QUADRATIC $\mathbb{Q}$-CURVES, UNITS AND HECKE L-VALUES

NEIL DUMMIGAN AND VASILY GOLYSHEV

Abstract. We show that if K is a quadratic field, and if there exists a quadratic $\mathbb{Q}$-curve E/K of prime degree N, satisfying weak conditions, then any unit u of O_K satisfies a congruence $u^r \equiv 1 \pmod{N}$, where $r = \text{g.c.d.}(N-1, 12)$. If K is imaginary quadratic, we prove a congruence, modulo a divisor of N, between an algebraic Hecke character $\tilde{\psi}$ and, roughly speaking, the elliptic curve. We show that this divisor then occurs in a critical value $L(\tilde{\psi}, 2)$, by constructing a non-zero element in a Selmer group and applying a theorem of Kato.

1. Introduction

An elliptic curve E defined over $\overline{\mathbb{Q}}$ is said to be a $\mathbb{Q}$-curve if it is isogenous, over $\overline{\mathbb{Q}}$, to all its $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates. If E has complex multiplication by an order in an imaginary quadratic field F, with Hilbert class field H, then E is a $\mathbb{Q}$-curve, and (with all the isogenies) can be defined over H. Let N be a square-free positive integer, with r prime factors, and let $X^*(N)$ be the quotient of the modular curve $X_0(N)$ by the group, of order 2^r, of Atkin-Lehner involutions. This curve is defined over $\mathbb{Q}$, and if $P \in X^*(N)(\mathbb{Q})$ is a non-cusp rational point, then the points on $X_0(N)$ projecting to P are defined over some number field K with $\text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^\rho$, for some $\rho \leq r$. These points represent a collection of isogenous $\mathbb{Q}$-curves, each of which can be defined over K (though maybe not the isogenies between them). A theorem of Elkies [E] implies that every non-CM $\mathbb{Q}$-curve is isogenous to such a collection of $\mathbb{Q}$-curves, for some square-free N. In this paper we concentrate on the case that N is prime (in which case we write $X_0^+(N)$ instead of $X^*(N)$) and K is a quadratic field, and call E a "quadratic $\mathbb{Q}$-curve", with N-isogenous conjugate E^σ.

In Section 2 we introduce, for a non-CM quadratic $\mathbb{Q}$-curve E, the character χ_1 by which $\text{Gal}(\overline{\mathbb{Q}}/K)$ acts on the kernel of the N-isogeny from E to E^σ. In Section 3 we examine the ramification properties of χ_1. In particular we use a proposition of Serre to identify with a fundamental tamely-ramified character its restriction to the inertia group at a prime divisor of N. In Section 4 this allows us, under certain hypotheses, to prove the first main result (Theorem 4.1), that if u is any unit in O_K, and $\mathfrak{q}$ a prime divisor of N, then $u \equiv \pm 1 \pmod{\mathfrak{q}}$. This is achieved by a simple application of global class field theory to the triviality of $\chi_1^2(u)$, and is only of interest when K is real quadratic.

The primes N for which $X_0^+(N)$ has genus zero (i.e. $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 47, 59, 71$) are well-known to be those dividing the order of the Monster group. In Section 5 we present numerical examples for several such N, using rational parametrisations found by González and Lario. We also consider the example $N = 43$, for which $X_0^+(N)$ is an elliptic curve with Mordell-Weil group of rank 1,

Date: March 24th, 2015.

and for which the map from $X_0(N)$ to $X_0^+(N)$ has been made explicit by Yamauchi. At the end of Section 5 we observe the congruences arising from the five values of N for which the genus of $X_0(N)^+$ is at least 2 but for which "exceptional" rational points (non-cuspidal, non-CM) were discovered by Elkies and Galbraith.

In Section 6 we consider $\mathbb{Q}$-abelian varieties of higher dimension, with everywhere good reduction, and make a link with Shimura's theory of abelian varieties arising from modular forms with nebentypus.

The character χ_1 takes values in $\mathbb{F}_N^\times$. In Section 7 we show, in the case that K is imaginary quadratic, that χ_1^2 is the reduction of an algebraic Hecke character $\tilde{\psi}$ of $\mathbb{A}_K^\times$, of type $(2,0)$. The L-function $L(\tilde{\psi}, s)$ has critical values at $s = 1, 2$. In Section 9 we use this congruence relation between $\tilde{\psi}$ and χ_1^2 to construct a non-zero element in a certain Selmer group for $\tilde{\psi}$, which, via the Bloch-Kato conjecture (Section 8), should lead to the appearance of a divisor of N in the algebraic part of $L(\tilde{\psi}, 2)$, and in fact it does, thanks to work of Kato and Rubin. In Section 10 we consider an example where this can be observed.

We were led to consider quadratic $\mathbb{Q}$-curves by the appearance of $E \times E^\sigma$ in pencils of abelian surfaces (fibred over an open subset of $X_0(N)^+$) which, for certain values of $N \leq 11$, are mirror dual to families of Fano 3-folds of Picard rank 1, [Gv, §3.2]. We wanted an arithmetical manifestation, as the modulus of a congruence or a factor in an L-value, of the factor N in the anticanonical degree of the Fano 3-folds.

We thank Anton Mellit and Don Zagier for discussions on this subject with the second named author, Takuya Yamauchi for correcting a sign error in 5.2, and the referee for a careful reading.

2. Kernels of cyclic isogenies

For a prime number N, let $Y_0(N)/\mathbb{Q}$ be the modular curve defined by the modular equation $\Phi(X,Y) = 0$ [Co, Chapter 11]. The Fricke involution $w_N : (X,Y) \mapsto (Y,X)$ is obviously defined over $\mathbb{Q}$. Let $Y_0^+(N)/\mathbb{Q}$ be the quotient curve $Y_0(N)/w_N$, and $\pi : Y_0(N) \to Y_0^+(N)$ the quotient map. If $P \in Y_0^+(N)(\mathbb{Q})$, and if $\pi^{-1}(P)$ contains two points that are not $\mathbb{Q}$-rational, then they are necessarily of the form (j, j^σ) and (j^σ, j), where $K/\mathbb{Q}$ is a quadratic extension, $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$ and $j \in K$. Let $\mathcal{F}$ be the functor from the category $\mathcal{C}$ of $\mathbb{Q}$-algebras to the category of sets, taking S to the set of S-isomorphism classes of (E, C), with the elliptic curve E and its N-cyclic subgroup scheme C both defined over S. If $\mathcal{G}$ is the functor of points from $\mathcal{C}$ to sets, $S \mapsto Y_0(N)(S)$, then there is a natural transformation of functors from $\mathcal{F}$ to $\mathcal{G}$. This is not an equivalence of functors ($Y_0(N)$ is only a coarse moduli space), but it does induce a bijection between $\mathcal{F}(\overline{\mathbb{Q}})$ and $Y_0(N)(\overline{\mathbb{Q}})$. The point (j, j^σ) represents a $\overline{\mathbb{Q}}$-isomorphism class (E, C), where moreover the j-invariants of E and E/C are j and j^σ respectively. Since $j \in K$, the $\overline{\mathbb{Q}}$-isomorphism class of E may be represented by a curve E defined over K. Then $E/C \simeq E^\sigma$ over $\overline{\mathbb{Q}}$, where E^σ is the result of applying σ to all the coefficients in a Weierstrass equation for E. Thus we get an isogeny $\phi : E \to E^\sigma$, with kernel C, determined up to an automorphism of E^σ (which we shall imagine to have been fixed). However, we do not know that the isogeny $\phi : E \to E^\sigma$ is defined over K, and in general it is not (see [Ha, Proposition 3.3] for example). The point is that although the isogeny $E \to E/C$ is defined over K, we are composing it with an isomorphism $E/C \to E^\sigma$, which might not be.

Lemma 2.1. *Suppose that E does not have complex multiplication. Then there exists a character $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \{\pm 1\}$ such that for all $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, $\phi^g = \chi(g)\phi$. It follows that also $\pm\widehat{\phi}^g = \chi(g)\widehat{\phi}$, where $\widehat{\phi}$ is the dual isogeny. Note that $\phi^g : E \to E^\sigma$, since E, E^σ are defined over K.*

Proof. Suppose, for a contradiction, that there exists $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ with $\phi^g \neq \pm\phi$. Then $\widehat{\phi^g} \circ \phi$ is an endomorphism of E, of degree N^2, but different from $\pm[N]$. This would imply that E had complex multiplication. □

The same argument shows that $\phi^\sigma : E^\sigma \to E$ is $\pm\widehat{\phi}$.

Consider the N-adic Tate modules $T_N(E)$ and $T_N(E^\sigma)$. Each is a free $\mathbb{Z}_N$-module of rank 2, with continuous $\mathbb{Z}_N$-linear action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. The reductions mod N are $E[N]$ and $E^\sigma[N]$. Choose $e_1 \in T_N(E)$ and $f_1 \in T_N(E^\sigma)$ such that their images in $E[N]$ and $E^\sigma[N]$ generate $\ker\phi$ and $\ker\widehat{\phi}$ respectively. Then $\phi(e_1) = Nf_2$ for some $f_2 \in T_N(E^\sigma)$, and $\widehat{\phi}(f_1) = Ne_2$ for some $e_2 \in T_N(E)$. Since $\widehat{\phi}\phi = \phi\widehat{\phi} = [N]$, $\widehat{\phi}(f_2) = e_1$ and $\phi(e_2) = f_1$. We have $\mathbb{Z}_N$-bases $\{e_1, e_2\}$ and $\{f_1, f_2\}$ for $T_N(E)$ and $T_N(E^\sigma)$ respectively, and with respect to these bases both ϕ and $\widehat{\phi}$ are represented by the matrix $\begin{bmatrix} 0 & 1 \\ N & 0 \end{bmatrix}$. We may choose e_1 and f_1 in such a way that for the Weil pairing, $\langle e_1, e_2\rangle = \langle f_2, f_1\rangle = 1$.

