(p), A_5\}. \tag{18}$$

**Proof** Since (18) is just a restatement of parts (a) and (c) of Lemma 3, it is enough to verify (17).

The first equality of (17) follows from Lemma 10 and from the fact that

$$\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$$

is abelian. For the second equality we first note that Lemma 9(b) implies that

$$\mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})) = \bigcup_{p^r \| m} \mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z}))$$

because $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) = \prod_{p^r \| m} \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$. Next we observe that

$$\mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})) = \mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}))$$

because $\mathrm{Ker}(pr_p)$ is a $p$-group (and hence is solvable). Since clearly

$$\mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})) = \mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/(\pm 1)),$$

this proves the second equality of (17). ∎

***Corollary 11*** *If $p > 5$ is a prime and $m$ is an integer such that $p \nmid m$, then* $\mathrm{PSL}_2(p) \notin \mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}))$.

**Proof** Since $p > 5$ we have by Lemma 3 that $\mathrm{PSL}_2(p) \not\simeq A_5$ and that $\mathrm{PSL}_2(p) \not\simeq \mathrm{PSL}_2(q)$ for any prime $q|m$. Thus, the assertion follows from Lemma 10. ■

***Lemma 12*** *Let $G \leq \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z})$, where $p \geq 5$ is a prime and $r$ is a positive integer. Then the following statements are equivalent:*

(i) $\mathrm{PSL}_2(p) \in \mathrm{Occ}(G)$.
(ii) $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z}) \leq G$.
(iii) $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \leq pr_p(G)$.

**Proof** (ii) $\Rightarrow$ (i). This is trivial, since $\mathrm{PSL}_2(p)$ is a composition factor of $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$.

(i) $\Rightarrow$ (iii). Since $pr_p(G) \simeq G/H$ where $H \leq \mathrm{Ker}(pr_p)$ is a $p$-group, we see by Lemma 9 that $\mathrm{Occ}(G) = \mathrm{Occ}(pr_p(G))$.

Now for any subgroup $K \leq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ we know by [La, Theorem XI.2.2] that

$$K \geq \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \Leftrightarrow p \,\Big|\, |K| \text{ and } K \text{ is not contained in a Borel subgroup.}$$

Since the Borel subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ are solvable, this therefore shows that the condition $\mathrm{PSL}_2(p) \in \mathrm{Occ}(pr_p(G))$ implies that $pr_p(G) \geq \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

(iii) $\Rightarrow$ (ii). Consider $H := G' \leq \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z})' = \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ by Corollary 8. Now since $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \leq pr_p(G)$ by hypothesis, we have $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})' \leq pr_p(G)' = pr_p(G') = pr_p(H) \leq \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. But $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})' = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ by Corollary 5, and so $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) = pr_p(H)$. It therefore follows from Lemma 6 that

$$\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z}) = H = G' \leq G,$$

and hence condition (ii) holds. ■

We are now ready to prove Theorem 2.

**Proof of Theorem 2**

(a) If $G = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, then clearly $G \geq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. Moreover, by Corollary 8 we have

$$\phi(m) = [\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})] = [\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})'] = [G : G'],$$

so in particular $\phi(m)|[G : G']$.

Conversely, if $G \geq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ and $\phi(m)|[G : G']$, then

$$|\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})| = \phi(m)\,|\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})|$$

is a divisor of $[G : G']\,|\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})| = |G|$, where the last equality follows from the fact that $G' = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ by Corollary 8. Thus $|\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})|$ divides $|G|$, and hence $G = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

(b) If $G \geq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$, then $G/\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ is abelian and so

$$\mathrm{Occ}(G) = \mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})) \supset \{\mathrm{PSL}_2(p) : p|m\}$$

by Lemma 10.

Conversely, suppose that $\mathrm{Occ}(G) \supset \{\mathrm{PSL}_2(p) : p|m\}$. For any prime $p|m$ and any subgroup $H \leq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ let $H^{(p)} = H \cap \mathrm{Ker}(pr_{m/p^r})$, where $p^r \parallel m$. Note that $H^{(p)} \trianglelefteq H$ is a normal subgroup of $H$ and that

$$H^{(p)} \leq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})^{(p)} \simeq \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z}).$$

We claim that $\mathrm{PSL}_2(p) \in \mathrm{Occ}(H^{(p)})$. Indeed, since $H/H^{(p)} \simeq pr_{m/p^r}(H)$, and since $\mathrm{PSL}_2(p) \notin \mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}/\frac{m}{p^r}\mathbb{Z}))$ by Corollary 11 (using the fact that $p > 5$ by our hypothesis), we have that $\mathrm{PSL}_2(p) \in \mathrm{Occ}(H^{(p)})$ by Lemma 9(b). Thus, by Lemma 12 (applied to $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})^{(p)} \simeq \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z})$) we see that $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{(p)} \leq H^{(p)}$ because $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{(p)} \simeq \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ (via the above isomorphism). Since this is true for all $p|m$, we obtain

$$\prod_{p|m} \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{(p)} \leq \prod_{p|m} H^{(p)} \leq H.$$

But by the Chinese remainder theorem we have

$$\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) = \prod_{p|m} \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})^{(p)} \quad \text{and} \quad \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) = \prod_{p|m} \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{(p)}$$

(as subgroups of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ ) and so we obtain $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \leq H$, as desired. This completes the proof of Theorem 2. ∎

***Remark*** Part (b) of this theorem is closely related to [Se68, Lemma 5]. However, the proof of that lemma has a small gap, for it is not true (or clear) that the subgroup $H_\ell$ (as defined on line 6) actually maps into $\mathrm{SL}_2(\mathbb{F}_\ell)$ (as is asserted on line 13). Nevertheless, the argument is easily repaired by the same argument as in the implication (iii) $\Rightarrow$ (ii) of Lemma 12.

