TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 367, Number 6, June 2015, Pages 4339–4358
S 0002-9947(2014)06271-5
Article electronically published on October 10, 2014

LOCAL INVARIANTS OF ISOGENOUS ELLIPTIC CURVES

TIM DOKCHITSER AND VLADIMIR DOKCHITSER

Abstract. We investigate how various invariants of elliptic curves, such as the discriminant, Kodaira type, Tamagawa number and real and complex periods, change under an isogeny of prime degree p. For elliptic curves over l-adic fields, the classification is almost complete (the exception is wild potentially supersingular reduction when $l = p$), and is summarised in a table.

Contents

1. Introduction

We address the question of how various invariants of elliptic curves, such as the discriminant, Kodaira type, Tamagawa number and real and complex periods, change under an isogeny. As every isogeny factors as a composition of endomorphisms and isogenies of prime degree, throughout the paper we just consider a fixed isogeny

$$\phi : E \longrightarrow E'$$

of prime degree p. The first result is a slight extension of a theorem of Coates ([3, Appendix]), relating the discriminants Δ_E and $\Delta_{E'}$:

Theorem 1.1. *Let $\mathcal{K}$ be a field of characteristic 0 and $\phi : E \to E'$ a p-isogeny of elliptic curves over $\mathcal{K}$. If $p > 3$, then $\Delta_E^p/\Delta_{E'}$ is a 12th power in $\mathcal{K}$. For $p = 2, 3$ this is a 3rd, respectively 4th, power.*

Received by the editors January 17, 2013 and, in revised form, August 4, 2013.
2010 *Mathematics Subject Classification.* Primary 11G07; Secondary 11G05, 11G40.
The first author was supported by a Royal Society University Research Fellowship.

TABLE 1. Local invariants of isogenous elliptic curves

Reduction type of E/K	δ, δ'	$\frac{\phi^*\omega'}{\omega}$ up to unit	$\frac{c}{c'}$	Kodaira types for E, E'
good ordinary	$\delta = \delta' = 0$	1 or p (†)	1	I_0
good supersingular		?		
split mult., $v(j) = pv(j')$	$\delta = p\delta'$	1	p	I_{pn}, I_n
split mult., $pv(j) = v(j')$	$\delta' = p\delta$	p	$\frac{1}{p}$	I_n, I_{pn}
nonsplit mult., $v(j) = pv(j')$	$\delta = p\delta'$	1	1 if $p \neq 2$ or $2 \mid \delta'$ 2 otherwise	I_{pn}, I_n
nonsplit mult., $pv(j) = v(j')$	$\delta' = p\delta$	p	1 if $p \neq 2$ or $2 \mid \delta$ $\frac{1}{2}$ otherwise	I_n, I_{pn}
additive pot. mult.				
$v(j) = pv(j')$	$\delta' = \delta + \frac{p-1}{p} v(j)$	1	1 if $p \geqslant 3$ (‡) if $p = 2$	I_n^*, $\mathrm{I}^*_{n + \frac{p-1}{p} v(j)}$ ($= \mathrm{I}^*_{n/p}$ if $l \neq 2$)
$pv(j) = v(j')$	$\delta' = \delta - (p-1)v(j)$	p	1 if $p \geqslant 3$ (‡) if $p = 2$	I_n^*, $\mathrm{I}^*_{n-(p-1)v(j)}$ ($= \mathrm{I}^*_{pn}$ if $l \neq 2$)
additive pot. good, $l \neq p$				
$p = 3$, type IV, IV^*, $\mu_3 \not\subset K$	$\delta' = \delta$	1	$(*)$	same
$p = 2$, type I_0^*			(‡)	
all other cases			1	
additive pot. good, $l = p$				
pot. ordinary	$\delta' = \delta$	1 or p (†)	1 if $p \geqslant 3$ (‡) if $p = 2$	same
pot. supersingular tame	$\delta' = 12 - \delta$	?	1	opposite
pot. supersingular wild	?	?	?	?

$K/\mathbb{Q}_l$ finite, $v\colon K^\times \twoheadrightarrow \mathbb{Z}$ valuation; $\phi\colon E/K \to E'/K$ p-isogeny; Δ, Δ' minimal discriminants; $\delta = v(\Delta)$, $\delta' = v(\Delta')$; ω, ω' minimal differentials; j, j' j-invariants; c, c' Tamagawa numbers.

$(*) = 3$ if E/K has nontrivial 3-torsion, and $\frac{1}{3}$ otherwise.

$$(\ddagger) = \begin{cases} 1 & \text{if } \frac{\Delta}{\Delta'} \text{ is a norm in } F/K \\ \frac{1}{2} & \text{if } \Delta' \text{ is a norm in } F/K \text{ and } \Delta \text{ is not} \\ 2 & \text{if } \Delta \text{ is a norm in } F/K \text{ and } \Delta' \text{ is not} \end{cases} \qquad (\dagger) = \begin{cases} p & \text{if } \ker\phi \subset \hat{E}(\mathfrak{m}_L) \\ 1 & \text{if } \ker\phi \not\subset \hat{E}(\mathfrak{m}_L) \end{cases} \qquad (L = F(\ker\phi))$$

F is any (†), respectively quadratic (‡), extension where E has good or split multiplicative reduction.

We present another proof of Coates' result, exploiting the fact that for $p > 3$, $\Delta(p\tau)^p/\Delta(\tau)$ is a 12th power of a modular form on $\Gamma_0(p)$ (§2, Appendix B). For one application, see Česnavičius' work on the parity conjecture [2, §5].

We then consider the standard invariants of elliptic curves over local fields. Table 1 summarises our results for the valuations of minimal discriminants δ, δ' of E, E', their Tamagawa numbers c, c', Kodaira types and the leading term $\frac{\phi^*\omega'}{\omega}$ of ϕ on the formal group (see §1.1 for the notation). The quotient of Tamagawa numbers $\frac{c}{c'}$ and the quantity $\frac{\phi^*\omega'}{\omega}$ classically appear in the applications of the isogeny invariance of the Birch–Swinnerton-Dyer formula to Selmer groups of elliptic curves; see e.g. [1], [18], [9], [6], [12] and [8]. The quotient $\frac{\phi^*\omega'}{\omega}$ is an important invariant of the isogeny ϕ, being the leading term of ϕ on the formal groups (cf. Lemma 4.2, [22, §IV.4] and also [18, p. 91], where it is denoted by $\phi'(0)$).

For curves defined over $\mathbb{R}$ and $\mathbb{C}$ the analogues of the local Tamagawa numbers are periods (cf. Remark 7.5)

$$\Omega(E, \omega) = \int_{E(\mathbb{R})} |\omega| \qquad \text{and} \qquad \Omega(E, \omega) = 2\int_{E(\mathbb{C})} |\omega \wedge \bar{\omega}|$$

computed with respect to some invariant differential ω on E. We show that these periods for E and E' are related as follows:

Theorem 1.2. *Suppose the base field of E, E' is $\mathcal{K} = \mathbb{R}$ or $\mathcal{K} = \mathbb{C}$. Choose invariant differentials ω, ω' for E and E'. Then*

$$\frac{\Omega(E,\omega)}{\Omega(E',\omega')} = \lambda\Big|\frac{\omega}{\phi^*\omega'}\Big|_{\mathcal{K}}.$$

Here $|\cdot|_{\mathcal{K}}$ is the standard normalised absolute value on $\mathcal{K}$, and λ is

- p *if* $\mathcal{K} = \mathbb{C}$,
- p *if* $\mathcal{K} = \mathbb{R}$, $p \neq 2$ *and* $\ker\phi \subset E(\mathbb{R})$,
- 1 *if* $\mathcal{K} = \mathbb{R}$, $p \neq 2$ *and* $\ker\phi \not\subset E(\mathbb{R})$.

If $\mathcal{K} = \mathbb{R}$ and $p = 2$, write E in the form $y^2 = x^3 + ax^2 + bx$ so that $(0,0) \in \ker\phi$. Then λ is

- 1 *if* $b > 0$, *and either* $a < 0$ *or* $4b > a^2$,
- 2 *otherwise.*

Finally, we look at periods of isogenous elliptic curves over $\mathbb{Q}$. In this case, $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ have global minimal differentials ω, ω', unique up to signs. The real periods $\Omega = \Omega(E/\mathbb{R}, \omega)$ and $\Omega' = \Omega(E'/\mathbb{R}, \omega')$ are the ones that enter the Birch–Swinnerton-Dyer conjecture over $\mathbb{Q}$. We prove that the quotient Ω/Ω' is 1, p or $1/p$ and give a criterion for when it is 1 (Theorem 8.2). For example, for $p > 3$ the periods are equal if and only if E has an odd number of primes of additive reduction with local root number -1. If $p > 2$ and E is semistable, then $\frac{\Omega}{\Omega'} = p^{\pm 1}$, and

$$\frac{\Omega}{\Omega'} = p \quad \Longleftrightarrow \quad \omega = \pm\phi^*\omega' \quad \Longleftrightarrow \quad \ker\phi \subset E(\mathbb{Q});$$

see Theorem 8.7.

1.1. **Notation.** Throughout the paper p is a prime number, and $\phi : E \to E'$ an isogeny of elliptic curves of degree p. We write $\phi^t : E' \to E$ for the dual isogeny. In §3-§6, the base field K is a finite extension of $\mathbb{Q}_l$; $l = p$ is allowed. There we use the following notation:

v	normalised valuation $K^\times \to \mathbb{Z}$
$\mathfrak{m}_K$	maximal ideal of the ring of integers of K
Δ, Δ'	minimal discriminants of E/K and E'/K
δ, δ'	their valuations: $\delta = v(\Delta), \delta' = v(\Delta')$
ω, ω'	minimal invariant differentials on E, E' (Néron differentials), unique up to units
$f = f'$	conductor exponent of E and E'
c, c'	local Tamagawa numbers of E and E'
m, m'	number of components in the special fibre of the minimal regular model of E, E'; so $\delta = f + m - 1, \delta' = f' + m' - 1$ by Ogg's formula
j, j'	j-invariants of E and E'
$\hat{E}, \hat{E}'$	the formal groups of E and E' with respect to a minimal Weierstrass equation
$\lvert\cdot\rvert_{\mathcal{K}}$	normalised absolute value; so $\lvert x\rvert_{\mathbb{R}} = \lvert x\rvert$, $\lvert x\rvert_{\mathbb{C}} = \lvert x\rvert^2$ and $\lvert x\rvert_K = q^{-v(x)}$ if $\mathcal{K} = K$ is as above, with residue field $\mathbb{F}_q$

When we work over an extension F/K, we write $\Delta_{E/F}, \Delta_{E'/F}$, etc. Any two invariant differentials on E/K differ by a scalar, $\omega_1 = a\omega_2$ with $a \in K^\times$, and we will abuse the notation slightly and write $\frac{\omega_1}{\omega_2}$ for a.