Lemma 2.2. *One has that $\ker\phi \subseteq E[N]$ and $\ker\widehat{\phi} \subseteq E^\sigma[N]$ are $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$-invariant.*

Proof. For $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$, $(\ker\phi)^g = \ker(\phi^g) = \ker(\pm\phi) = \ker\phi$. Similarly for $\ker\widehat{\phi}$. □

Hence if, with respect to the bases $\{e_1, e_2\}$ and $\{f_1, f_2\}$, $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ is represented by matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ (on $T_N(E)$) and $\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ (on $T_N(E^\sigma)$) then $N \mid c$ and $N \mid c'$.

Lemma 2.3.

$$\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \chi(g) \begin{bmatrix} d & c/N \\ Nb & a \end{bmatrix},$$

with χ as in Lemma 2.1.

Proof. On $T_N(E^\sigma)$,

$$g = \frac{1}{N}\phi\widehat{\phi}g = \frac{\chi(g)}{N}\phi g\widehat{\phi} = \frac{\chi(g)}{N}\begin{bmatrix} 0 & 1 \\ N & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ N & 0 \end{bmatrix} = \chi(g)\begin{bmatrix} d & c/N \\ Nb & a \end{bmatrix},$$

where the second equality follows from Lemma 2.1. □

3. Restrictions of characters to inertia subgroups

The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ on $E[N]$ is reducible, with composition factors $\chi_1, \chi_2 : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathbb{F}_N^\times$. If $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ is represented by the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ as above, then $\chi_1(g) \equiv a \pmod{N}$ and $\chi_2(g) \equiv d \pmod{N}$. Considering the Weil pairing, $\chi_1\chi_2 = \epsilon$, the mod N cyclotomic character (giving the action on N^{th} roots of unity), which is ramified precisely at primes dividing N.

Let $\mathfrak{q}$ be a prime of O_K, the ring of integers of K, dividing the rational prime N, and let $K_\mathfrak{q}$ be the completion of K at $\mathfrak{q}$, with uniformiser π. Let $K_\mathfrak{q}^u$ and $K_\mathfrak{q}^t$ be the maximal unramified and tamely ramified extensions (respectively) of $K_\mathfrak{q}$. For each integer $d > 1$ with $N \nmid d$, there is a character $\theta_d : \mathrm{Gal}(K_\mathfrak{q}^t/K_\mathfrak{q}^u) \to \mu_d$ (where μ_d denotes the group of d^{th} roots of unity inside $K_\mathfrak{q}^u$) such that $g(\pi^{1/d}) = \theta_d(g)\pi^{1/d}$, for all $g \in \mathrm{Gal}(K_\mathfrak{q}^t/K_\mathfrak{q}^u)$ and all choices of $\pi^{1/d}$. Viewing $\mathrm{Gal}(K_\mathfrak{q}^t/K_\mathfrak{q}^u)$ as the tame quotient of the inertia group $I_\mathfrak{q}$, and reducing mod π, we get a character $\theta_d : I_\mathfrak{q} \to \overline{\mathbb{F}}_N^\times$. Letting $d = N^r - 1$ for some integer $r \geq 1$, this is a "fundamental character of level r", $\theta_{N^r-1} : I_\mathfrak{q} \to \mathbb{F}_{N^r}^\times$. Deviating from the notation of Serre [Se, 1.7], in the case $r = 1$ we relabel this $\theta_\mathfrak{q}$.

Proposition 3.1. *Let E/K be an elliptic curve with a cyclic N-isogeny $\phi : E \to E^\sigma$, and no complex multiplication, as in the previous section, and $\chi_1, \chi_2 : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathbb{F}_N^\times$ be as above. Suppose also that $N > 5$, and that E has good reduction at any divisor of N.*

1. *The good reduction at any divisor of N is ordinary.*
2. *The prime N splits in O_K, say $(N) = \mathfrak{q}\overline{\mathfrak{q}}$.*
3. *Without loss of generality,*

$$\chi_1 \mid_{I_\mathfrak{q}} = \theta_\mathfrak{q},\ \chi_1 \mid_{I_{\overline{\mathfrak{q}}}} = \mathrm{id.},$$
$$\chi_2 \mid_{I_\mathfrak{q}} = \mathrm{id.},\ \chi_2 \mid_{I_{\overline{\mathfrak{q}}}} = \theta_{\overline{\mathfrak{q}}}.$$

Proof. It follows from [Se, Proposition 12(c)] that if the reduction were supersingular then the action on $E[N]$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ (or even of the subgroup $I_\mathfrak{q}$) would be irreducible, which it clearly is not. Hence the reduction is ordinary, and by [Se, Proposition 11] $\{\chi_1 \mid_{I_\mathfrak{q}}, \chi_2 \mid_{I_\mathfrak{q}}\} = \{\mathrm{id.}, \theta_\mathfrak{q}^e\}$, where e is the ramification index of $K_\mathfrak{q}/\mathbb{Q}_N$. If N does not split in O_K then $\mathfrak{q}$ is the unique prime divisor of N. Now $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ acts on $\ker\phi$ as χ_1 and on $\ker\widehat{\phi}$ as $\chi\chi_2$, where χ is as in Lemma 2.1. Restricting to $I_\mathfrak{q}$, we get either id. on $\ker\phi$ with $\chi\theta_\mathfrak{q}^e$ on $\ker\widehat{\phi}$, or $\theta_\mathfrak{q}^e$ on $\ker\phi$ with χ on $\ker\widehat{\phi}$. Either way, the $\mathrm{Gal}(K/\mathbb{Q})$-symmetry between $\ker\phi$ and $\ker\widehat{\phi}$ is violated, since the condition $N > 5$ ensures that, unlike χ, $\theta_\mathfrak{q}^e$ is not quadratic or trivial.

We have $(N) = \mathfrak{q}\overline{\mathfrak{q}}$, and $e = 1$. Now $\{\chi_1 \mid_{I_\mathfrak{q}}, \chi_2 \mid_{I_\mathfrak{q}}\} = \{\theta_\mathfrak{q}, \mathrm{id.}\}$ and $\{\chi_1 \mid_{I_{\overline{\mathfrak{q}}}}, \chi_2 \mid_{I_{\overline{\mathfrak{q}}}}\} = \{\theta_{\overline{\mathfrak{q}}}, \mathrm{id.}\}$, but (after ordering $\mathfrak{q}$ and $\overline{\mathfrak{q}}$ appropriately) it must be as stated in the proposition, otherwise again the symmetry is violated. (We see also that χ is unramified at $\mathfrak{q}$ and $\overline{\mathfrak{q}}$.) □

Note that the discussion in §2 determined E only up to quadratic twist, so we are really assuming that some E/K within the $\overline{K}$-isomorphism class has good reduction at primes dividing N.

Proposition 3.2. *Let $\mathfrak{p}$ be a prime of O_K not dividing N. Then $\chi_2 \mid_{I_\mathfrak{p}} = \chi_1^{-1} \mid_{I_\mathfrak{p}}$ and, if $r := \mathrm{g.c.d.}(N-1, 12)$ then $\chi_1 \mid_{I_\mathfrak{p}}$ has order dividing r.*

Proof. We have $\chi_2 \mid_{I_\mathfrak{p}} = \chi_1^{-1} \mid_{I_\mathfrak{p}}$ because $\chi_1\chi_2 = \epsilon$, which is unramified at $\mathfrak{p}$. If E has good reduction at $\mathfrak{p}$ then the action of $I_\mathfrak{p}$ on $E[N]$ is trivial. If E has multiplicative reduction at $\mathfrak{p}$ then E is isomorphic, over an unramified extension of $K_\mathfrak{p}$ (which makes no difference when we restrict to $I_\mathfrak{p}$), to the Tate curve E_q, with $E_q(\overline{K_\mathfrak{p}}) \simeq \overline{K_\mathfrak{p}}^\times/q^\mathbb{Z}$, where q is the Tate parameter. Now $E_q[N] \simeq (\mu_N \times \langle q^{1/N}\rangle)/q^\mathbb{Z}$ has a submodule μ_N on which $\mathrm{Gal}(\overline{K_\mathfrak{p}}/K_\mathfrak{p})$ acts via ϵ (whose restriction to $I_\mathfrak{p}$ is trivial), and a quotient the image of $\langle q^{1/N}\rangle$ (on which $\mathrm{Gal}(\overline{K_\mathfrak{p}}/K_\mathfrak{p})$ acts via the trivial character). So in both cases, of good or multiplicative reduction, $\chi_1 \mid_{I_\mathfrak{p}}$ is trivial. Similarly, if the reduction at $\mathfrak{p}$ is bad but potentially multiplicative then $\chi_1 \mid_{I_\mathfrak{p}}$ has order 2 (which divides r, since r is necessarily even). Finally, if the reduction at $\mathfrak{p}$ is bad but potentially good then, using a theorem of Serre and Tate [ST], as in [Se, 5.6], $\chi_1 \mid_{I_\mathfrak{p}}$ could have order $2, 3, 4$ or 6 (the possible orders of non-trivial automorphisms of an elliptic curve), but since $\mid \mathbb{F}_N^\times \mid = N-1$, the only possibilities are divisors of g.c.d.$(N-1, 12)$. □