**Proof of Theorem 1** If $\overline{\rho}_{E,m}$ is surjective, then clearly so is $\overline{\rho}_{E,p} = pr_p^{(m)} \circ \overline{\rho}_{E,m}$ for every $p|m$.

Conversely, suppose $\overline{\rho}_{E,p}$ is surjective for all $p|m$. Then $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is a quotient of $G := \mathrm{im}(\overline{\rho}_{E,m}) \leq \mathrm{GL}_m(\mathbb{Z}/m\mathbb{Z})$, and so $\mathrm{PSL}_2(p) \in \mathrm{Occ}(G)$, for every $p|m$ and hence $G \geq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ by Theorem 2(b).

Moreover, since $G \simeq \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ and since $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(E[m])$, we see that $\phi(m)|[G : G']$. Thus, by Theorem 2(a) we have that $G = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, *i.e.,* that $\overline{\rho}_{E,m}$ is surjective.

The last assertion is clear, for by definition $A(E) = 30 \prod_{p \in S_E} p$, where $S_E$ is the set of primes $p$ such that $\overline{\rho}_{E,p}$ is not surjective. ∎

***Corollary 13*** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and let $m$ be a positive integer coprime to $A(E)$. Then $\mathbb{Q}(\zeta_m)$ is the maximal abelian extension of $\mathbb{Q}$ in $\mathbb{Q}(E[m])$ and* $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

**Proof** Let $G := \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \simeq \mathrm{im}(\overline{\rho}_{E,m})$. By Theorem 1 we know that $\overline{\rho}_{E,m}$ is surjective, so $G \simeq \mathrm{im}(\overline{\rho}_{E,m}) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Thus, by Corollary 8 we have $[G : G'] = \phi(m)$ and so the maximal abelian extension in $\mathbb{Q}(E[m])$ has degree $\phi(m)$. Since $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(E[m])$, the assertion follows. ∎

## References


[BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises.* J. Amer. Math. Soc. **14**(2001), 843–939.

[Co] A. C. Cojocaru, *Cyclicity of elliptic curves modulo p*. PhD thesis, Queen's University, 2002.

[De] P. Deligne, *Représentations l-adiques.* Astérisque, **127**(1985), 249–255.

[Hu] B. Huppert, *Endliche Gruppen I.* Grundlehren Math. Wiss., 134, Springer-Verlag, Berlin, 1967.

[Iw] H. Iwaniec, *Topics in classical automorphic forms.* Graduate Studies in Mathematics, 17, Amer. Math. Soc, Providence, RI, 1997.

[Kr] A. Kraus, *Une remarque sur les points de torsion des courbes elliptiques.* C. R. Acad. Sci. Paris, t. 321, Sér. I Math.**321**(1995), 1143–1146.

[La] S. Lang, *Introduction to modular forms.* Grundlehren Math. Wiss. 222, Springer-Verlag, Berlin, 1976.

[MaWü] D. W. Masser and G. Wüstholz, *Galois properties of division fields of elliptic curves.* Bull. London Math. Soc. **25**(1993), 247–254.

[Maz] B. Mazur, *Rational isogenies of prime degree.* Invent. Math. **44**(1978), 129–162.

[Mer] Loic Merel, *Arithmetic of elliptic curves and diophantine equations.* J. Théor. Nombres Bordeaux **11**(1999), 173–200.

[RM97] M. Ram Murty, *Congruences between modular forms.* In: Analytic Number Theory (ed. Y. Motohashi), London Math. Soc. Lecture Note Series 247, 1997, pp. 309–320.

[RM99] ———, *Bounds for congruence primes.* In: Automorphic Forms, Automorphic Representations and Arithmetic, (ed. Robert S. Doran, Ze-Li Dou and George T. Gilbert), Amer. Math. Soc., Providence, Ri, 1999, pp. 177–192.

[Se68] J.-P. Serre, *Abelian l-adic representations and elliptic curves.* W. A. Benjamin, New York, 1968.

[Se72] ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* Invent. Math. **15**(1972), 259–331.

[Se81] ———, *Quelques applications du théorème de densité de Chebotarev.* Inst. Hautes Études Sci. Publ. Math. **54**(1981), 123–201.

[Se85] ———, *Collected papers.* volume III, Springer-Verlag, 1985.

[Si84] J. H. Silverman, *Heights and elliptic curves.* In: Arithmetic Geometry (G. Cornell, J. H. Silverman, eds.), Springer-Verlag, New York, 1986, pp. 253–265.

[Si86] ———, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.

[StYu] C. L. Stewart and Kunrui Yu, *On the ABC conjecture.* Duke Math. J. **108**(2001), 169–181.



*The Fields Institute*
*222 College Street*
*Toronto, ON*
*M5T 3J1*
*e-mail: alina@fields.utoronto.ca*

*Queen's University*
*Department of Mathematics and Statistics*
*Kingston, ON,*
*K7L 3N6*
*e-mail: kani@mast.queensu.ca*