Recall that a curve E/K has additive reduction if and only if it has conductor exponent $f \geqslant 2$, and $f = 2$ if and only if the ℓ-adic Tate module of E is tamely ramified for some (any) $\ell \neq l$. We will call this a *tame* reduction (and *wild* otherwise). If $l \geqslant 5$, the reduction is always tame; when $l = 2$ it is tame if and only if E has Kodaira type $\mathrm{IV}, \mathrm{IV}^*$; when $l = 3$ it is tame if and only if E has Kodaira type $\mathrm{III}, \mathrm{III}^*$ or I_0^* (cf. Theorem 3.1). In Table 1, *opposite* Kodaira types refer to $\mathrm{II} \leftrightarrow \mathrm{II}^*$, $\mathrm{III} \leftrightarrow \mathrm{III}^*$, $\mathrm{IV} \leftrightarrow \mathrm{IV}^*$, $\mathrm{I}_0^* \leftrightarrow \mathrm{I}_0^*$.

1.2. **Layout.** Theorem 1.1 is proved in §2. In §3-§6 we prove the results summarised in Table 1: for δ see Theorem 5.1 and Corollary 3.3; for $\phi^*\omega'/\omega$ see Propositions 4.8 and 4.10, Lemma 4.3 and Proposition 4.9; for the Tamagawa numbers, see Theorem 6.1; for Kodaira symbols, see Theorem 5.4. Real and complex periods are discussed in §7 and the particular case of elliptic curves over $\mathbb{Q}$ in §8. Appendix A recalls the theory of the Tate curve and some standard facts about quadratic twists. Appendix B reviews the connection between values of modular forms and invariants of elliptic curves with a cyclic isogeny.

2. $\Delta(E') = \Delta(E)^p$ up to 12th powers

In this section we relate the discriminants Δ and Δ' of p-isogenous elliptic curves E and E'. Here we work over an arbitrary field of characteristic 0, so these are discriminants of some (not necessarily minimal) Weierstrass models. They depend on the choice of models, and are well-defined up to 12th powers.

Theorem 2.1 (Coates [3, appendix, Thm. 8])**.** *Let $\mathcal{K}$ be a field of characteristic* 0 *and $\phi : E \to E'$ a p-isogeny of elliptic curves over $\mathcal{K}$ with $p>3$. Then Δ^p/Δ' is a* 12*th power in $\mathcal{K}$.*

Proof. We may assume that $\mathcal{K} \subset \mathbb{C}$, embedding the field of definition of E, E' and ϕ into $\mathbb{C}$ if necessary (Lefschetz principle).

Let τ be a complex variable in the upper half-plane, and let $\eta(\tau)$ be the Dedekind eta-function. By a classical theorem, $\eta(p\tau)^p/\eta(\tau)$ is a modular form of weight $\frac{p-1}{2}$ on $\Gamma_0(p)$, with character $(\frac{d}{p})$, and its square $f(\tau) = [\eta(p\tau)^p/\eta(\tau)]^2$ is a modular form of weight $p-1$ on $\Gamma_0(p)$, with trivial character ([13, Thm. 2.2], or [17, Thm. 1.1] and [10, remark below Thm. 1]). Its q-expansion

$$f(\tau) = q^{\frac{p^2-1}{12}} \prod_{n\geqslant 1} \frac{(1-q^{pn})^{2p}}{(1-q^n)^2} \qquad\qquad (q = e^{2\pi i\tau})$$

clearly has integer coefficients. Note that $f(\tau)$ is a 12th root of $\frac{\Delta(p\tau)^p}{\Delta(\tau)}$.

Choose models for $E/\mathcal{K}, E'/\mathcal{K}$ of the form

$$E : y^2 = 4x^3 + ax + b, \qquad\qquad E' : y^2 = 4x^3 + a'x + b',$$

with $\phi^*\frac{dx}{y} = p\frac{dx}{y}$, and complex uniformisations $E = \mathbb{C}/\Lambda$, $E' = \mathbb{C}/\Lambda'$ so that

$$\varphi : \mathbb{C}/\Lambda \ni z \mapsto (\wp_\Lambda(z), \wp'_\Lambda(z)) \in E(\mathbb{C})$$

satisfies $\varphi^* \frac{dx}{y} = dz$ and similarly for Λ' (cf. Appendix B). From $\phi^* dz = p dz$ we see that $\Lambda \subset \Lambda'$ has index p, and so we can write the two lattices in the form $\Lambda = \mathbb{Z}\Omega_1 + \mathbb{Z}\Omega_2$, $\Lambda' = \mathbb{Z}\Omega_1 + \mathbb{Z}p\,\Omega_2$.

By the q-expansion principle (or Theorem B.3),

$$\left(\tfrac{2\pi}{\Omega_1}\right)^{p-1} f(\tau) \in \mathcal{K}, \qquad \tau = \tfrac{\Omega_2}{\Omega_1}.$$

On the other hand,

$$f(\tau)^{12} = \frac{\Delta(p\tau)^p}{\Delta(\tau)} = \frac{\left(\frac{\Omega_1}{2\pi}\right)^{12p} \Delta_{E'}^p}{\left(\frac{\Omega_1}{2\pi}\right)^{12} \Delta_E};$$

here Δ_E and $\Delta_{E'}$ are the discriminants of the models $E : y^2 = x^3 + \frac{a}{4}x + \frac{b}{4}$ and $E' : y^2 = x^3 + \frac{a'}{4}x + \frac{b'}{4}$, and the second equality follows from the relation between $\Delta(\tau)$ and Δ_E proved in (B.2). It follows that

$$\frac{\Delta_{E'}^p}{\Delta_E} = [\left(\tfrac{2\pi}{\Omega_1}\right)^{p-1} f(\tau)]^{12} \in \mathcal{K}^{\times 12}.$$

Swapping E and E' (or using the fact that $(\Delta^p)^p$ is Δ up to a 12th power, as $p^2 \equiv 1 \mod 12$ for $p \neq 2, 3$) gives the claim. $\square$

Now we prove analogues for $p = 2$ and $p = 3$, using an explicit computation with a universal family:

Theorem 2.2. *Let $\mathcal{K}$ be a field of characteristic 0 and $\phi : E \to E'$ a 2-isogeny of elliptic curves over $\mathcal{K}$. Then Δ^2/Δ' is a 3rd power in $\mathcal{K}$.*

Proof. Any 2-isogeny $\phi : E \to E'$ of elliptic curves over a field of characteristic not 2 or 3 has a model

$$\begin{array}{lcl} E & : & y^2 = x^3 + ax^2 + bx, \\ E' & : & y^2 = x^3 - 2ax^2 + (a^2 - 4b)x, \\ \phi(x, y) & = & (x + a + bx^{-1}, y - byx^{-2}), \end{array}$$

and

$$\frac{\Delta^2}{\Delta'} = \frac{[16b^2(a^2 - 4b)]^2}{256b(a^2 - 4b)^2} = b^3.$$

$\square$

Theorem 2.3. *Let $\mathcal{K}$ be a field of characteristic 0 and $\phi : E \to E'$ a 3-isogeny of elliptic curves over $\mathcal{K}$. Then Δ^3/Δ' is a 4th power in $\mathcal{K}$.*

Proof. Any 3-isogeny $\phi : E \to E'$ of elliptic curves over a field of characteristic not 2 or 3 has a model

$$\begin{array}{lcl} E & : & y^2 = x^3 + a(x - b)^2, \\ E' & : & y^2 = x^3 + ax^2 + 18abx + ab(16a - 27b), \\ \phi(x, y) & = & (x - 4abx^{-1} + 4ab^2x^{-3}, y + 4abyx^{-2} - 8ab^2yx^{-3}), \end{array}$$

and

$$\frac{\Delta^3}{\Delta'} = \frac{[-16a^2b^3(4a + 27b)]^3}{-16a^2b(4a + 27b)^3} = (4ab^2)^4.$$

$\square$

3. Discriminants and Kodaira types I

Throughout §3-§6 we follow the notation of §1.1. In particular, K is a finite extension of $\mathbb{Q}_l$, and $\phi : E/K \to E'/K$ is a p-isogeny (in 3.1, 3.3).

Theorem 3.1. *Suppose E/K has additive potentially good reduction. Then E has tame reduction (equivalently, has conductor exponent 2) if and only if*

- $l \geqslant 5$, *or*
- $l = 3$ *and E has Kodaira type* III, III*, I$_0^*$, *or*
- $l = 2$ *and E has Kodaira type* IV, IV*.

In this case E' is tame as well, and

$$0 < \delta, \delta' < 12 \qquad \textit{and} \qquad \delta' \equiv p\,\delta \mod 12.$$

Proof. For the first statement, see [23, IV. 9, Table 4.1] for $l \geqslant 5$, [15, Thm. 1] for $l = 3$, and [14, Prop. 8.20] for $l = 2$. From [23, IV. 9, Table 4.1] it also follows that $0 < \delta, \delta' < 12$ in all these cases. The last congruence follows from Theorems 2.1–2.3. □

Theorem 3.2. *Suppose E/K has additive potentially good reduction and is not a quadratic twist of a curve with good reduction. Then*

- *If $l = 2, 3$ or $l \equiv -1 \mod 12$, then E is potentially supersingular.*
- *If $l \equiv 1 \mod 12$, then E is potentially ordinary.*
- *If $l \equiv 5 \mod 12$, then E is potentially ordinary if and only if its Kodaira type is* III *or* III*.
- *If $l \equiv 7 \mod 12$, then E is potentially ordinary if and only if its Kodaira type is* II, II*, IV *or* IV*.