Corollary 3.3. *The character χ_1^r is unramified away from $\mathfrak{q}$, while $\chi_1^r \mid_{I_\mathfrak{q}} = \theta_\mathfrak{q}^r$. The character χ_2^r is unramified away from $\overline{\mathfrak{q}}$, while $\chi_2^r \mid_{I_{\overline{\mathfrak{q}}}} = \theta_{\overline{\mathfrak{q}}}^r$.*

4. Congruences for units

Theorem 4.1. *For a prime $N > 5$, let $K/\mathbb{Q}$ be a quadratic extension such that K is the field of definition of some point P on $Y_0(N)$ mapping to $Y_0^+(N)(\mathbb{Q})$. Suppose that P can be represented by (E, C), where E/K is an elliptic curve without complex multiplication, and with good reduction at primes dividing N. If u is any unit in O_K and $(N) = \mathfrak{q}\overline{\mathfrak{q}}$, then $u^r \equiv 1 \pmod{\mathfrak{q}}$ and $u^r \equiv 1 \pmod{\overline{\mathfrak{q}}}$, i.e. $u^r \equiv 1 \pmod{N}$, where $r :=$ g.c.d.$(N-1, 12)$.*

Proof. The character $\chi_1 : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathbb{F}_N^\times$ factors through the abelianisation of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ hence, by global class field theory, through $\mathbb{A}_K^\times/K^\times$, necessarily killing the connected components $\mathbb{R}_{>0}$ at real places and $\mathbb{C}^\times$ at complex places (embedded in $\mathbb{A}_K^\times$ with 1 at all other places). Now $\chi_1^r : \mathbb{A}_K^\times/K^\times \to \mathbb{F}_N^\times$ is trivial on every local $O_\mathfrak{p}^\times$ for $\mathfrak{p} \neq \mathfrak{q}$, by Corollary 3.3, since this $O_\mathfrak{p}^\times$ (embedded in $\mathbb{A}_K^\times$ with 1 at all other places) is the image of the abelianisation of $I_\mathfrak{p}$ under the global reciprocity map. By [Se, Proposition 3], if $g \in I_\mathfrak{q}$ maps to $s \in O_\mathfrak{q}^\times$ under the local reciprocity map, then $\theta_\mathfrak{q}(g) = \overline{s}^{-1}$ in $\mathbb{F}_N^\times$, where 'bar' stands for the reduction mod $\mathfrak{q}$.

Viewing χ_1^r as a character from $\mathbb{A}_K^\times$ to $\mathbb{F}_N^\times$, killing $K^\times$, it must kill u. But χ_1^r is trivial at all the real and complex places, and at all finite $\mathfrak{p} \neq \mathfrak{q}$, u lies in $O_\mathfrak{p}^\times$, on which χ_1^r is trivial. It follows then that for the local component $\chi_{1,\mathfrak{q}}^r$ at $\mathfrak{q}$ of χ_1^r, one has $\chi_{1,\mathfrak{q}}^r(u) = 1$. On the other hand, by Corollary 3.3 and the above, one also has $\chi_{1,\mathfrak{q}}^r(u) = \overline{u^{-r}}$. Hence $u^r \equiv 1 \pmod{\mathfrak{q}}$. To prove the congruence mod $\overline{\mathfrak{q}}$, we apply the same argument with χ_2 in place of χ_1. It can also be deduced from the congruence mod $\mathfrak{q}$ by applying σ and using $u^\sigma = \pm u^{-1}$. □

As already remarked, $2 \mid r$. In the special case $2 = r$, which is equivalent to $N \equiv 11 \pmod{12}$, we will have $u \equiv \pm 1 \pmod{\mathfrak{q}}$. Note that r need not be the smallest positive integer m such that $u^m \equiv 1 \pmod{N}$ for all units. In the example in §5.2 below, where $N = 43$, we have $r = 6$ but $m = 2$.

The above theorem is really only of interest when K is real quadratic, since when K is imaginary quadratic the only units satisfy $u^r = 1$. The interest of the imaginary quadratic case is in a different phenomenon, involving the appearance of N in the values of L-functions of certain Hecke characters. We explain this from §7 onwards.

The condition that E/K be without complex multiplication is easy to verify in practice. Berwick gave a list of all 14 quadratic fields generated by j-invariants of elliptic curves with complex multiplication [B]. They are $\mathbb{Q}(\sqrt{m})$ with $m = 2, 3, 5, 6, 7, 13, 17, 21, 29, 33, 37, 41, 61$ or 89.

The Weierstrass equation $y^2 = x^3 - 27j(j-1728)x + 54j(j-1728)^2$ has j-invariant j. It also has discriminant $\Delta = j^2(j-1728)^3$, so defines an elliptic curve with good reduction at primes dividing N as long as the norms of j and $j-1728$ are not divisible by N.

For us N is prime, but we could modify the proof to work for general square-free N, proving congruences modulo prime divisors of q, a prime number dividing N, with $q > 5$ and r now g.c.d.$(q-1, 12)$. According to Quer [Q, Table 4] there are eight square-free values of N for which $X_0(N)/W_N$ has genus zero, which guarantees the existence of infinitely many quadratic $\mathbb{Q}$-curves of degree N. They are $N = 6, 10, 14, 15, 21, 26, 35$ and 39. For all $q \mid N$ here we have $r = q-1$, so that automatically $u^r \equiv 1 \pmod{\mathfrak{q}}$, and the theorem does not give us anything interesting.

5. Examples

5.1. $X_0^+(N)$ **genus zero.** Let $X_0^+(N)$ be the nonsingular projective curve birational to $Y_0^+(N)$. It has genus zero for precisely the following prime values of $N \equiv 11 \pmod{12}$: $11, 23, 47, 59, 71$. González and Lario [GoL] showed how to obtain a rational parametrisation of $Y_0^+(N)$, working out the cases $N = 11$ and $N = 23$ in detail. Quer used their method to work out the details for all cases, giving a polynomial $f(t) \in \mathbb{Z}[t]$ [Q, Table 1] such that if $t \in \mathbb{Q}$ represents a rational point $P \in Y_0^+(N)(\mathbb{Q})$ then the Galois conjugate points in the inverse image on $Y_0(N)$ are defined over $K = \mathbb{Q}(\sqrt{f(t)})$.

(1) When $N = 11$ we use González and Lario's rational parametrisation of $Y_0^+(N)$, for which $f(t) = (6+t)(t^3 - 2t^2 - 76t - 212)$, since they also tell us that j, j^σ are roots of $x^2 - J_1 x + J_2$, where

$$J_1 = 8720000 + 19849600t + 8252640t^2 - 1867712t^3 - 1675784t^4 - 184184t^5$$
$$+57442t^6 + 11440t^7 - 506t^8 - 187t^9 + t^{11},$$
$$J_2 = (38800 + 21920t + 4056t^2 + 248t^3 + t^4)^3.$$

When $t = -8$ we find $K = \mathbb{Q}(\sqrt{122})$ and $(11) = \mathfrak{q}\bar{\mathfrak{q}}$, with $\mathfrak{q} = (11, \sqrt{122} - 1)$, $\bar{\mathfrak{q}} = (11, \sqrt{122} + 1)$. The norms of j and $j - 1728$ are $2^{12}3^6$ and $2^{14}3^{16}$, respectively. The fundamental unit $u = 11 - \sqrt{122}$ is clearly $\equiv -1 \pmod{\mathfrak{q}}$ and $1 \pmod{\bar{\mathfrak{q}}}$.

When $t = -9$ we find $K = \mathbb{Q}(\sqrt{1257})$, and the norms of j and $j - 1728$ are $-5^6 167^3$ and 2322647^2, respectively. (Note that the fact that the norm of j is a cube (when $N \equiv 2 \pmod 3$) also follows from [Go, Proposition 1.2].) Using the computer package Magma we find a fundamental unit $u = 101399 - 2860\sqrt{1257}$. Since $101399 \equiv 1 \pmod{11}$ and $2860 \equiv 0 \pmod{11}$, visibly $u \equiv 1 \pmod{\mathfrak{q}\bar{\mathfrak{q}}}$.

(2) When $N = 59$, Quer's $f(t) = (t^3 - t^2 - t - 2)(t^9 - 7t^8 + 16t^7 - 21t^6 + 12t^5 - t^4 - 9t^3 + 6t^2 - 4t - 4)$. Letting $t = -2$, $K = \mathbb{Q}(\sqrt{47968})$. A fundamental unit is

$$u = 2767242120542753585032568410 1 - 50539547041025801957952897 0\sqrt{47968}.$$

Since $27672421205427535850325684101 \equiv -1 \pmod{59}$ and $-505395470410258019579528970 \equiv 0 \pmod{59}$, we see directly that $u \equiv -1 \pmod{\mathfrak{q}\bar{\mathfrak{q}}}$. In this case we did not calculate the j-invariant.

One easily checks that (in cases where $u \equiv \pm 1 \pmod{N}$), $b \equiv 0 \pmod{N}$ when $\mathrm{Norm}_{K/\mathbb{Q}} = 1$, while $a \equiv 0 \pmod{N}$ when $\mathrm{Norm}_{K/\mathbb{Q}} = -1$.

5.2. $X_0^+(N)$ **genus one.** $X_0^+(N)$ has genus 1 for the following prime values of N: $37, 43, 53, 61, 79, 83, 89, 101, 131$. Yamauchi worked out an equation for the canonical embedding in $\mathbb{P}^2$ of the genus 3 curve $X_0(43)$. A dehomogenisation is

$$x^4 + 10x^2y^2 + 21y^4 + 4x^2y + 52y^3 + 2x^2 - 26y^2 + 20y - 3 = 0.$$

He also showed that $X_0^+(43)$ is the elliptic curve $s^2 + s = t^3 + t^2$, and that the quotient morphism of degree two is given by $t = \frac{y}{1-y}$, $s = \frac{x^2+3y^2+6y-1}{4(y-1)^2}$ [Y]. Rearranging, $y = \frac{t}{1+t}$ and $x^2 = 4s(y-1)^2 - 3y^2 - 6y + 1$, which can be expressed in terms of s and t.

If (t, s) is a rational point on $X_0^+(43)$ then its inverse image points on $X_0(43)$ are defined over $K = \mathbb{Q}(\sqrt{x^2})$. Plotting $x^2 = 0$ as a curve in the (t, s)-plane, we can identify the region $x^2 > 0$, and find that only a small portion of the curve $s^2 + s = t^3 + t^2$ (approximately for $s > 0$ and $-0.7 \le t \le 0.2$) lies inside it. The Mordell-Weil group $X_0^+(43)(\mathbb{Q})$ is generated by $P := (0, 0)$, and the first positive multiple for which $x^2 > 0$ is $12P = \left(\frac{-3629}{7569}, \frac{71117}{658503}\right)$. This gives $x^2 = \frac{37\cdot 79\cdot 29611}{2^4 5^2 197^2}$, so $K = \mathbb{Q}(\sqrt{37 \cdot 79 \cdot 29611}) = \mathbb{Q}(\sqrt{d})$, where $d = 86552953$. Using the long formulas in [Y, Section 2], the points on $X_0(43)(K)$ mapping to $12P$ represent elliptic curves with j-invariants

$$(-756085166179320265296984452968269379228116825502930471115222326067869$$
$$73125 \pm 812699088738328883317660839595404939890770971787509297042962213 03$$
$$39500\sqrt{86552953})/969180887103306711282438050172566448361641654073 0367659.$$

Since the norms of j and $j - 1728$ are

$$\frac{5^6 7^2 71^3 644047036117^3 33370009^3 2459^3}{19^{44}} \text{ and}$$
$$\frac{23^4 71^2 125992149329030121192353^2 737471659^2 1931^2}{19^{44}}$$

respectively, we have good reduction at primes dividing 43. (For more on the cubes in the norm of j, see [Go].)

Using Magma we find a fundamental unit of the form $u = a + b\sqrt{d}$, where a and b each have around 2800 digits, with $a \equiv -1 \pmod{43}$ and $b \equiv 0 \pmod{43}$, so that $u \equiv -1 \pmod{43}$. As already remarked, Theorem 4.1 only gives us $u^6 \equiv 1 \pmod{43}$, whereas in fact $u^2 \equiv 1 \pmod{43}$.

5.3. $X_0^+(N)$ **genus** > 1**.** There are only five known examples of $\mathbb{Q}$-rational points on $Y_0^+(N)$ where N is prime and the genus of $X_0^+(N)$ is greater than 1. The values of N are $73, 103, 137, 191$ and 311. These examples were discovered by Galbraith [Ga], and those for $N = 73, 103$ and 191 independently by Elkies. Only for $N = 103, 191$ or 311 is K real quadratic.

(1) When $N = 191$, $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{61 \cdot 229 \cdot 145757})$. In O_K we have $(191) = \mathfrak{q}\bar{\mathfrak{q}}$, with $\mathfrak{q} = (191, \sqrt{d} - 54)$, $\bar{\mathfrak{q}} = (191, \sqrt{d} + 54)$. The factorisations of the norms of j and $j - 1728$ given in [Ga, Table 1] do not involve the prime 191, so we may choose E/K within its $\overline{K}$-isomorphism class to have good reduction at $\mathfrak{q}$ and $\bar{\mathfrak{q}}$. Using Magma we find a fundamental unit of the form $u = a + b\sqrt{d}$, where a and b have 158 and 153 digits respectively,

$a \equiv 0 \pmod{191}$ and $b \equiv 46 \pmod{191}$. Since $46 \cdot 54 \equiv 1 \pmod{191}$, we have $u \equiv 1 \pmod{\mathfrak{q}}$, and similarly $u \equiv -1 \pmod{\overline{\mathfrak{q}}}$.

(2) When $N = 311$, $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{11 \cdot 17 \cdot 9011 \cdot 23629})$. In O_K we have $(311) = \mathfrak{q}\overline{\mathfrak{q}}$, with $\mathfrak{q} = (311, \sqrt{d}-42), \overline{\mathfrak{q}} = (311, \sqrt{d}+42)$. Again, E has good reduction at $\mathfrak{q}$ and $\overline{\mathfrak{q}}$. A fundamental unit is $u = a + b\sqrt{d}$, where a and b each have just under 3000 digits, $a \equiv 1 \pmod{311}$ and $b \equiv 0 \pmod{311}$, so $u \equiv 1 \pmod{\mathfrak{q}\overline{\mathfrak{q}}}$.

(3) When $N = 103$, $K = \mathbb{Q}(\sqrt{2885})$, $(103) = \mathfrak{q}\overline{\mathfrak{q}}$ with $\mathfrak{q} = (103, \sqrt{2885} - 1)$, $\overline{\mathfrak{q}} = (103, \sqrt{2885} + 1)$, E has good reduction at $\mathfrak{q}$ and $\overline{\mathfrak{q}}$, and a fundamental unit is $u = (11011 - 205\sqrt{2885})/2$. One finds that $u \equiv 47 \pmod{\mathfrak{q}}$ and $u \equiv 46 \pmod{\overline{\mathfrak{q}}}$, so something appears to be wrong, but then we recall the condition $N \equiv 11 \pmod{12}$, which, though holding for $N = 191$ and $N = 311$, is not satisfied by $N = 103$, for which g.c.d.$(N - 1, 12) = 6$. So Theorem 4.1 only gives us $u^6 \equiv 1 \pmod{\mathfrak{q}\overline{\mathfrak{q}}}$ (with $\chi_1 |_{I_\mathfrak{p}}$ of order 3 or 6 for at least one prime $\mathfrak{p}$ of bad but potentially good reduction). One checks directly that $47^6 \equiv 1 \pmod{103}$ and $46^3 \equiv 1 \pmod{103}$. We have g.c.d.$(N - 1, 12) = 6$ also in the case $N = 43$ above, but that time we were lucky.

6. Modular forms with nebentypus, and $\mathbb{Q}$-abelian varieties with everywhere good reduction

Let $D > 1$ be a square-free integer with $D \equiv 1 \pmod 4$. Let $\chi_D : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ be the unique primitive quadratic character mod D (so $\chi_D(-1) = 1$), and let $K = \mathbb{Q}(\sqrt{D})$, $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle$. Let $f = \sum_{n=1}^{\infty} a_n q^n \in S_2(\Gamma_0(D), \chi_D)$ be a normalised, new, Hecke eigenform, and let $F = \mathbb{Q}(\{a_n\})$. Shimura [Sh, Section 7.7] proved that F is a CM field. Let F' be its totally real subfield, and $\mathrm{Gal}(F/F') = \langle \rho \rangle$. He also constructed an abelian variety $A/\mathbb{Q}$, of dimension $[F : \mathbb{Q}]$, naturally associated to f, with an injection from F into $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$. This A is isogenous to a factor of the jacobian of the modular curve $X_1(D)$, and may be chosen (in its isogeny class) so that the ring of integers O_F injects into $\mathrm{End}_{\mathbb{Q}}(A)$. Shimura constructed an abelian subvariety B, defined over K, such that A is isogenous over K to $B \times B^\sigma$, and $O_{F'}$ preserves B. Furthermore, if $x \in O_F$ with $x \neq 0$ and $x^\rho = -x$ then inside A, x gives an isogeny from B to B^σ, so B is a "$\mathbb{Q}$-abelian variety". Let $\mathfrak{b}$ be the ideal of O_F generated by $\{x \in O_F \mid x^\rho = -x\}$, $\mathfrak{c} = \mathrm{Norm}_{F/F'}(\mathfrak{b})$, and let $\lambda \mid \mathfrak{b}$ be a prime ideal dividing an odd rational prime q (if such a prime ideal exists). Then $\lambda' := \mathrm{Norm}_{F/F'}(\lambda)$ is a prime ideal of $O_{F'}$, with $O_F\lambda' = \lambda^2$ (see [Sh], just after Remark 7.28').

Shimura proved that B has good reduction at all primes of O_K not dividing D. Casselman [Ca] proved that in fact B has good reduction at *all* primes of O_K, for the examples examined by Shimura, namely $D = 29, 37, 41$ (for which B is an elliptic curve), $D = 53, 61, 73$ (for which B is an abelian surface) and $D = 89, 97$ (for which B is an abelian three-fold). See the table on p. 207 of [Sh]. In the general case, Deligne and Rapoport showed [DR, V.3.7(iii)] that a certain subfactor of the jacobian of $X_1(D)$ (take their H to be the kernel of χ_D) has good reduction at all primes of O_K. Since B is isogenous to a factor in the isogeny decomposition of this subfactor, it then follows from the criterion of Néron-Ogg-Shafarevich [ST, Theorem 1] that B too has everywhere good reduction. The elliptic curve for $D = 29$ was discovered independently by Tate (via a Weierstrass equation) and studied by Serre

[Se, 5.10]. The abelian surface for $D = 53$ has been realised as the jacobian of an explicitly given curve of genus 2, and good reduction proved directly, by Dembélé and Kumar [DK]. We should mention that Shimura's purpose in [Sh, Section 7.7] is the explicit construction of ray class fields of real quadratic fields.