Proof. Let K^{nr} be the maximal unramified extension of K, and F/K^{nr} the (finite) extension cut out by the Galois action on any ℓ-adic Tate module of E for $\ell \neq l$. By the criterion of Néron-Ogg-Shafarevich, F is the unique minimal Galois extension of K^{nr} where E has good reduction.

The Galois group $\mathrm{Gal}(F/K^{nr})$ has order at least 3, since E is not a quadratic twist of a curve with good reduction (cf. Lemma A.3). As explained in [21, proof of Thm. 2], it acts faithfully on the reduced curve $\tilde{E}$ defined over the residue field of F as a group of automorphisms. This forces $j(\tilde{E})$ to be either 0 or 1728; see e.g. [22, Thm. III.10.1]. If $l = 2$ or 3, then $1728 = 0$ is a supersingular j-invariant, as asserted.

Now suppose $l > 3$. By [23, IV.9, Table 4.1], either a) E has reduction type $\mathrm{II}, \mathrm{II}^*, \mathrm{IV}$ or IV* and $j(E)$ reduces to 0, or b) E has reduction type $\mathrm{III}, \mathrm{III}^*$ and $j(E)$ reduces to 1728. The j-invariant 0 is ordinary if and only if $l \equiv 1 \mod 3$, and 1728 is ordinary if and only if $l \equiv 1 \mod 4$; see [22, Ex. V. 4.4, V. 4.5]. □

Corollary 3.3. *Suppose $l = p$ and E has additive tame potentially good reduction. If the reduction is potentially ordinary, then $\delta = \delta'$ and E, E' have the same Kodaira type. If the reduction is potentially supersingular, then $\delta = 12 - \delta'$ and E, E' have opposite Kodaira types* (II $\leftrightarrow$ II*, III $\leftrightarrow$ III*, IV $\leftrightarrow$ IV*, I$_0^*$ $\leftrightarrow$ I$_0^*$).

Proof. By Theorem 3.1, we have $\delta, \delta' < 12$. Also, if $\delta \neq \delta'$, then $\delta \not\equiv p\delta \mod 12$; equivalently $12 \nmid \delta(p-1)$. Exchanging E, E' if necessary, the possibilities with $\delta \neq \delta'$

are (cf. [23, IV.9, Table 4.1])

- $\delta = 2$, $\delta' = 10$, $p \equiv 2 \mod 3$,
- $\delta = 4$, $\delta' = 8$, $p \equiv 2 \mod 3$,
- $\delta = 3$, $\delta' = 9$, $p \equiv 3 \mod 4$.

By Theorem 3.2, these are precisely the cases of potentially supersingular reduction unless E is a quadratic twist of a curve with good reduction. In the latter case, l cannot be 2 (as E has tame reduction), so E and E' have Kodaira type I_0^* and $\delta = \delta' = 6$. □

4. Differentials

Notation 4.1. We will write

$$\alpha_{\phi/K} = \left|\frac{\phi^*\omega'}{\omega}\right|_K^{-1}.$$

Lemma 4.2.

(1) *The isogeny ϕ induces a map on formal groups,*

$$\phi : \hat{E}(\mathfrak{m}_K) \to \hat{E}'(\mathfrak{m}_K), \qquad \phi(T) = aT + \cdots,$$

with leading term $a = \frac{\phi^*\omega'}{\omega} \times unit \in \mathcal{O}_K$.

(2)

$$\frac{|\operatorname{coker}\phi : E(K) \to E'(K)|}{|\ker\phi : E(K) \to E'(K)|} = \alpha_{\phi/K}\,\frac{c'}{c}.$$

Proof. (1) By the Néron universal property, ϕ extends to a morphism of Néron models, and thus induces a map on formal groups. For the leading term, see [22, Ch. IV, especially Cor. IV.4.3].

(2) [18, Lemma 3.8]. □

Lemma 4.3. *If $l \neq p$, then $\phi^*\omega'$ is minimal, so $\alpha_{\phi/K} = 1$.*

Proof. Write $\phi^*\omega' = a\omega$, $(\phi^t)^*\omega = a'\omega'$ with $a, a' \in \mathcal{O}_K$ by Lemma 4.2. Because $\phi^t\phi = [p]$, we have $aa' = p \in \mathcal{O}_K^\times$. So a and a' are units, and $\phi^*\omega'$ is minimal. □

Lemma 4.4. *Suppose F/K is a finite extension. Then*

$$\frac{\phi^*\omega_{E'/K}}{\omega_{E/K}} = \frac{\phi^*\omega_{E'/F}}{\omega_{E/F}} \times unit \qquad \Longleftrightarrow \qquad \frac{\Delta_{E/K}}{\Delta_{E'/K}} = \frac{\Delta_{E/F}}{\Delta_{E'/F}} \times unit.$$

If $l \neq p$, or E/K is semistable, or $l = p$ and E has tame potentially ordinary reduction, then the formulae hold.

Proof. It is easy to see that up to units (cf. [22, Table III.1.2]),

$$\frac{\Delta_{E/K}}{\Delta_{E/F}} = \left(\frac{\omega_{E/K}}{\omega_{E/F}}\right)^{-12} \qquad \text{and} \qquad \frac{\Delta_{E'/K}}{\Delta_{E'/F}} = \left(\frac{\omega_{E'/K}}{\omega_{E'/F}}\right)^{-12} = \left(\frac{\phi^*\omega_{E'/K}}{\phi^*\omega_{E'/F}}\right)^{-12}.$$

So $\frac{\Delta_{E/K}}{\Delta_{E'/K}} / \frac{\Delta_{E/F}}{\Delta_{E'/F}}$ is the 12th power of $\frac{\phi^*\omega_{E'/F}}{\omega_{E/F}} / \frac{\phi^*\omega_{E'/K}}{\omega_{E/K}}$, up to a unit.

For the second claim, if $l \neq p$ or E/K is semistable, then the left-hand formula holds (Lemma 4.3 and the fact that for semistable curves minimal differentials stay minimal in all extensions). If $l = p$ and E is tame, the right-hand formula holds by Corollary 3.3. □

Remark 4.5. Suppose E and E' are in Weierstrass form,

$$E : y^2 = f(x), \qquad E' : y^2 = g(x).$$

Since $\phi(-P) = -\phi(P)$ and every even rational function on E is a function of x (cf. [22, proof of Cor. III.2.3.1]), ϕ has the form

$$\phi : (x, y) \longmapsto (\xi(x), y\eta(x)), \qquad \xi(x), \eta(x) \in K(x).$$

If $F = K(\sqrt{d})$ is a quadratic extension, and

$$E_d : dy^2 = f(x), \qquad E'_d : dy^2 = g(x)$$

the quadratic twists of E, E' by d, then the same formula $(\xi(x), y\eta(x))$ defines an isogeny $\phi_d : E_d \to E'_d$. It fits into a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_d(K) & \longrightarrow & E(F) & \xrightarrow{N} & E(K) & \longrightarrow & \frac{E(K)}{NE(F)} & \longrightarrow & 0 \\ & & \phi_d\big\downarrow & & \phi\big\downarrow & & \phi\big\downarrow & & \phi\big\downarrow & & \\ 0 & \longrightarrow & E'_d(K) & \longrightarrow & E'(F) & \xrightarrow{N} & E'(K) & \longrightarrow & \frac{E'(K)}{NE'(F)} & \longrightarrow & 0, \end{array}$$

where the map $E_d(K) \to E(F)$ is $(x, y) \mapsto (x, y\sqrt{d})$, and N is the norm (or trace) map $E(F) \to E(K)$, $E'(F) \to E'(K)$.

Lemma 4.6. *Let $F = K(\sqrt{d})$ be a quadratic extension, E_d, E'_d the quadratic twists of E, E' by d, and ϕ_d the corresponding isogeny. The groups $\frac{E(K)}{NE(F)}$, $\frac{E'(K)}{NE'(F)}$ are finite, and*

$$\Big(\alpha_{\phi_d/K}\frac{c_{E'_d/K}}{c_{E_d/K}}\Big)^{-1} \cdot \alpha_{\phi/F}\frac{c_{E'/F}}{c_{E/F}} \cdot \Big(\alpha_{\phi/K}\frac{c_{E'/K}}{c_{E/K}}\Big)^{-1} \cdot \frac{|\frac{E'(K)}{NE'(F)}|}{|\frac{E(K)}{NE(F)}|} = 1.$$

Proof. The groups $\frac{E(K)}{NE(F)}$, $\frac{E'(K)}{NE'(F)}$ are quotients of $\frac{E(K)}{2E(K)}$, $\frac{E'(K)}{2E'(K)}$, which are finite. Now consider the commutative diagram above. Because the alternating product of $|\ker|/|\operatorname{coker}|$ is 1, Lemma 4.2(2) gives the claim. $\square$

Proposition 4.7. *Let $F = K(\sqrt{d})$ be a quadratic extension, E_d, E'_d the quadratic twists of E, E' by d, and ϕ_d the corresponding isogeny.*

(1) Write K_n, F_n for the degree n unramified extensions of K, F. Then

$$\frac{\alpha_{\phi/K}\alpha_{\phi_d/K}}{\alpha_{\phi/F}} = \lim_{\substack{n\to\infty \\ n \text{ odd}}} \sqrt[n]{\frac{|E'(K_n)/NE'(F_n)|}{|E(K_n)/NE(F_n)|}}.$$

If $l \neq 2$, this quotient is 1.

(2) We have $\alpha_{\phi_d/K} = \alpha_{\phi/K}$ and $\alpha_{\phi/F} = \alpha^2_{\phi/K}$ unless (i) $l = p$ and E has additive potentially supersingular reduction or (ii) $l = p = 2$ and E has supersingular reduction.

Proof. (1) We apply Lemma 4.6 for E in F_n/K_n; because n is odd, we have $F_n = K_n(\sqrt{d})$. The minimal differentials stay the same in unramified extensions, so $\alpha_{\phi/K_n} = \alpha^n_{\phi/K}$, and similarly for α_{ϕ/F_n} and α_{ϕ_d/K_n}. Thus,

$$\frac{c_{E'/F_n}}{c_{E/F_n}}\frac{c_{E/K_n}}{c_{E'/K_n}}\frac{c_{E_d/K_n}}{c_{E'_d/K_n}}\frac{|E'(K_n)/NE'(F_n)|}{|E(K_n)/NE(F_n)|} = \frac{\alpha^n_{\phi/K}\alpha^n_{\phi_d/K}}{\alpha^n_{\phi/F}}.$$

All the Tamagawa numbers are bounded, so the claim follows by taking nth roots and letting $n \to \infty$. Moreover, if $l \neq 2$, because the norm quotients are 2-groups and the α's are powers of l, we can compare the l-parts before taking the limit, and we find that $\frac{\alpha_{\phi/K}\alpha_{\phi_d/K}}{\alpha_{\phi/F}} = 1$.

(2) We may assume $l = p$, as otherwise all α's are 1 by Lemma 4.3.

(a) If $l \neq 2$, or E has either good ordinary or split multiplicative reduction, we have $\alpha_{\phi/F} = \alpha_{\phi/K}\alpha_{\phi_d/K}$: if $l \neq 2$, this is proved in (1); otherwise, the norm quotients have size at most 4 by [14, Prop. 8.6, Prop. 4.1], and so $\alpha_{\phi/F} = \alpha_{\phi/K}\alpha_{\phi_d/K}$ by (1).

(b) If either E is semistable or $l = p > 3$ and E is potentially ordinary,

$$\frac{\phi^*\omega_{E'/K}}{\omega_{E/K}} = \frac{\phi^*\omega_{E'/F}}{\omega_{E/F}} \times \text{unit},$$

by Lemma 4.4, and

$$\alpha_{\phi/F} = \left|\frac{\phi^*\omega_{E'/F}}{\omega_{E/F}}\right|_F^{-1} = \left|\frac{\phi^*\omega_{E'/K}}{\omega_{E/K}}\right|_K^{-2} = \alpha^2_{\phi/K}.$$

(c) Combining (a) and (b), we find that $\alpha_{\phi/K} = \alpha_{\phi_d/K}$ and $\alpha_{\phi/F} = \alpha^2_{\phi/K}$ in the following three cases:

- $l > 3$ and E is semistable or potentially ordinary,
- $l = 3$ and E is semistable,
- $l = 2$ and E is split multiplicative or good ordinary.

It follows that $\alpha_{\phi/K} = \alpha_{\phi_d/K}$ and $\alpha_{\phi/F} = \alpha^2_{\phi/K}$ also hold for quadratic twists of all such curves, as $\alpha_{\phi_{d_1}/K} = \alpha_{\phi/K} = \alpha_{\phi_{d_2}/K}$ for any pair of twists. Since a curve with potentially multiplicative reduction is a quadratic twist of a semistable one, and a curve with potentially ordinary reduction a quadratic twist of a good ordinary one when $l \leqslant 3$ (Theorem 3.2), the result holds in all the cases claimed. $\square$

Proposition 4.8. *Suppose $l = p$ and E has good ordinary reduction. Let $F = K(\ker\phi)$ be the field obtained by adjoining the coordinates of points in $\ker\phi$. Then*

$$\frac{\phi^*\omega'}{\omega} = \begin{cases} p\times \textit{unit}, & \textit{if } \ker\phi \subset \hat{E}(\mathfrak{m}_F), \\ \textit{unit}, & \textit{otherwise}. \end{cases}$$

Proof. The isogeny ϕ induces an isogeny on formal groups

$$\phi : \hat{E}(\mathfrak{m}_F) \to \hat{E}'(\mathfrak{m}_F), \qquad \phi(T) = aT + \cdots,$$

with $a = \frac{\phi^*\omega'}{\omega}$ by Lemma 4.2 (1). Define a' similarly for ϕ^t. The reduction $\tilde{E} = E \mod \mathfrak{m}_F$ is an ordinary elliptic curve, so $[p] = \tilde{\phi} \circ \tilde{\phi}^t$ is an isogeny of height 1 on its formal group. Hence either $\tilde{\phi}$ or $\tilde{\phi}^t$ is an isomorphism on formal groups of the reduced curves; in other words, either $a \mod \mathfrak{m}_F$ or $a' \mod \mathfrak{m}_F$ is nonzero. Because $aa' = p$, one of a, a' is a unit and the other one is $p\times$unit. If a is a unit, then $\ker\phi$ is trivial on $\hat{E}$. Otherwise, ϕ reduces to an inseparable isogeny of prime degree, and hence $\ker\tilde{\phi} = 0$ on $\tilde{E}$. Therefore $\ker\phi$ lies on the formal group. $\square$

Proposition 4.9. *If $l = p$ and E has potentially ordinary reduction, then $\frac{\phi^*\omega'}{\omega}$ is either a unit or $p\times$unit. If F/K is finite, then $\frac{\phi^*\omega_{E'/F}}{\omega_{E/F}} = \frac{\phi^*\omega_{E'/K}}{\omega_{E/K}} \times$ unit.*

Proof. When $p = 2$ or 3, Theorem 3.2 shows that E is a quadratic twist of a curve with good reduction. The result follows from Propositions 4.8 and 4.7(2).

When $p \geqslant 5$, Lemma 4.4 shows that $\frac{\phi^*\omega_{E'/K}}{\omega_{E/K}} = \frac{\phi^*\omega_{E'/F}}{\omega_{E/F}}$ for any F/K. Taking F to be the field where E acquires good reduction, we see that this quantity is a unit or $p\times$unit by Proposition 4.8. $\square$

Proposition 4.10. *If E has potentially multiplicative reduction, then*

$$\frac{\phi^*\omega'}{\omega} = \begin{cases} \text{unit}, & \text{if } v(j) = p\,v(j'), \\ p \times \text{unit}, & \text{otherwise.} \end{cases}$$

In particular, $\frac{\phi^*\omega_{E'/K}}{\omega_{E/K}} = \frac{\phi^*\omega_{E'/F}}{\omega_{E/F}} \times$ *unit for every finite extension F/K.*

Proof. Note that if $l \neq p$, the result follows from Lemma 4.3. Because both the j-invariant and α are unchanged under quadratic twists (Proposition 4.7), we may assume that E has split multiplicative reduction.

By the theory of the Tate curve (Theorem A.1), the pair E, E' is $E^{(q^p)}, E^{(q)}$ (in some order), with $q \in \mathfrak{m}_K$. In particular, either $v(j) = p\,v(j')$ or $v(j') = p\,v(j)$. Because

$$\frac{\phi^*\omega'}{\omega}\frac{(\phi^t)^*\omega}{\omega'} = \frac{\phi^*\omega'}{\omega}\frac{\phi^*(\phi^t)^*\omega}{\phi^*\omega'} = \frac{\phi^*\omega'}{\omega}\frac{p\,\omega}{\phi^*\omega'} = p,$$

the claim for ϕ is equivalent to that for ϕ^t. Swapping E and E' if necessary, assume that $E = E^{(q^p)}, E' = E^{(q)}$, in which case ϕ is given by

$$\phi : E(K) = K^\times/(q^p)^{\mathbb{Z}} \longrightarrow K^\times/q^{\mathbb{Z}} = E'(K),$$

induced by the identity map on $K^\times$. Here $|\ker\phi| = p$, $|\operatorname{coker}\phi| = 1$ on $E(K)$, and $\frac{c}{c'} = \frac{v(q^p)}{v(q)} = p$. By Lemma 4.2, the quotient $\frac{\phi^*\omega'}{\omega}$ is a unit. ∎

5. Discriminants and Kodaira types II

Theorem 5.1.

(1) *If E has potentially good reduction, and either $l \neq p$ or the reduction is good or potentially ordinary, then $\delta = \delta'$.*
(2) *If E has multiplicative reduction, then $\frac{\delta}{\delta'} = \frac{v(j)}{v(j')} = p^{\pm 1}$.*
(3) *If E has potentially multiplicative reduction, then*

$$\delta - \delta' = v(j') - v(j) = \begin{cases} \frac{1-p}{p}v(j), & \text{if } v(j) = pv(j'), \\ (p-1)v(j), & \text{if } v(j') = pv(j). \end{cases}$$

Proof. If E has good reduction, then $\delta = \delta' = 0$. If E has split multiplicative reduction, then E and E' are Tate curves with parameters q and q^p, in some order (Theorem A.1). So $\delta = -v(j)$ and $\delta' = -v(j')$ are $v(q)$ and $pv(q)$, in some order. Thus (1) holds in the good reduction case, and (2), (3) in the split multiplicative case.

If either $l \neq p$ or E is potentially multiplicative, then $\frac{\phi^*\omega_{E'/K}}{\omega_{E/K}} = \frac{\phi^*\omega_{E'/F}}{\omega_{E/F}}$ for any F/K, by Lemma 4.3 and Proposition 4.10. Taking F to be a field where E has good or split multiplicative reduction, we find that the claim for E/F implies that for E/K, by Lemma 4.4.