Ohta proved [O, Theorem 2] that if u_0 is a fundamental unit of K, chosen totally positive if $\mathrm{Norm}_{K/\mathbb{Q}}(u_0) = 1$, then $\mathrm{Norm}_{K/\mathbb{Q}}(u_0 - 1) \equiv 0 \pmod{q}$, from which it easily follows that $u \equiv \pm 1 \pmod{\mathfrak{q}}$ for any prime divisor of q in O_K. This was observed experimentally by Shimura (see just before Proposition 7.34 in [Sh]). A nice example is $D = 97$, for which $q = 467$. A fundamental unit is $u = 5604 - 569\sqrt{97} \equiv 0 - 569 \cdot 87 \equiv -1 \pmod{\mathfrak{q}}$, where $\mathfrak{q} = (467, \sqrt{97} - 87)$.

Our proof of Theorem 4.1 employs essentially the same argument as Ohta. In place of our χ_1, he considers the character by which $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ acts on the one-dimensional $\mathbb{F}_{\lambda'}$-vector space $B(\overline{\mathbb{Q}}) \cap A[\lambda]$. For the determination of the restriction to $I_{\mathfrak{q}}$ in terms of fundamental characters, he uses results of Raynaud [Ra] in place of [Se, Proposition 11], which is specific to one-parameter formal groups so applies only to elliptic curves. It is not necessary to worry about the restriction to $I_{\mathfrak{p}}$ for $\mathfrak{p} \neq \mathfrak{q}$, thanks to the everywhere good reduction. His argument for q not being inert in K is different.

Note that the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the 2-dimensional $\mathbb{F}_\lambda$-vector space $A[\lambda]$ has dihedral image. For a converse of Ohta's theorem, identifying divisors of $\mathrm{Norm}_{K/\mathbb{Q}}(u_0 - 1)$ as the characteristics of dihedral residual representations, and generalisations to higher weights and non-primitive quadratic characters, see the work of Koike, Hida, and Brown and Ghate [Ko, Hi1, BG]. It is known, by theorems of Khare-Wintenberger and Ribet, [KW, Corollary 10.2(i)], [Ri2, Theorem 6.1] that every $\mathbb{Q}$-curve "is modular", yet our Theorem 4.1 cannot be a corollary of [BG, Theorem 2.1], for at least two reasons. Theorem 4.1 includes cases where $r > 2$, but even in the case $r = 2$, [BG, Theorem 2.1] can apply only to elliptic curves with everywhere potentially good reduction (by [DR, V.3.7(iii)]), hence not, for example, to the curve in §5.2, which has multiplicative reduction at some divisor of 19.

7. Congruences with Hecke characters

In the remainder of the paper we concentrate on the case where K is imaginary quadratic. The first part of the following proposition is well-known.

Proposition 7.1. *Let K be an imaginary quadratic field, and let $s = \#O_K^\times$, so that $s = 4$ when $K = \mathbb{Q}(i)$, 6 when $K = \mathbb{Q}(\sqrt{-3})$, and 2 otherwise.*

(1) *There exists a finite extension L of K, and a continuous homomorphism $\tilde{\psi} : \mathbb{A}_K^\times \to L^\times$ such that*
   (a) *$\tilde{\psi}|_{\mathbb{C}^\times}$ and $\tilde{\psi}|_{O_{\mathfrak{p}}^\times}$ (for any finite prime $\mathfrak{p}$) are trivial;*
   (b) *$\tilde{\psi}(\alpha) = \alpha^s$ for all $\alpha \in K^\times$.*

   In other words, $\tilde{\psi}$ is an algebraic Hecke character of type $(s, 0)$. In (a), each local completion is embedded in $\mathbb{A}_K^\times$ by putting 1 in the other components, while in (b), $K^\times$ is embedded diagonally in $\mathbb{A}_K^\times$.

(2) *Suppose that E/K is a quadratic $\mathbb{Q}$-curve of prime degree $N > 5$, without complex multiplication, and with good reduction at the primes $\mathfrak{q}, \overline{\mathfrak{q}}$ dividing N. Let χ_1 and $\mathfrak{q}$ be as at the beginning of §3, and $r = \mathrm{g.c.d.}(N-1, 12)$. Then $s \mid r$. Let λ be a divisor of $\mathfrak{q}$ in L. Define $\psi : \mathbb{A}_K^\times \to L_\lambda^\times$ by $\psi(a) := (\tilde{\psi}(a))^{r/s}/a_{\mathfrak{q}}^r$. Then $\psi|_{K^\times}$ is trivial, and since $\psi|_{\mathbb{C}^\times}$ is also trivial, ψ may be*

identified, by global class field theory, with a character $\psi : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to L_\lambda^\times$*, factoring through the Galois group of the maximal abelian extension of* K*. The image of* ψ *is contained in* $O_\lambda^\times$*, and letting* $\overline{\psi} : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathbb{F}_\lambda^\times$ *be the reduction, we may choose* ψ *so that*

$$\overline{\psi} = \chi_1^r.$$

Proof. (1) Having specified condition (a), it remains to show that $\tilde{\psi}(\mathfrak{p})$ (i.e. $\tilde{\psi}(\pi_{\mathfrak{p}})$, which is independent of the choice of uniformiser $\pi_{\mathfrak{p}}$), may be chosen, for each finite prime $\mathfrak{p}$, in such a way that (b) also holds. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ represent independent generators of the ideal class group of O_K, with $\mathfrak{p}_i$ of order c_i and $\mathfrak{p}_i^{c_i} = (\beta_i)$, with $\beta_i \in K^\times$. Choosing the $\mathfrak{p}_i$ also to be integral ideals, $\beta_i \in O_K$. We must have $(\tilde{\psi}(\mathfrak{p}_i))^{c_i} = \beta_i^s$ (which is well-defined, independent of the choice of β_i up to a unit), so we set $\tilde{\psi}(\mathfrak{p}_i) = (\beta_i^s)^{1/c_i}$ in some extension of K. Now take $\mathfrak{p}$ a prime ideal different from the $\mathfrak{p}_i$. Then there exist $a_i \in \mathbb{Z}$ and $\gamma \in K^\times$ such that $\mathfrak{p} = (\prod_{i=1}^t \mathfrak{p}_i^{a_i})(\gamma)$, so we set $\tilde{\psi}(\mathfrak{p}) = (\prod_{i=1}^t (\tilde{\psi}(\mathfrak{p}_i))^{a_i})\gamma^s$, which again is well-defined, and clearly leads to (b) being satisfied.

(2) By Proposition 3.1, N splits in O_K, so $N \equiv 1 \pmod 4$ if $K = \mathbb{Q}(i)$ and $N \equiv 1 \pmod 3$ if $K = \mathbb{Q}(\sqrt{-3})$. Since also N is odd, it is now easy to see that $s \mid r$. If $a \in K^\times$ then $\psi(a) := (\tilde{\psi}(a))^{r/s}/a_{\mathfrak{q}}^r = a^r/a^r = 1$, as required. If in the proof of (1) we choose the $\mathfrak{p}_i$ to be different from $\mathfrak{q}$, we see that all the $\tilde{\psi}(\mathfrak{p})$ are integral at λ.

Because of the choices of the $(\beta_i^s)^{1/c_i}$, $\tilde{\psi}$ is in general not unique, but may be adjusted by a character of the class group of O_K. At any finite prime $\mathfrak{p}$, the abelianisation of the inertia group, $I_{\mathfrak{p}}^{\mathrm{ab}}$, is identified with the image, under the Artin map, of $O_{\mathfrak{p}}^\times$ (embedded in $A_K^\times$ with 1 at all the other components). Since $\tilde{\psi}|_{O_{\mathfrak{q}}^\times}$ is trivial, by (1)(a), $\overline{\psi}|_{I_{\mathfrak{q}}}$ maps $s \in O_{\mathfrak{q}}^\times$ to $\overline{s}^{-r}$ and so by [Se, Proposition 3] (already referred to in the proof of Theorem 4.1), $\overline{\psi}|_{I_{\mathfrak{q}}} = \theta_{\mathfrak{q}}^r$. By Corollary 3.3, $\overline{\psi}/\chi_1^r : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathbb{F}_\lambda^\times$ is everywhere unramified, hence identifiable with a character of the class group. Since such a character lifts to $L_\lambda^\times$, we may choose a different ψ if necessary, to ensure that $\overline{\psi} = \chi_1^r$.

□

8. The Bloch-Kato conjecture

Consider $\tilde{\psi} : \mathbb{A}_K^\times \to L^\times$ as in Proposition 7.1. From now on we assume that $r = 2$, i.e. that $N \equiv 11 \pmod{12}$ (so also $s = 2$). We use the same notation as in the previous section. Consider the L-function

$$L(\tilde{\psi}, s) = \prod_{\mathfrak{p}} (1 - \tilde{\psi}(\mathfrak{p})(\mathrm{N}\mathfrak{p})^{-s})^{-1},$$

where the product is over all prime ideals $\mathfrak{p}$ of O_K. We may also write $L(\tilde{\psi}, s) = \sum_{\mathfrak{a}} \tilde{\psi}(\mathfrak{a})(\mathrm{N}\mathfrak{a})^{-s}$, where the sum is over all non-zero integral ideals of O_K. For $\mathfrak{p} \neq \mathfrak{q}$ the Euler factor at $\mathfrak{p}$ is $(1 - \psi^{-1}(\mathrm{Frob}_{\mathfrak{p}}^{-1})(\mathrm{N}\mathfrak{p})^{-s})^{-1}$, in fact $L(\tilde{\psi}, s)$ is the L-function attached to the λ-adic representation ψ^{-1} of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, or equivalently $\mathrm{Ind}_K^{\mathbb{Q}}(\psi^{-1})$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If K has discriminant $-D$ then by a theorem of Hecke, for which a convenient reference is [Hi2, Theorem 5.1.4], $\sum_{\mathfrak{a}} \tilde{\psi}(\mathfrak{a})q^{\mathrm{N}\mathfrak{a}}$ is the q-expansion of a cusp form of weight $k = 3 = r + 1$ for $\Gamma_1(D)$, with character χ_K, i.e. the Legendre symbol $\left(\frac{-D}{\cdot}\right)$. Fixing $\tilde{\psi}$, we call this form f. If Σ is a finite set of prime numbers, we put $L_\Sigma(\tilde{\psi}, s) = \prod_{\mathfrak{p} \notin \Sigma_K} (1 - \tilde{\psi}(\mathfrak{p})(\mathrm{N}\mathfrak{p})^{-s})^{-1}$, where Σ_K is the set of prime divisors in O_K of primes in Σ. We shall assume that Σ contains all the prime divisors of D, and that it does not contain N.

Attached to $\tilde{\psi}$ is a "premotivic structure" $M_{\tilde{\psi}}$ over $\mathbb{Q}$ with coefficients in L. Thus there are 2-dimensional L-vector spaces $M_{\tilde{\psi},B}$ and $M_{\tilde{\psi},\mathrm{dR}}$ (the Betti and de Rham realisations) and, for each finite prime λ of O_L, a 2-dimensional L_λ-vector space $M_{\tilde{\psi},\lambda}$, the λ-adic realisation. These come with various structures and comparison isomorphisms, such as $M_{\tilde{\psi},B} \otimes_L L_\lambda \simeq M_{\tilde{\psi},\lambda}$. See [DFG, 1.1.1] for the precise definition of a premotivic structure. In our case the premotivic structures come from elliptic curves with complex multiplication, as described in [Ka, 15.7], see also [Sch, I.4.1.3]. Note that those are premotivic structures over K, but we are restricting the field of definition from K to $\mathbb{Q}$, turning rank-1 into rank-2. Though temporarily λ has denoted any finite prime of O_L, from now on we are only interested in the particular choice of λ in the previous section. The λ-adic realisation $M_{\tilde{\phi},\lambda}$ comes with a continuous linear action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This is by $\mathrm{Ind}_K^{\mathbb{Q}}(\psi^{-1})$.

On $M_{\tilde{\psi},B}$ there is an action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, and the eigenspaces $M^{\pm}_{\tilde{\psi},B}$ are 1-dimensional. On $M_{\tilde{\psi},\mathrm{dR}}$ there is a decreasing filtration, with F^j a 1-dimensional space precisely for $1 \leq j \leq k-1 = 2$. The de Rham isomorphism $M_{\tilde{\psi},B} \otimes_L \mathbb{C} \simeq M_{\tilde{\psi},\mathrm{dR}} \otimes_L \mathbb{C}$ induces isomorphisms between $M^{\pm}_{\tilde{\psi},B} \otimes \mathbb{C}$ and $(M_{\tilde{\psi},\mathrm{dR}}/F) \otimes \mathbb{C}$, where $F := F^1 = F^2$. Define $\Omega^{\pm}$ to be the determinants of these isomorphisms. These depend on the choice of L-bases for $M^{\pm}_{\tilde{\psi},B}$ and $M_{\tilde{\psi},\mathrm{dR}}/F$, so should be viewed as elements of $\mathbb{C}^\times/L^\times$. For $1 \leq j \leq 2$, the Tate-twisted premotivic structure $M_{\tilde{\psi}}(j)$ is *critical* (i.e. the above map *is* an isomorphism, with $F = F^j$), and its Deligne period c^+ (see [De]) is $(2\pi i)^j \Omega^{(-1)^j}$. Deligne's conjecture for $M_{\tilde{\psi}}(j)$, known in this case, asserts then that $L(\tilde{\psi}, j)/(2\pi i)^j \Omega^{(-1)^j}$ is an element of L. The points $j = 1$ and $j = 2$ are paired by the functional equation, and we shall concentrate on $j = 2$.

We would like to choose L-bases for $M_{\tilde{\psi},B}$ and $M_{\tilde{\psi},\mathrm{dR}}$, to pin down $\Omega := \Omega^+$ locally at λ. We shall choose $O_{(\lambda)}$-lattices $\mathcal{M}_{\tilde{\psi},B}$ in $M_{\tilde{\psi},B}$ and $\mathcal{M}_{\tilde{\psi},\mathrm{dR}}$ in $M_{\tilde{\psi},\mathrm{dR}}$. (Here $O_{(\lambda)}$ is a localisation, not a completion.) We get these from the integral structures described in [Ka, 15.7]. With these choices it is still natural to talk of an element "$L_\Sigma(\tilde{\psi}, 2)/(2\pi i)^2\Omega$" of $L_\lambda^\times/O_\lambda^\times$, and the Bloch-Kato conjecture predicts its order at λ.

A comparison isomorphism identifies $\mathcal{M}_{\tilde{\psi},\lambda} := \mathcal{M}_{\tilde{\psi},B} \otimes O_\lambda$ with a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable O_λ-lattice in $M_{\tilde{\psi},\lambda}$. For ease of notation we now let $\tilde{V} := M_{\tilde{\psi},\lambda}$, $\tilde{T} := \mathcal{M}_{\tilde{\psi},\lambda}$, and $\tilde{W} := \tilde{V}/\tilde{T}$.

Following [BK, Section 3], for $p \neq N$ and $j \in \mathbb{Z}$, let

$$H^1_f(\mathbb{Q}_p, \tilde{V}(j)) = \ker\bigl(H^1(D_p, \tilde{V}(j)) \to H^1(I_p, \tilde{V}(j))\bigr).$$

Here D_p is a decomposition subgroup at a prime above p, I_p is the inertia subgroup, and $\tilde{V}(j)$ is a Tate twist of $\tilde{V}$. The cohomology is for continuous cocycles and coboundaries. For $p = N$ (which is the rational prime that λ divides) let

$$H^1_f(\mathbb{Q}_N, \tilde{V}(j)) = \ker\bigl(H^1(D_N, \tilde{V}(j)) \to H^1(D_N, \tilde{V}(j) \otimes_{\mathbb{Q}_N} B_{\mathrm{crys}})\bigr).$$

(See [BK, Section 1] for the definition of Fontaine's ring B_{crys}.) There is a natural exact sequence

$$0 \longrightarrow \tilde{T}(j) \longrightarrow \tilde{V}(j) \xrightarrow{\pi} \tilde{W}(j) \longrightarrow 0.$$

Let $H^1_f(\mathbb{Q}_p, \tilde{W}(j)) = \pi_* H^1_f(\mathbb{Q}_p, \tilde{V}(j))$. Define the λ-Selmer group $H^1_\Sigma(\mathbb{Q}, \tilde{W}(j))$ to be the subgroup of elements of $H^1(\mathbb{Q}, \tilde{W}(j))$ whose local restrictions lie in $H^1_f(\mathbb{Q}_p, \tilde{W}(j))$ for all primes $p \notin \Sigma$. Recall that Σ is a finite set of primes, containing all the prime divisors of D, but not containing N.

The following is a reformulation of the λ-part of the Bloch-Kato conjecture, as in (59) of [DFG], similarly using the exact sequence in their Lemma 2.1.

Conjecture 8.1 (Case of λ-part of Bloch-Kato)**.**

$$\text{ord}_\lambda\left(\frac{L_\Sigma(\tilde{\psi}, 2)}{(2\pi i)^2\Omega}\right) = \text{ord}_\lambda\left(\frac{\text{Tam}^0_\lambda(\tilde{W}(2))\ \#H^1_\Sigma(\mathbb{Q}, \tilde{W}(1))}{\#H^0(\mathbb{Q}, \tilde{W}(1))}\right). \tag{1}$$

We omit the definition of the Tamagawa factor $\text{Tam}^0_\lambda(\tilde{W}(2))$, but note that (since $N > k = 3$), its triviality is a direct consequence of [BK, Theorem 4.1(iii)]. It is also easy to see that $H^0(\mathbb{Q}, \tilde{W}(1))$ is trivial, so in fact the conjecture predicts that

$$\text{ord}_\lambda\left(\frac{L_\Sigma(\tilde{\psi}, 2)}{(2\pi i)^2\Omega}\right) = \text{ord}_\lambda(\#H^1_\Sigma(\mathbb{Q}, \tilde{W}(1))).$$

Note that if A is a finite O_λ-module then $\#A$ denotes its Fitting ideal.