We are left with the case that E has additive potentially ordinary reduction with $l = p$. If $p > 3$, the claim is proved in Corollary 3.3. If $p = 2, 3$, then E/K is a quadratic twist of a curve E_d/K with good ordinary reduction (Theorem 3.2). Let $F = K(\sqrt{d})$ be the corresponding quadratic extension. In the notation of Proposition 4.7 we have $\alpha_{\phi/K} = \alpha_{\phi_d/K}$ and, since the minimal model of E_d stays minimal in F/K and $E/F \cong E_d/F$, also $\alpha_{\phi/F} = \alpha^2_{\phi_d/K}$. So $\alpha_{\phi/F} = \alpha^2_{\phi/K}$. In other words, $\frac{\phi^*\omega_{E'/K}}{\omega_{E/K}} = \frac{\phi^*\omega_{E'/F}}{\omega_{E/F}}$, and the claim follows, again by Lemma 4.4. ∎

Remark 5.2. Note that in the potentially good case, the formulae $\delta = \delta'$ (Theorem 5.1) and $\delta' \equiv p\delta \mod 12$ (Theorem 3.1) do not contradict each other. The reason is that the possible reduction types are restricted in the potentially ordinary case; see Theorem 3.2.

Remark 5.3. In the potentially supersingular case the formulae in Proposition 4.9 and Theorem 5.1(1) may not hold. For example, consider the 5-isogenous elliptic curves $E = 50b1$, $E' = 50b3$. Their reduction types over $\mathbb{Q}_5$ are II and II* respectively, so $\delta \neq \delta'$. Also, over $\mathbb{Q}_5(\sqrt{5})$ the reduction types become IV and IV*, and $\phi^*\omega'/\omega = \sqrt{5}$ (computed as in Lemma 4.4 from the minimal discriminants), which is neither a unit nor $5\times$unit.

Theorem 5.4.

(1) *If E has potentially good reduction and $p \neq l$, then the Kodaira types of E and E' are the same.*
(2) *If E has potentially good ordinary reduction and $p = l$, then the Kodaira types of E and E' are the same.*
(3) *If E has tame potentially good supersingular reduction and $p = l$, then E and E' have opposite Kodaira type* (II $\leftrightarrow$ II*, III $\leftrightarrow$ III*, IV $\leftrightarrow$ IV*, $\mathrm{I}_0^* \leftrightarrow \mathrm{I}_0^*$).
(4) *If E has multiplicative reduction, then the Kodaira type is I_n for E, and either I_{pn} or $\mathrm{I}_{n/p}$ for E', corresponding to $v(j')=pv(j)$ and $pv(j')=v(j)$.*
(5) *If E has additive potentially multiplicative reduction, then the Kodaira type is I_n^* for E and $\mathrm{I}_{n'}^*$ for E', where either*
$$v(j')=pv(j) \quad \text{and} \quad n'=pn-4(a-1)(p-1)=n-v(j)(p-1)$$
or vice versa (swap $n \leftrightarrow n', j \leftrightarrow j'$); here a is the conductor exponent of the quadratic character of $K(\sqrt{-c_6})/K$ (it is 1 *if $l \neq 2$), where c_6 is the standard invariant of E as in* [22, §III.1].

Proof. Write f, f' for the conductor exponents of E and E', and m, m' for the number of connected components of the special fibre of their minimal regular models. Because ϕ induces an isomorphism between the ℓ-adic Tate modules of E and E' for $\ell \neq l, p$, we have $f = f'$. Recall that $\delta = f + m - 1$ and $\delta' = f' + m' - 1$ by Ogg's formula [23, IV.11.1].

(1) By Theorem 5.1, $\delta = \delta'$, and so $m = m'$. If $l \neq 2$, then from the reduction type table [23, IV.9, Table 4.1] we see that the Kodaira type in the additive potentially good case is determined by m, so they are the same for E and E'. (Note that I_n^* is necessarily potentially multiplicative even when $l = 3$.)

Suppose $l = 2$. Then m almost determines the reduction type, except for the pairs $\{\mathrm{I}_2^*, \mathrm{IV}^*\}$, $\{\mathrm{I}_3^*, \mathrm{III}^*\}$ and $\{\mathrm{I}_4^*, \mathrm{II}^*\}$. Passing to the maximal unramified extension if necessary, we see that I_0^* and I_n^* are the only reduction types with (the 2-part of) the local Tamagawa number equal to 4. Since the 2-part of the Tamagawa number is invariant under ϕ (as $p = \deg\phi$ is odd, ϕ induces an isomorphism between the 2-parts of E/E_0 and E'/E_0'), the Kodaira types must be the same.

(2) In the tame case, this is Corollary 3.3. By Theorem 3.2, the only wild case is when $p = l = 2$ and E, E' are quadratic twists of curves with good ordinary reduction by some character χ. Here $\delta = \delta'$ by Theorem 5.1(1), so $m = m'$ as in (1). Again as in (1), the Kodaira types of E and E' are the same, except possibly for 3 pairs of cases, $\{\mathrm{I}_2^*, \mathrm{IV}^*\}$, $\{\mathrm{I}_3^*, \mathrm{III}^*\}$ and $\{\mathrm{I}_4^*, \mathrm{II}^*\}$. We claim that none of these

can occur. For the first one, the reduction type IV* is tame by Theorem 3.1. For the second one, $m = 8$ and $6|\delta$ (since E acquires good reduction after a quadratic extension), so f is odd by Ogg's formula; however, f is twice the conductor exponent of χ, a contradiction. In the last case, pass to the maximal unramified extension as in (1). Then the Tamagawa numbers of E and E' become 1 and 4 ([23, IV.9, Table 4.1]), but their quotient is $1, 2$ or $\frac{1}{2}$ by the very last case of Theorem 6.1. (The proof of this case does not use the present theorem.)

(3) This is a special case of Corollary 3.3.

(4) This follows from the theory of the Tate curve (Theorem A.1).

(5) The quadratic twists E_{-c_6}, E'_{-c_6} have split multiplicative reduction and are p-isogenous (Lemma A.2, Remark 4.5). If $v(j') = pv(j)$, then these twists have Kodaira types I_ν, $\mathrm{I}_{p\nu}$ with $-\nu = v(j_{E_{-c_6}}) = v(j)$ (Theorem A.1). By Theorem A.5, E and E' have Kodaira types I_n^* and $\mathrm{I}_{n'}^*$ with $n = \nu + 4a - 4$ and $n' = p\nu + 4a - 4$. Clearly

$$n' = p(n - 4a + 4) + 4a - 4 = pn - 4(p - 1)(a - 1).$$

Because $v(j) = -\nu = -n + 4a - 4$, also

$$n' = pn - (p - 1)(4a - 4) = pn - (p - 1)(v(j) + n) = n - (p - 1)v(j).$$

If, on the other hand, $v(j) = pv(j')$, swap E and E'. □

6. Tamagawa numbers

Theorem 6.1. *If E is semistable, then the ratio of Tamagawa numbers $\frac{c}{c'}$ is*

- 1 *if E has good reduction;*
- $\frac{\delta}{\delta'} = \frac{v_K(j(E))}{v_K(j(E'))} = p^{\pm 1}$ *if E has split multiplicative reduction;*
- *if E has nonsplit multiplicative reduction:*
  - 1 *if $p \neq 2$, or if both δ and δ' are even,*
  - 2 *if $p = 2$ and δ' is odd,*
  - $\frac{1}{2}$ *if $p = 2$ and δ is odd.*

If E has additive reduction and $p > 3$, then $c/c' = 1$.
If E has additive reduction and $p = 3$, then c/c' is

- 1 *if $l \neq 3$, unless E has type* IV, IV* *and $\mu_3 \not\subset K$. In this exceptional case,*
  - 3 *if $E(K)[3] \neq 0$,*
  - $\frac{1}{3}$ *if $E(K)[3] = 0$.*
- 1 *if $l = 3$ and E has Kodaira type* III, III*, I_0^*, I_n^* *(equivalently, E does not have wild potentially supersingular reduction).*

If E has additive reduction and $p = 2$, then c/c' is

- 1 *if $l \neq 2$ and E is not of type I_0^* or I_n^*;*
- 1 *if $l = 2$ and E has tame potentially good reduction (i.e. type* IV, IV**);*
- *if a) $l \neq 2$ and E has type I_0^* or I_n^*, or b) $l = 2$ and E does not have potentially supersingular reduction,*
  - 1 *if $\frac{\Delta}{\Delta'}$ is a norm in F/K,*
  - $\frac{1}{2}$ *if Δ' is a norm in F/K and Δ is not,*
  - 2 *if Δ is a norm in F/K and Δ' is not,*

  where F/K is a quadratic extension such that E/F has good or split multiplicative reduction.

Lemma 6.2. *The quotient c/c' is a power of p.*

Proof. The isogeny ϕ induces maps $E(K) \to E'(K)$ and $E_0(K) \to E'_0(K)$, and so $E/E_0 \to E'/E'_0$. These are finite groups, and since $\phi\phi^t = [p] = \phi^t\phi$ are automorphisms on their prime-to-p parts, ϕ is an isomorphism between these prime-to-p parts. □

Proof of Theorem 6.1. In the semistable case this follows from Tate's algorithm [23, IV.9] and Theorem 5.1. Assume henceforth that E and E' have additive reduction. In particular, $1 \leqslant c, c' \leqslant 4$ (cf. [22, VII.6.1], [23, IV.9 Table 4.1]), so for $p > 3$ the result follows by Lemma 6.2.

For $p = 3$, $l \neq 3$, see [6, Lemma 11].

Suppose $p = 2$, $l \neq 2$. If the Kodaira type is not I_0^* or I_n^*, the Kodaira types of E and E' are the same by Theorem 5.4. By the reduction type table ([23, IV.9, Table 4.1]) in the case II, II*, IV, IV* the 2-parts of the Tamagawa numbers are trivial, and in the case III, III* they are both 2. Hence c and c' have the same 2-part, and are therefore equal. When the reduction type is I_0^*, see the computation in [6, §7.4].

For $p = l = 3$ and type III, III*, I_0^*, the isogenous curve E' also has one of these three Kodaira types (Theorem 3.1). The Tamagawa numbers for these types can be 1, 2 or 4, so the 3-isogeny forces the equality $c = c'$ (Lemma 6.2). Similarly, for $p = l = 2$ and type IV, IV*, the Tamagawa numbers are 1 or 3, and are unchanged by a 2-isogeny.

Finally, in the three remaining cases ($p = l = 3$, type I_n^*; $p = l = 2$, E not potentially supersingular; or $p = 2$, $l \neq 2$, type I_n^*), some quadratic twist E_d/K of E/K has either good or split multiplicative reduction (Theorem 3.2, Lemma A.2). Let $F = K(\sqrt{d})$ be the corresponding quadratic extension. By Lemma 4.6 (see Notation 4.1 and Remark 4.5 for the notation),

$$\Big(\alpha_{\phi/K}\frac{c_{E'/K}}{c_{E/K}}\Big)^{-1}\cdot\alpha_{\phi/F}\frac{c_{E'_d/F}}{c_{E_d/F}}\cdot\Big(\alpha_{\phi_d/K}\frac{c_{E'_d/K}}{c_{E_d/K}}\Big)^{-1}\cdot\frac{\big|\frac{E'_d(K)}{NE'_d(F)}\big|}{\big|\frac{E_d(K)}{NE_d(F)}\big|}=1.$$

Proposition 4.7(2) shows that $\alpha_{\phi/K} = \alpha_{\phi_d/K}$, and $\alpha_{\phi/F} = \alpha^2_{\phi/K} = \alpha_{\phi/K}\alpha_{\phi_d/K}$. Also,

$$\frac{c_{E'_d/F}}{c_{E_d/F}} = \frac{c_{E'_d/K}}{c_{E_d/K}}$$

by the good and split multiplicative cases of the theorem. Hence

$$\frac{c_{E'/K}}{c_{E/K}} = \Big|\frac{E'_d(K)}{NE'_d(F)}\Big| / \Big|\frac{E_d(K)}{NE_d(F)}\Big|.$$

If $p = 3$, then $\frac{c_{E'/K}}{c_{E/K}}$ is a power of 3 (Lemma 6.2) but the groups in the right-hand side are 2-groups, so $c_{E'/K} = c_{E/K}$.

Finally, suppose $p = 2$. If E_d has good reduction (so $l = p$ and the reduction is good ordinary), by [14, Prop. 8.6] $\frac{E_d(K)}{NE_d(F)}$ has order 4 or 2, corresponding to whether $\Delta_{E_d/K}$ is a norm in F/K or not, and similarly for E'. This gives the result for c/c', noting that $\Delta_{E_d/K}$ can be replaced by $\Delta_{E/K}$ in this criterion, since they differ by a 6th power (Lemma A.4).

If E_d has split multiplicative reduction, by [14, Prop. 4.1] $\frac{E_d(K)}{NE_d(F)}$ has order 2 or 1, depending on whether the Tate parameter q of E_d/K is a norm in F/K or not. Because $\Delta_{E_d/K}/q = \prod(1-q^n)^{24}$ is a square ([23, §V.3]) and $\Delta_{E/K}/\Delta_{E_d/K}$ is a 6th power, we get the same result as in the potentially ordinary case. □

7. Real and complex periods

Notation 7.1. In this section the field $\mathcal{K}$ will be $\mathbb{R}$ or $\mathbb{C}$, and $\phi : E \to E'$ a $\mathcal{K}$-rational p-isogeny of elliptic curves over $\mathcal{K}$.

Definition 7.2. The *period* of an elliptic curve $E/\mathcal{K}$ with respect to an invariant differential ω is

$$\Omega(E,\omega) = \int_{E(\mathcal{K})} |\omega| \quad \text{if } \mathcal{K} \cong \mathbb{R},$$

and

$$\Omega(E,\omega) = 2\int_{E(\mathcal{K})} |\omega \wedge \bar{\omega}| \quad \text{if } \mathcal{K} \cong \mathbb{C}.$$

Remark 7.3. For $\mathcal{K} = \mathbb{R}$, one sometimes uses the period $\Omega^+(E,\omega)$, which is obtained by integrating only over the connected component of $E(\mathbb{R})$. Thus $\Omega = \Omega^+$ or $2\Omega^+$, depending on whether or not $E(\mathbb{R})$ is connected. When working over $\mathbb{Q}$, one usually takes ω to be the global minimal differential and omits it from the notation.

Lemma 7.4. *The periods of E and E' satisfy*

$$\frac{\Omega(E,\omega)}{\Omega(E',\omega')} = \frac{|\ker\phi : E(\mathcal{K}) \to E'(\mathcal{K})|}{|\operatorname{coker}\phi : E(\mathcal{K}) \to E'(\mathcal{K})|} \cdot \Big|\frac{\omega}{\phi^*\omega'}\Big|_{\mathcal{K}}.$$

Proof. The map $\phi : E(\mathcal{K}) \to E'(\mathcal{K})$ is an n-to-1 unramified cover of $\phi(E(\mathcal{K}))$, with $n = |\ker\phi|$. Therefore, if $\mathcal{K} = \mathbb{R}$, then

$$\int_{E(\mathcal{K})} |\phi^*\omega'| = n\int_{\phi(E(\mathcal{K}))} |\omega'| = \frac{n}{[E'(\mathcal{K}) : \phi(E(\mathcal{K}))]}\int_{E'(\mathcal{K})} |\omega'|,$$

and similarly for $\omega \wedge \bar{\omega}$ when $\mathcal{K} = \mathbb{C}$. Hence

$$\frac{\Omega(E,\omega)}{\Omega(E',\omega')} = \frac{\Omega(E,\phi^*\omega')}{\Omega(E',\omega')} \cdot \frac{\Omega(E,\omega)}{\Omega(E,\phi^*\omega')} = \frac{|\ker\phi : E(\mathcal{K}) \to E'(\mathcal{K})|}{|\operatorname{coker}\phi : E(\mathcal{K}) \to E'(\mathcal{K})|} \cdot \Big|\frac{\omega}{\phi^*\omega'}\Big|_{\mathcal{K}}.$$

□

Remark 7.5. If K is an l-adic field with residue field k, then

$$\int_{E(K)} |\omega|_K = c_{E/K}\frac{|E(k)|}{|k|},$$

and $\frac{|E(k)|}{|k|}$ is the value of the Euler factor of E at $s = 1$. These local integrals enter Tate's formulation of the Birch–Swinnerton-Dyer conjecture [24]. Lemma 7.4 is the Archimedean analogue of Lemma 4.2(2).

Proposition 7.6. *The quotient* $\frac{|\ker\phi : E(\mathcal{K}) \to E'(\mathcal{K})|}{|\operatorname{coker}\phi : E(\mathcal{K}) \to E'(\mathcal{K})|}$ *is*

- p *if* $\mathcal{K} = \mathbb{C}$,
- p *if* $\mathcal{K} = \mathbb{R}$, $p \neq 2$ *and* $\ker\phi \subset E(\mathcal{K})$,
- 1 *if* $\mathcal{K} = \mathbb{R}$, $p \neq 2$ *and* $\ker\phi \not\subset E(\mathcal{K})$.

If $\mathcal{K} = \mathbb{R}$ *and* $p = 2$, *write* E *in the form* $y^2 = x^3 + ax^2 + bx$ *so that* $(0,0) \in \ker\phi$. *In this case, the quotient is*

- 1 *if* $b > 0$, *and either* $a < 0$ *or* $4b > a^2$,
- 2 *otherwise.*

Proof. When $p \neq 2$, the cokernel is trivial and the result follows immediately. For $p = 2$, the kernel has size 2, and the cokernel is computed in [6, §7.1]. □

8. Periods of elliptic curves over $\mathbb{Q}$

Finally, we turn to periods of elliptic curves over $\mathbb{Q}$.

Notation 8.1. For an elliptic curve E over $\mathbb{Q}$ we write ω for the global minimal differential on E and

$$\Omega = \Omega(E/\mathbb{R}, \omega), \qquad \Omega_{\mathbb{C}} = \Omega(E/\mathbb{C}, \omega)$$

for its real and complex periods. We similarly use ω', Ω' and $\Omega'_{\mathbb{C}}$ for $E'/\mathbb{Q}$.

Theorem 8.2. *Let $\phi : E \to E'$ be a rational p-isogeny of elliptic curves over $\mathbb{Q}$. Then the quotient Ω/Ω' is $p, 1$ or p^{-1}, and the following are equivalent:*

(1) $\Omega = \Omega'$.

(2) $\sum_l \mathrm{ord}_p(\frac{c_{E/\mathbb{Q}_l}}{c_{E'/\mathbb{Q}_l}}) \equiv \mathrm{ord}_{s=1} L(E,s) \mod 2$.

If $p \neq 2, 3$, this is also equivalent to

(3) *E has an odd number of primes of additive reduction with local root number -1.*

The quotient $\Omega_{\mathbb{C}}/\Omega'_{\mathbb{C}}$ is p or p^{-1}, and it is p if and only if $\omega = \pm\phi^*\omega'$.

Proof. By Lemma 7.4,

$$\frac{\Omega}{\Omega'} = \frac{|\ker \phi : E(\mathbb{R}) \to E'(\mathbb{R})|}{|\operatorname{coker} \phi : E(\mathbb{R}) \to E'(\mathbb{R})|} \cdot \Big|\frac{\omega}{\phi^*\omega'}\Big|.$$

The first term is p or 1 by Proposition 7.6, and the second term $|\frac{\omega}{\phi^*\omega'}|$ is either 1 or p^{-1}. So $\Omega/\Omega' \in \{1, p, p^{-1}\}$. By the same argument over $\mathbb{C}$, $|\frac{\omega}{\phi^*\omega'}|_{\mathbb{C}}$ is either 1 or p^{-2}, which immediately gives the claim for the complex periods.

It remains to prove the equivalence of (1), (2) and (3). Now $\Omega = \Omega'$ if and only if $\mathrm{ord}_p(\frac{\Omega}{\Omega'})$ is even, and we can relate this to the parity of the analytic rank and of the p^∞-Selmer rank of $E/\mathbb{Q}$:

$$\mathrm{ord}_{s=1} L(E,s) \equiv \mathrm{rk}_p\, E/\mathbb{Q} \equiv \mathrm{ord}_p \frac{\Omega}{\Omega'} + \sum_l \mathrm{ord}_p(\frac{c_{E/\mathbb{Q}_l}}{c_{E'/\mathbb{Q}_l}}) \mod 2,$$

by the p-parity conjecture over $\mathbb{Q}$ ([7, Thm. 1.4]) and Cassels' formula for the parity of the p^∞-Selmer rank for an elliptic curve with a p-isogeny ([7, Rmk. 4.4]). This proves the equivalence (1) $\Leftrightarrow$ (2).