Proposition 8.2.

$$\text{ord}_\lambda\left(\frac{L_\Sigma(\tilde{\psi}, 2)}{(2\pi i)^2\Omega}\right) \geq \text{ord}_\lambda(\#H^1_\Sigma(\mathbb{Q}, \tilde{W}(1))).$$

This follows from results of Kato [Ka, Proposition 14.21(2), 15.23], which rely on earlier work of Rubin [Ru]. Note that our λ is one of the "almost all" primes in [Ka, 15.23], since $\tilde{T}/\lambda\tilde{T}$ is an irreducible representation of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

9. Construction of an element in a Selmer group

Our goal in this section is to construct a non-zero element of $H^1_\Sigma(\mathbb{Q}, \tilde{W}(1))$, for a suitable choice of Σ, using the congruence $\overline{\psi} = \chi_1^2$ from (2) of Proposition 7.1. Recall from §2 the bases $\{e_1, e_2\}$, $\{f_1, f_2\}$ for the N-adic Tate modules $T_N(E), T_N(E^\sigma)$. Consider the free rank-4 $\mathbb{Z}_N$-module $T_N(E) \otimes T_N(E^\sigma)$. This is isomorphic to $\text{Hom}(T_N(E), T_N(E^\sigma))(1)$, where the identification of $T_N(E)$ with $\text{Hom}(T_N(E), \mathbb{Z}_N(1))$, via the Weil pairing, is such that $e_2 : e_1 \mapsto 1,\ e_1 : e_2 \mapsto -1$. Ignoring the Tate twist, $-e_1 \otimes f_1 + Ne_2 \otimes f_2$ is the element of $T_N(E) \otimes T_N(E^\sigma)$ corresponding to the map $T_N(E) \to T_N(E^\sigma)$ induced by ϕ, since $\phi(e_2) = f_1$ and $\phi(e_1) = Nf_2$. (One may also think of this as a projection of the cycle-class of the graph in $H^2(E \times F, \mathbb{Z}_N)(1)$.) Its orthogonal complement, with respect to the bilinear pairing of $T_N(E) \otimes T_N(E^\sigma)$ induced by the Weil pairings (i.e. the intersection pairing on $H^2(E \times F)$), is $\mathfrak{T} := \langle e_1 \otimes f_1 + Ne_2 \otimes f_2, e_2 \otimes f_1, e_1 \otimes f_2 \rangle_{\mathbb{Z}_N}$. With respect to this basis, the action of $g \in \text{Gal}(\overline{\mathbb{Q}}/K)$ (as in §2) on this invariant submodule is by the matrix $\begin{bmatrix} ad + bc & bd & ac/N \\ 2cd & d^2 & c^2/N \\ 2Nab & Nb^2 & a^2 \end{bmatrix}$, c.f. [Gv, Section 3]. By considering the second cohomology of the Weil restriction of scalars (from K to $\mathbb{Q}$) of E (or E^σ), we see that the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ on $T_N(E) \otimes T_N(E^\sigma)$ extends to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. A complex conjugation $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts by switching the factors, using the map induced by the conjugation isomorphism $E \simeq E^\sigma$, which is $(x, y) \mapsto (\overline{x}, \overline{y})$, equivalently $z \pmod{\Lambda} \mapsto \overline{z} \pmod{\overline{\Lambda}}$. This has the effect of swapping each e_i with the corresponding f_i, and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ preserves $\mathfrak{T}$, with σ acting by the matrix $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$.

On $\mathfrak{T}/N\mathfrak{T}$, $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ acts by $\begin{bmatrix} ad & bd & a(c/N) \\ 0 & d^2 & 0 \\ 0 & 0 & a^2 \end{bmatrix}$. Looking also at the matrix by which σ acts, we see that $\mathfrak{T}/N\mathfrak{T}$ is an extension of a 1-dimensional submodule spanned by (the image of) $e_1 \otimes f_1 + Ne_2 \otimes f_2$, by a 2-dimensional quotient. On the submodule, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts via the character $\epsilon\chi_K$, since $ad = \epsilon(g)$ but $\epsilon(\sigma) = -1$, while it follows from the fact that $a^2 = \chi_1^2(g) = \overline{\psi}(g)$ that the quotient is isomorphic to $\mathrm{Ind}_K^{\mathbb{Q}}(\overline{\psi})$. Let T be $\mathfrak{T}$ with the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action multiplied by χ_K. Then T/NT is an extension of ϵ (the cyclotomic character) by $\chi_K \mathrm{Ind}_K^{\mathbb{Q}}(\overline{\psi})$. But $\chi_K \mathrm{Ind}_K^{\mathbb{Q}}(\overline{\psi}) \simeq \mathrm{Ind}_K^{\mathbb{Q}}(\overline{\psi})$, so we have an extension of ϵ by $\mathrm{Ind}_K^{\mathbb{Q}}(\overline{\psi})$. We would like to use this to produce a Galois cohomology class that will give us the required non-zero element of $H^1_\Sigma(\mathbb{Q}, \tilde{W}(1))$. The trouble is, if the extension is trivial then the class will be zero. Before addressing this problem, we need the following lemma.

Lemma 9.1. *The 3-dimensional representation $V := T \otimes_{\mathbb{Z}_N} \mathbb{Q}_N$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is irreducible.*

Proof. Let $V_N(E) := T_N(E) \otimes \mathbb{Q}_N$ and $V_N(E^\sigma) := T_N(E^\sigma) \otimes \mathbb{Q}_N$. If V is not irreducible, then it has a 1-dimensional subquotient, necessarily reducing to ϵ, so a finite order character times the N-adic cyclotomic character. Restricting to $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$, for F sufficiently large, we may remove the finite order character. If the subquotient is a submodule, we get an element of $\mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)}(V_N(E), V_N(E^\sigma))$, not a multiple of the graph of ϕ. By Faltings' Theorem [F, Theorem 4, Corollary 1], there is an isogeny from E to E^σ, defined over F, independent of ϕ, contrary to E not having complex multiplication. If the subquotient is not a submodule, we may apply the same argument to $\mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbb{Q}}/F)}(V_N(E^\sigma), V_N(E))$. □

It now follows, by imitating the proof of a well-known result of Ribet [Ri1, Proposition 2.1], that for *some* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant $\mathbb{Z}_N$-lattice T' in V, T'/NT' is a non-trivial extension of ϵ by $\mathrm{Ind}_K^{\mathbb{Q}}(\overline{\psi})$. In a standard way, this gives us a non-zero class $\gamma \in H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Hom}_{\mathbb{F}_N}(\mathrm{Ind}_K^{\mathbb{Q}}(\overline{\psi}), \epsilon)) \simeq H^1(\mathbb{Q}, \mathrm{Ind}_K^{\mathbb{Q}}(\overline{\psi}^{-1})(1))$. In the notation of the previous section, this is $H^1(\mathbb{Q}, (\tilde{T}/N\tilde{T})(1))$. The inclusion $i : \tilde{T}/N\tilde{T} \hookrightarrow \tilde{W}$ gives us $\delta := i_*(\gamma) \in H^1(\mathbb{Q}, \tilde{W}(1))$, and $\delta \neq 0$ since $H^0(\mathbb{Q}, \tilde{W})$ is trivial.

Theorem 9.2. *Let $\Sigma = \{p \mid D\} \cup \Sigma'$, where $p \in \Sigma' \iff$ no quadratic twist of E/K has good reduction at all divisors of p. Then $d \in H^1_\Sigma(\mathbb{Q}, \tilde{W}(1))$.*

Proof. If $p \neq N$ and $p \notin \Sigma$, then T is unramified at p, i.e. the action of I_p is trivial. (Note that in $T_N(E) \otimes T_N(E^\sigma)$, E may be replaced by a quadratic twist without changing the representation.) Reducing modulo N, I_p acts trivially on T/NT, so clearly γ, and hence δ, is trivial on I_p. It follows that $\mathrm{res}_p(\delta) \in H^1_f(\mathbb{Q}_p, \tilde{W}(1))$, as explained in the proof of [Br, Lemma 7.4]. That $\mathrm{res}_N(\delta) \in H^1_f(\mathbb{Q}_N, \tilde{W}(1))$ is an almost immediate consequence of the second part of [DFG, Proposition 2.2]. $\square$

Corollary 9.3. $\mathrm{ord}_\lambda\left(\frac{L_\Sigma(\tilde{\psi},2)}{(2\pi i)^2\Omega}\right) > 0$.

10. A further example

Revisiting the case $N = 11$ from 5.1(1), putting $t = -3$ gives $K = \mathbb{Q}(\sqrt{-87})$, $j = -34481 + 16588\sqrt{-87}$. The class group of O_K is cyclic of order 6. The Weierstrass equation $y^2 = x^3 - 27j(j-1728)x + 54j(j-1728)^2$ has j-invariant j, $\Delta = j^2(j-1728)^3$, $c_4 = j(j-1728)$ and $c_6 = -j(j-1728)^2$. We find that $\mathrm{Norm}_{K/\mathbb{Q}}(j) = 29^3 101^3$, while $\mathrm{Norm}_{K/\mathbb{Q}}(j-1728) = 131^2 1213^2$. In O_K, $(29) = (29, \sqrt{-87})^2$, $(101) = (101, \sqrt{-87}+32)(101, \sqrt{-87}-32)$, $(131) = (131, \sqrt{-87}+31)(131, \sqrt{-87}-31)$, $(1213) = (1213, \sqrt{-87}+139)(1213, \sqrt{-87}-139)$, and

$$(j) = (29, \sqrt{-87})^3(101, \sqrt{-87}+32)^3,$$
$$(j-1728) = (131, \sqrt{-87}-31)^2(1213, \sqrt{-87}-139)^2.$$

Simultaneously making a quadratic twist and changing the equation, replacing x by ux, y by $u^{3/2}y$, $\Delta \mapsto u^6\Delta$, $c_4 \mapsto u^2 c_4$ and $c_6 \mapsto u^3 c_6$. If $\mathfrak{p}$ is any of the prime ideals $(29, \sqrt{-87}), (101, \sqrt{-87}+32)$, $(131, \sqrt{-87}-31)$ or $(1213, \sqrt{-87}-139)$ (i.e. the possible primes of bad reduction), by choosing u with $\mathrm{ord}_\mathfrak{p}(u) = -1$ we get a quadratic twist with good reduction at $\mathfrak{p}$. So in this case, $\Sigma' = \emptyset$ and $\Sigma = \{3, 29\}$.