For (2) $\Leftrightarrow$ (3), suppose $p \geqslant 5$. Then by Theorem 6.1, $\mathrm{ord}_p(\frac{c_{E/\mathbb{Q}_l}}{c_{E'/\mathbb{Q}_l}})$ is odd if and only if E has split multiplicative reduction at l. So the left-hand side in (2) is the number of primes of split multiplicative reduction. The right-hand side is determined by the global root number w of E: it is even if $w = +1$ and odd if $w = -1$. Because w is the product of local root numbers,

$$w = -\prod_l w_l$$

and the local root numbers $w_l = \pm 1$ are -1 for primes of split multiplicative reduction and $+1$ for primes of good and nonsplit multiplicative reduction, the result follows. $\square$

Lemma 8.3. *Suppose $K/\mathbb{Q}_p$ is unramified. There are no elliptic curves over K with good supersingular reduction that admit a p-isogeny.*

Proof. If E has good supersingular reduction and $K/\mathbb{Q}_p$ is unramified, Serre [20, Prop. 12] proves that the image of Galois in $\operatorname{Aut} E[p]$ contains the nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. In particular, it acts irreducibly on $E[p]$, so E/K cannot have a p-isogeny. $\square$

Lemma 8.4. *Suppose $K/\mathbb{Q}_p$ is unramified, p is odd, E/K is semistable and ω, ω' are minimal differentials on E and E'. If $\ker\phi \subset E(K)$, then $\frac{\omega}{\phi^*\omega'}$ is a p-adic unit.*

Proof. The curve E cannot have supersingular reduction (Lemma 8.3) or nonsplit multiplicative reduction (as $\ker\phi \cong \mathbb{Z}/p\mathbb{Z}$ or μ_p in the split multiplicative case, and it has no points after an unramified quadratic twist). In the good ordinary case, Proposition 4.8 gives the claim. In the split multiplicative case, see the proof of Proposition 4.10. $\square$

Lemma 8.5. *If $\phi : E \to E'$ is a p-isogeny of elliptic curves over $\mathbb{Q}$, with p odd, $\ker\phi \subset E(\mathbb{Q})$ and E is semistable at p, then $\frac{\Omega}{\Omega'} = \frac{\Omega_{\mathbb{C}}}{\Omega'_{\mathbb{C}}} = p$.*

Proof. We have

$$\frac{\Omega}{\Omega'} \overset{7.4}{=} \frac{|\ker\phi : E(\mathbb{R}) \to E'(\mathbb{R})|}{|\operatorname{coker}\phi : E(\mathbb{R}) \to E'(\mathbb{R})|} \cdot \left|\frac{\omega}{\phi^*\omega'}\right| \overset{7.6}{=} p\left|\frac{\omega}{\phi^*\omega'}\right| \overset{8.4}{=} p,$$

and similarly for $\Omega_{\mathbb{C}}$. $\square$

Remark 8.6. Note from the proof of the lemma that without the semistability assumption for real periods we still have $\Omega \geqslant \Omega'$ when $\ker\phi \subset E(\mathbb{Q})$.

Theorem 8.7. *Let $\phi : E \to E'$ be a p-isogeny of semistable elliptic curves over $\mathbb{Q}$, with p odd. Then $\frac{\Omega}{\Omega'} = \frac{\Omega_{\mathbb{C}}}{\Omega'_{\mathbb{C}}}$ is either p or p^{-1}. Moreover,*

$$\frac{\Omega}{\Omega'} = \frac{\Omega_{\mathbb{C}}}{\Omega'_{\mathbb{C}}} = p \iff \frac{\omega}{\phi^*\omega'} = \pm 1 \iff \ker\phi \subset E(\mathbb{Q}).$$

Proof. If $\ker\phi \subset E(\mathbb{Q})$, then $\frac{\omega}{\phi^*\omega'}$ is a p-adic unit by Lemma 8.4 and a unit at all other primes by Lemma 4.3, so it is ± 1. Also, $\frac{\Omega}{\Omega'} = \frac{\Omega_{\mathbb{C}}}{\Omega'_{\mathbb{C}}} = p$ by Lemma 8.5. If $\ker\phi \not\subset E(\mathbb{Q})$, then by a result of Serre ([20, p. 307]), $\ker\phi^t \subset E'(\mathbb{Q})$. The result now follows from that for ϕ^t, as

$$p \cdot \frac{\omega}{\phi^*\omega'} = \frac{\phi^*(\phi^t)^*\omega}{\phi^*\omega'} = \frac{(\phi^t)^*\omega}{\omega'} = \pm 1.$$

$\square$

Appendix A. Tate curve and quadratic twists

For completeness, we recall the following well-known facts. These concern the Tate curve and quadratic twists of elliptic curves, and do not assume that E admits a p-isogeny. As usual, K is a finite extension of $\mathbb{Q}_l$, and the notation is as in §1.1.

Theorem A.1. *An elliptic curve E/K with split multiplicative reduction of type I_n is isomorphic to a Tate curve $E^{(q)}/K$ for some Tate parameter $q \in \mathfrak{m}_K$ with $v(q) = n = \delta = -v(j) = c$. For a prime p,*

$$E^{(q)}(\bar{K}) \cong \bar{K}^\times/q^{\mathbb{Z}} \qquad \textit{and} \qquad E^{(q)}[p] \cong \langle \zeta_p, \sqrt[p]{q} \rangle$$

as Galois modules. There is a K-rational p-isogeny

$$\begin{array}{ccccccc} E^{(q)}(K) & = & K^\times/q^{\mathbb{Z}} & \longrightarrow & K^\times/q^{p\mathbb{Z}} & = & E^{(q^p)}(K) \\ & & z & \mapsto & z^p. & & \end{array}$$

The other p-isogenies from $E^{(q)}$ are parametrised by choices of a pth root of q in $\bar{K}^\times$, and given by

$$\begin{array}{ccccccc} E^{(q)}(K) & = & K^\times/q^{\mathbb{Z}} & \longrightarrow & K^\times/(\sqrt[p]{q})^{\mathbb{Z}} & = & E^{(\sqrt[p]{q})}(K) \\ & & z & \mapsto & z. & & \end{array}$$

Such an isogeny is defined over K if and only if $\sqrt[p]{q} \in K$.

Proof. For the basic theory of the Tate curve, see [23, §§V.3-V.5]. For the statements about isogenies, see [19, §A.1.4] (Theorem and the proof of (2) $\implies$ (1)), and the description of the function field of E_q in §A.1.1. □

Lemma A.2. *If E/K has potentially multiplicative reduction, both the quadratic twist of E by $-c_6$ and $E/K(\sqrt{-c_6})$ have split multiplicative reduction. Here c_6 is the standard invariant of E as in* [22, §III.1].

Proof. See [23, §V.5]. □

Lemma A.3. *Let $E/K : y^2 = f(x)$ be an elliptic curve with additive potentially good reduction. Then the following are equivalent:*

(1) *E has good reduction over a quadratic extension $K(\sqrt{d})$.*
(2) *The quadratic twist $E_d/K : dy^2 = f(x)$ has good reduction.*
(3) *The inertia group $\mathrm{Gal}(\bar{K}/K^{nr})$ acts on the ℓ-adic Tate module of E ($\ell \neq l$) through $\mathrm{Gal}(K^{nr}(\sqrt{d})/K^{nr})$.*

Proof. This follows from the criterion of Néron-Ogg-Shafarevich, and the fact that the Tate module of E_d is the Tate module module of E twisted by the character of $\mathrm{Gal}(K(\sqrt{d})/K)$ of order 2. □

Lemma A.4. *Let E/K be an elliptic curve, and E_d/K its quadratic twist by $d \in K^\times$. Then the minimal discriminants of E and E_d are related by $\Delta_{E/K} = d^6u^{12}\Delta_{E_d/K}$ for some $u \in K^\times$.*

Proof. Choose models $E : y^2 = x^3 + ax + b$ and $E_d : y^2 = x^3 + d^2ax + d^3b$. Their discriminants differ by d^6, and they differ from the minimal discriminants by 12th powers. □

Theorem A.5 ([16, Thm. 2.8])**.** *Suppose E/K has multiplicative reduction of type I_n, so $n = \delta = -v(j)$. Let $K(\sqrt{d})/K$ be a quadratic extension, and $\chi : \mathrm{Gal}(K(\sqrt{d})/K) \to \pm 1$ the corresponding character. Then the quadratic twist E_d has potentially multiplicative reduction of type $\mathrm{I}^*_{n+4f_\chi-4}$, where f_χ is the conductor exponent of χ. If $p \neq 2$, then $f_\chi = 1$ and the type is I^*_n.*

Appendix B. Values of modular forms

We briefly recall the well-known connection between values of modular forms on $\Gamma_0(N)$ and invariants of elliptic curves with a cyclic N-isogeny. In the proof of Theorem 2.1, we used the exact relation (B.2) between the discriminant of an elliptic curve and the value of the modular Δ-function, and rationality properties of values of modular forms. For the latter, the modern approach of Katz proceeds via the q-expansion principle (see [11] or [5]). For convenience of the reader, we also give a low-tech description, which relies only on classical results (Theorem B.3).

Let $E/\mathbb{C}$ be an elliptic curve with an invariant differential ω. Put (E,ω) in the form

$$E: y^2 = 4x^3 + ax + b, \qquad \omega = \frac{dx}{y}. \tag{B.1}$$

By the uniformisation theorem, there is a unique lattice $\Lambda = \mathbb{Z}\Omega_1 + \mathbb{Z}\Omega_2 \subset \mathbb{C}$ such that

$$\begin{array}{rcl} \phi : \mathbb{C}/\Lambda & \longrightarrow & E(\mathbb{C}) \\ z & \longmapsto & (\wp_\Lambda(z), \wp'_\Lambda(z)) \end{array}$$

is an isomorphism (of complex Lie groups), and $\phi^* \frac{dx}{y} = dz$. Here $\wp_\Lambda(z)$ is the Weierstrass $\wp$-function

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{v \in \Lambda \setminus \{0\}} \Big(\frac{1}{(z-v)^2} - \frac{1}{v^2} \Big).$$

The coefficients of E are $a = -60G_4(\Lambda)$ and $b = -140G_6(\Lambda)$, where the G_k are the standard modular functions

$$G_k(\Lambda) = \sum_{v \in \Lambda \setminus \{0\}} v^{-k}.$$

Let $\tau = \frac{\Omega_2}{\Omega_1}$, changing the sign of Ω_2 if necessary to get $\tau \in \mathbb{H}$. Write $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$ and $q = e^{2\pi i \tau}$. Then

$$\Lambda = \Omega_1 \Lambda_\tau, \qquad G_k(\Lambda) = \Omega_1^{-k} G_k(\Lambda_\tau),$$

and $\tau \mapsto G_k(\Lambda_\tau)$ is, up to a constant, the Eisenstein series of weight k,

$$E_k(\tau) = \frac{1}{2\zeta(k)} G_k(\Lambda_\tau) = 1 + \frac{2}{\zeta(1-2k)} \sum_{n=1}^{\infty} \frac{n^{2k-1} q^n}{1-q^n}.$$

The modular discriminant function $\Delta(\tau) = \frac{1}{1728}(E_4(\tau)^3 - E_6(\tau)^2)$ satisfies

$$\Delta(\tau) = -16\Big(4(\tfrac{a}{4})^3 + 27(\tfrac{b}{4})^2\Big) \cdot \Big(\frac{\Omega_1}{2\pi}\Big)^{12} = \Big(\frac{\Omega_1}{2\pi}\Big)^{12} \Delta_E, \tag{B.2}$$

where Δ_E is the discriminant of the Weierstrass model $y^2 = x^3 + \frac{a}{4}x + \frac{b}{4}$ of E obtained by rescaling $y \mapsto 2y$ in (B.1) (so $\frac{dx}{y}$ becomes $\frac{dx}{2y}$).

Now suppose that the pair (E,ω) is defined over a subfield $\mathcal{K} \subset \mathbb{C}$. Then $a, b, \Delta \in \mathcal{K}$, and therefore

$$\big(\tfrac{2\pi}{\Omega_1}\big)^4 E_4(\tau), \quad \big(\tfrac{2\pi}{\Omega_1}\big)^6 E_6(\tau), \quad \big(\tfrac{2\pi}{\Omega_1}\big)^{12} \Delta(\tau) \quad \in \ \mathcal{K}.$$

In fact, suppose $f(\tau)$ is any modular form on $\Gamma_0(N)$ whose q-expansion has $\mathcal{K}$-rational coefficients. For any choice of nonnegative integers m, n, u with $4m + 6n + k = 12u$, the form $\tilde{f} = fE_4^m E_6^n / \Delta^u$ on $\Gamma_0(N)$ has weight 0 (i.e. is a modular function). By a classical theorem (see [4, Thm. 11.9(b)]),

$$\tilde{f}(\tau) = F(j(\tau), j(N\tau))$$

for some rational function $F \in \mathbb{C}(x,y)$. In fact, $F \in \mathcal{K}(x,y)$ since F has a $\mathcal{K}$-rational q-expansion.[1] Summarising the whole discussion, we have

Theorem B.3. *Let $f \in M_k(\Gamma_0(N))$ be a modular form whose q-expansion has $\mathcal{K}$-rational coefficients, $\mathcal{K} \subset \mathbb{C}$. There are natural numbers m, n, u and a rational function $F \in \mathcal{K}(x,y)$ such that for every cyclic isogeny of elliptic curves $\phi : E \to E'$ of degree N, with E in the form* (B.1) *with corresponding complex lattices $\Lambda = \mathbb{Z}\Omega_1 + \mathbb{Z}\Omega_2 \subset \mathbb{C}$, $\Lambda' = \mathbb{Z}\Omega_1 + \mathbb{Z}N\Omega_2 \subset \mathbb{C}$, we have*

$$\left(\tfrac{2\pi}{\Omega_1}\right)^k f\left(\tfrac{\Omega_2}{\Omega_1}\right) = \frac{a^m b^n}{\Delta_E^u} F(j(E), j(E')).$$

In particular, if E and E' are defined over $\mathcal{K}$, the left-hand side lies in $\mathcal{K}$.

Acknowledgements

The authors would like to thank Anthony Scholl, William Hart and John Coates for discussions related to modular forms and the $\Delta(E') = \Delta(E)^p$ result, and the referee for helpful comments. The authors would also like to thank Emmanuel College, Cambridge, where the second author was based.

References

[1] B. J. Birch, *Conjectures concerning elliptic curves*, Proc. Sympos. Pure Math., Vol. VIII, Amer. Math. Soc., Providence, R.I., 1965, pp. 106–112. MR0174558 (30 #4759)

[2] K. Česnavičius, *The p-parity conjecture for elliptic curves with a p-isogeny*, 2012, arxiv: 1207.0431, to appear in J. Reine Angew. Math.

[3] John Coates, *Elliptic curves with complex multiplication and Iwasawa theory*, Bull. London Math. Soc. **23** (1991), no. 4, 321–350, DOI 10.1112/blms/23.4.321. MR1125859 (92i:11115)

[4] David A. Cox, *Primes of the form x^2+ny^2*, A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication. MR1028322 (90m:11016)

[5] Fred Diamond and John Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993), CMS Conf. Proc., vol. 17, Amer. Math. Soc., Providence, RI, 1995, pp. 39–133. MR1357209 (97g:11044)

[6] Tim Dokchitser and Vladimir Dokchitser, *Parity of ranks for elliptic curves with a cyclic isogeny*, J. Number Theory **128** (2008), no. 3, 662–679, DOI 10.1016/j.jnt.2007.02.008. MR2389862 (2009c:11079)

[7] Tim Dokchitser and Vladimir Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) **172** (2010), no. 1, 567–596, DOI 10.4007/annals.2010.172.567. MR2680426 (2011h:11069)

[8] T. Dokchitser and V. Dokchitser, *Growth of Ш in towers for isogenous curves*, preprint, 2013, arxiv:1301.4257.

[9] Vladimir Dokchitser, *Root numbers of non-abelian twists of elliptic curves*, Proc. London Math. Soc. (3) **91** (2005), no. 2, 300–324, DOI 10.1112/S0024611505015261. With an appendix by Tom Fisher. MR2167089 (2006f:11060)

[10] Basil Gordon and Dale Sinor, *Multiplicative properties of η-products*, Number theory, Madras 1987, Lecture Notes in Math., vol. 1395, Springer, Berlin, 1989, pp. 173–200, DOI 10.1007/BFb0086404. MR1019331 (90k:11050)

[1] This is clear for rational functions of $j(\tau)$, since the q-expansion of $j(\tau)$ is rational, hence Galois invariant, and $\mathbb{C}(t)^{\mathrm{Aut}(\mathbb{C}/\mathcal{K})} = \mathcal{K}(t)$. In general, write $\tilde{f}$ as a unique polynomial in $j(N\tau)$ with coefficients in $\mathbb{C}(j(\tau))$ of degree $< n$, where n is the degree of the modular polynomial $\Phi_N(x,y)$ relating $j(\tau)$ and $j(N\tau)$, and apply the same Galois invariance argument to it and its coefficients.

[11] Nicholas M. Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350. MR0447119 (56 #5434)

[12] Stefan Keil, *Examples of non-simple abelian surfaces over the rationals with non-square order Tate–Shafarevich group*, J. Number Theory **144** (2014), 25–69, DOI 10.1016/j.jnt.2014.04.018. MR3239151

[13] A. A. Klyachko, *Modular forms and representations of symmetric groups* (Russian), Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **116** (1982), 74–85, 162. Integral lattices and finite linear groups. MR687842 (85f:11034)

[14] K. Kramer and J. Tunnell, *Elliptic curves and local ε-factors*, Compositio Math. **46** (1982), no. 3, 307–352. MR664648 (83m:14031)

[15] Alain Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive* (French, with English summary), Manuscripta Math. **69** (1990), no. 4, 353–385, DOI 10.1007/BF02567933. MR1080288 (91j:11045)

[16] Dino Lorenzini, *Models of curves and wild ramification*, Pure Appl. Math. Q. **6** (2010), no. 1, Special Issue: In honor of John Tate, 41–82, DOI 10.4310/PAMQ.2010.v6.n1.a3. MR2591187 (2012a:11068)

[17] Morris Newman, *Construction and application of a class of modular functions. II*, Proc. London Math. Soc. (3) **9** (1959), 373–387. MR0107629 (21 #6354)

[18] Edward F. Schaefer, *Class groups and Selmer groups*, J. Number Theory **56** (1996), no. 1, 79–114, DOI 10.1006/jnth.1996.0006. MR1370197 (97e:11068)

[19] Jean-Pierre Serre, *Abelian l-adic representations and elliptic curves*, 2nd ed., Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. With the collaboration of Willem Kuyk and John Labute. MR1043865 (91b:11071)

[20] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques* (French), Invent. Math. **15** (1972), no. 4, 259–331. MR0387283 (52 #8126)

[21] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR0236190 (38 #4488)

[22] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210 (87g:11070)

[23] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368 (96b:11074)

[24] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, No. 306, 415–440, Soc. Math. France, Paris, 1995. MR1610977

Department of Mathematics, University of Bristol, University Walk, Bristol BS8 1TW, United Kingdom

E-mail address: tim.dokchitser@bristol.ac.uk

Department of Pure Mathematics and Mathematical Statistics, Emmanuel College, Cambridge CB2 3AP, United Kingdom

E-mail address: v.dokchitser@dpmms.cam.ac.uk

Current address: Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom

E-mail address: v.dokchitser@warwick.ac.uk