If $\mathfrak{p}$ is a prime of O_K such that $\mathfrak{p}^2 = (3)$ or $\mathfrak{p}^2 = (29)$ then $\tilde{\psi}(\mathfrak{p}) = \pm 3$ or ± 29, so the missing Euler factors, evaluated at $s = 2$, are $(1 \pm 3^{-1})^{-1}$ and $(1 \pm 29^{-1})^{-1}$. Since $3 \not\equiv \pm 1 \pmod{11}$ and $29 \not\equiv \pm 1 \pmod{11}$, $\mathrm{ord}_\lambda\left(\frac{L_\Sigma(\tilde{\psi},2)}{(2\pi i)^2\Omega}\right) = \mathrm{ord}_\lambda\left(\frac{L(\tilde{\psi},2)}{(2\pi i)^2\Omega}\right)$, so Corollary 9.3 shows that $\mathrm{ord}_\lambda\left(\frac{L(\tilde{\psi},2)}{(2\pi i)^2\Omega}\right) > 0$.

The computer package Magma has a command "Lratio" which computes the product (over the Galois conjugates of f) of such L-values, divided by some period. In fact it computes this rational number exactly using modular symbols, without having to approximate either the numerator or the denominator; see [St, Theorem 3.41]. In §8 above, we could have used a premotivic structure (and an S-integral premotivic structure) attached to the newform f, constructed using the cohomology of modular curves (hence close to modular symbols), as in [DFG, 1.6.2], instead of that attached to $\tilde{\psi}$ using elliptic curves with complex multiplication. The only difference this might make is that we should substitute a different period Ω' for Ω, but they ought to be the same. See the comment immediately preceding [Ka, 15.12]. The period used by Magma can be related to our Ω' sufficiently well to show that we should see a factor of 11 in the numerator of this Lratio. To justify this, we need conditions that 11 does not divide the class number of O_K (which is true in our case) and that 11 is not a prime of congruence between the Galois conjugacy class of f and its orthogonal complement in $S_3(\Gamma_1(87), \chi_K)$ (which can be checked using Magma). We find that $S_3(\Gamma_1(87), \chi_K)$ is 18-dimensional, and that the Galois conjugacy classes of newforms span subspaces of dimensions 3, 3 and 12. The two subspaces of dimension 3 must account for the 6 unramified algebraic Hecke characters of type $(2, 0)$, of which one is $\tilde{\psi}$, associated with the newform f. One of these subspaces has Lratio $11/2$, the other $1/4$, so f must belong to the first one, and we can check this directly as follows. In O_K, $(17) =$

$\mathfrak{p}\overline{\mathfrak{p}} = (17, \sqrt{-87}-7)(17, \sqrt{-87}+7)$. We find $j \equiv 1 \pmod{\mathfrak{p}}$ and $j \equiv 6 \pmod{\overline{\mathfrak{p}}}$. Using this to reduce the Weierstrass equation for E, we can count the number of points, and find that if $E(\mathbb{F}_{\mathfrak{p}}) = 1 + 17 - a_{\mathfrak{p}}$ then $a_{\mathfrak{p}} = 6$, and similarly $a_{\overline{\mathfrak{p}}} = -6$. Since $a_{\mathfrak{p}} \equiv \chi_1(\mathfrak{p}) + \chi_2(\mathfrak{p}) \equiv \chi_1(\mathfrak{p}) + 17/\chi_1(\mathfrak{p}) \pmod{11}$, we find that $\chi_1(\mathfrak{p}) = -2$ or -3 in $\mathbb{F}_{11}$, while $\chi_1(\overline{\mathfrak{p}}) = 2$ or 3, so $\chi_1^2(\mathfrak{p}) = 4$ or -2. The two 3-dimensional spaces contain newforms with coefficients generating the same cubic field, which has a unique prime divisor of norm 11, modulo which the coefficient $a_{17}(f)$ must be congruent to $\tilde{\psi}(\mathfrak{p}) + \tilde{\psi}(\overline{\mathfrak{p}}) \equiv \chi_1^2(\mathfrak{p}) + 17^2/\chi_1^2(\mathfrak{p}) \equiv 2$. This puts f in the first space, with Lratio 11/2. (For the other one $a_{17}(f)$ would have to be congruent to -2 instead.)

References

[B] W. E. H. Berwick, Modular invariants expressible in terms of quadratic and cubic irrationalities, *Proc. London Math. Soc.* **28** (1927), 53–69.

[BK] S. Bloch, K. Kato, L-functions and Tamagawa numbers of motives, The Grothendieck Festschrift Volume I, 333–400, Progress in Mathematics, 86, Birkhäuser, Boston, 1990.

[BG] A. F. Brown, E. P. Ghate, Dihedral congruence primes and class fields of real quadratic fields, *J. Number Theory* **95** (2002), 14–37.

[Br] J. Brown, Saito-Kurokawa lifts and applications to the Bloch-Kato conjecture, *Compos. Math.* **143** (2007), 290–322.

[Ca] W. Casselman, On Abelian Varieties with Many Endomorphisms and a Conjecture of Shimura's, *Invent. Math.* **12** (1971), 225–236.

[Co] D. A. Cox, *Primes of the form* $x^2 + ny^2$, Wiley, New York, 1989.

[De] P. Deligne, Valeurs de Fonctions L et Périodes d'Intégrales, *AMS Proc. Symp. Pure Math.,* Vol. 33 (1979), part 2, 313–346.

[DR] P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972),* 143–316. Lect. Notes in Math., **349**. Springer, Berlin, 1973.

[DK] L. Dembélé, A. Kumar, Examples of abelian surfaces with everywhere good reduction, preprint, https://homepages.warwick.ac.uk/staff/L.Dembele/paper.html

[DFG] F. Diamond, M. Flach, L. Guo, The Tamagawa number conjecture of adjoint motives of modular forms, *Ann. Sci. École Norm. Sup. (4)* **37** (2004), 663–727.

[E] N. Elkies, On Elliptic K-curves, 81–91 in *Modular Curves and Abelian Varieties*, J. Cremona, J.-C. Lario, J. Quer, K. Ribet, eds., Progress in Mathematics, Vol. 224, Birkhäuser, Basel, 2004.

[F] G. Faltings, Finiteness Theorems for Abelian Varieties over Number Fields. In *Arithmetic Geometry (Storrs, Conn., 1984),* G. Cornell, J. Silverman, eds., 9–27. Springer, New York, 1986.

[Ga] S. Galbraith, Rational points on $X_0^+(p)$, *Experimental Math.* **8** (1999), 311–318.

[Go] J. González, On cubic factors of j-invariants of quadratic $\mathbb{Q}$-curves of prime degree, *J. Number Theory* **128** (2008), 377–389.

[GoL] J. González, J.-C. Lario, Rational and elliptic parametrizations of $\mathbb{Q}$-curves, *J. Number Thoery* **72** (1998), 13–31.

[Gv] V. Golyshev, Classification problems and mirror duality. Surveys in geometry and number theory: reports on contemporary Russian mathematics, 88121, London Math. Soc. Lecture Note Ser., 338, Cambridge Univ. Press, Cambridge, 2007.

[Ha] Y. Hasegawa, $\mathbb{Q}$-curves over quadratic fields, *Manuscripta Math.* **94** (1997), 347–364.

[Hi1] H. Hida, Global quadratic units and Hecke algebras, *Doc. Math.* **3** (1998), 273–284.

[Hi2] H. Hida, *Geometric modular forms and elliptic curves,* World Scientific, Singapore, 2000.

[Ka] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms. Cohomologies p-adiques et applications arithmétiques. III. Astérisque No. 295 (2004), ix, 117290.

[KW] C. Khare, J.-P. Wintenberger, Serre's modularity conjecture (I), *Invent. Math.* **178** (2009), 485–504.

[Ko] M. Koike, Congruences between cusp forms and linear representations of the Galois group, *Nagoya Math. J.* **64** (1976), 63–85.

[O] M. Ohta, The representation of Galois group attached to certain finite group schemes, and its application to Shimura's theory, 149–156 in *Algebraic Number Theory*, Proc. Int. Symp. Kyoto 1976, Japan Soc. Prom. Sci., Tokyo, 1977.

[Q] J. Quer, $\mathbb{Q}$-curves and abelian varieties of GL_2 type, *Proc. London Math. Soc. (3)* **81** (2000), 285–317.

[Ra] M. Raynaud, Schémas en groupes de type $(p,\ldots,p)$, *Bull. Soc. Math. France* **102** (1974), 241–280.

[Ri1] K. Ribet, A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$, *Invent. Math.* **34** (1976), 151–162.

[Ri2] K. Ribet, Abelian Varieties over $\mathbb{Q}$ and Modular Forms, 241–261 in *Modular Curves and Abelian Varieties*, J. Cremona, J.-C. Lario, J. Quer, K. Ribet, eds., Progress in Mathematics, Vol. 224, Birkhäuser, Basel, 2004.

[Ru] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* **103** (1991), 25–68.

[Sch] N. Schappacher, Periods of Hecke characters. Lecture Notes in Mathematics, 1301. Springer-Verlag, Berlin, 1988.

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

[ST] J.-P. Serre, J. Tate, Good reduction of abelian varieties, *Ann. of Math.* **88** (1968), 492–517.

[Sh] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions,* Princeton Univ. Press, 1971.

[St] W. A. Stein, Explicit approaches to modular abelian varieties, Ph. D. thesis, University of California at Berkeley, 2000.

[Y] T. Yamauchi, The modularity of $\mathbb{Q}$ curves of degree 43, *Houston Jour. Math.* **34** (2008), 1025–1035.

University of Sheffield, School of Mathematics and Statistics, Hicks Building, Hounsfield Road, Sheffield, S3 7RH, U.K.

Algebra and Number Theory Sector, Institute for Information Transmission Problems, B. Karetny 19, Moscow 127994, Russia.

E-mail address: `n.p.dummigan@shef.ac.uk`

E-mail address: `golyshev@mccme.ru`