The Cassels-Tate Pairing and the Platonic Solids

Tom Fisher
Department of Pure Mathematics and Mathematical Statistics
University of Cambridge
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WB
E-mail: T.A.Fisher@dpmms.cam.ac.uk

Version: 11th October 2001

We perform descent calculations for the families of elliptic curves whose m-torsion splits as $\mu_m \times \mathbf{Z}/m\mathbf{Z}$ for $m = 3, 4$ or 5. These curves are parametrised by the modular curve $X(m) \simeq \mathbf{P}^1$, whose cusps are arranged as the vertices of one of the Platonic solids. Following McCallum [McC] we write the Cassels-Tate pairing as a sum of local pairings. In the case $m = 5$ our results extend the work of Beaver [Be].

INTRODUCTION

Let $E/\mathbf{Q}$ be an elliptic curve and let $m \geq 2$ be an integer. The process of m-descent bounds the group $E(\mathbf{Q})/mE(\mathbf{Q})$ and so gives an estimate for the Mordell-Weil rank. It is both convenient and instructive to work with special cases where the m-torsion of E takes a simple form. For example, many authors introduce 2-descent by considering the elliptic curves

$$E: \quad y^2 = (x - a_1)(x - a_2)(x - a_3) \tag{1}$$

with rational 2-torsion. More generally we consider elliptic curves E with $E[m] \simeq \mu_m \times \mathbf{Z}/m\mathbf{Z}$. For $m \geq 3$ these curves are parametrised by the modular curve $X(m)$, or strictly speaking by its open subset $Y(m)$ obtained by deleting the cusps. Our interest is in the cases $m = 3, 4$ and 5 when $X(m) \simeq \mathbf{P}^1$. Relabelling torsion gives an action of $\mathrm{PSL}_2(\mathbf{Z}/m\mathbf{Z})$ on $X(m)$ defined over $\mathbf{Q}(\mu_m)$. The quotient map $j : X(m) \to \mathbf{P}^1$ is ramified above $j = 0$, 1728 and ∞. Under stereographic projection these points are arranged as the faces, edges and vertices of one of the Platonic solids.

		$j = 0$	$j = 1728$	$j = \infty$	$\mathrm{PSL}_2(\mathbf{Z}/m\mathbf{Z})$
	Platonic Solid	#Faces	#Edges	#Vertices	Symmetries
$m = 3$	tetrahedron	4	6	4	A_4
$m = 4$	octahedron	8	12	6	S_4
$m = 5$	icosahedron	20	30	12	A_5

In particular the cusps, *i.e.* the points above $j=\infty$, form a single orbit under the action of $\mathrm{PSL}_2(\mathbf{Z}/m\mathbf{Z})$.

In §1 we prove

THEOREM 1. *Let K a number field and let $m=3,4$ or 5. Then the Tate-Shafarevich group of an elliptic curve over K may contain arbitrarily many elements of order m.*

Special cases of this result are proved in [CaVI], [Bö], [Kr], [McG], [L] and [F1]. Our method is that used in [F1]. Since $X(m)\simeq\mathbf{P}^1$ there are infinitely many elliptic curves E/K with $E[m]\simeq\mu_m\times\mathbf{Z}/m\mathbf{Z}$. We write $\alpha:E\to E'$ and $\widehat{\beta}:E\to E''$ for the isogenies with kernel μ_m and $\mathbf{Z}/m\mathbf{Z}$ respectively. We may estimate the Mordell-Weil rank using either the pair of isogenies α and $\widehat{\alpha}$, or the pair of isogenies β and $\widehat{\beta}$. In general these estimates do not agree, and an application of Dirichlet's theorem on primes in arithmetic progression suffices to prove the theorem. We do not make use of the Cassels-Tate pairing. The method does not extend to $m=7$, since the only $\mathbf{Q}$-rational points on the Klein quartic $X(7)$ are the cusps.

In §2 we give a survey of duality results for elliptic curves, and in particular the Cassels-Tate pairing. We then develop the methods of McCallum [McC] and Beaver [Be] for computing the pairing in the split torsion case. The action of $\mathrm{PSL}_2(\mathbf{Z}/m\mathbf{Z})$ is used to make explicit the parameter λ_v appearing in [Be, Theorems 1.1,1.2]. As in [F1] we find that our descent calculations are governed not only by the primes of bad reduction, but by the cusps we obtain when we reduce mod $\mathfrak{p}$. We also explain how our results may be applied to curves without split torsion, by giving an example in this direction.

In §3 we restrict to $K=\mathbf{Q}$ and $m=3$ or 5. We make explicit our various estimates for the Mordell-Weil rank. In particular the Cassels-Tate pairing is used to give a description of $S^{(m)}(E/\mathbf{Q})$ as the kernel of a skew-symmetric matrix. The explicit nature of our results enables us to compute a large amount of numerical data, and to give some interesting examples. In particular we exhibit some elliptic curves over $\mathbf{Q}$ whose Tate-Shafarevich group contains an element of order m^2.

Preliminaries on descent calculations

Let K be a field of characteristic zero. Let $\phi:C\to D$ be an isogeny of elliptic curves over K with $m=\deg\phi$. The dual isogeny $\widehat{\phi}:D\to C$ satisfies $\widehat{\phi}\circ\phi=[m]$ and $\phi\circ\widehat{\phi}=[m]$. The Weil pairing $e_\phi:C[\phi]\times D[\widehat{\phi}]\to\mu_m$ is defined in [Si1, Exercise 3.15]. We write $G_K=\mathrm{Gal}(\overline{K}/K)$ and $H^i(K,-)$ for $H^i(G_K,-)$. Taking Galois cohomology of the exact sequence

$$0\longrightarrow C[\phi]\longrightarrow C\xrightarrow{\ \phi\ }D\longrightarrow 0$$

we obtain the Kummer exact sequence

$$C(K) \xrightarrow{\phi} D(K) \xrightarrow{\delta_\phi} H^1(K, C[\phi]) \xrightarrow{\iota_\phi} H^1(K, C) \xrightarrow{\phi} H^1(K, D). \quad (2)$$

For K a number field the Selmer group attached to ϕ is

$$S^{(\phi)}(C/K) = \{\, x \in H^1(K, C[\phi]) \mid x_v \in \operatorname{im} \delta_{\phi,v} \text{ for all places } v \,\}.$$

Here our convention is that for $(*)$ a global object we write $(*)_v$ for the corresponding local object. The exact sequence (2) becomes

$$0 \longrightarrow D(K)/\phi C(K) \xrightarrow{\delta_\phi} S^{(\phi)}(C/K) \xrightarrow{\iota_\phi} Ш(C/K)[\phi] \longrightarrow 0 \qquad (3)$$

where $Ш(C/K) = \ker\left(H^1(K, C) \to \prod_v H^1(K_v, C)\right)$ is the Tate-Shafarevich group. The Selmer groups attached to ϕ and $\widehat{\phi}$ may then be used to give an upper bound for the Mordell-Weil rank.

Let E be an elliptic curve, and let T be a smooth curve of genus 1, both defined over K. We say that T is a *torsor* under E if there is a simple transitive action $E \times T \to T$ defined over K. Equivalently there is an isomorphism $\psi : T \to E$ defined over $\overline{K}$ such that the cocycle $\sigma(\psi)\psi^{-1}$ takes values in the translation subgroup of $\operatorname{Aut}(E)$. In this way we identify $H^1(K, E)$ with the set of torsors T under E, and $Ш(E/K)$ with those torsors that are everywhere locally soluble. From either point of view it is easy to define a map, sum : $\operatorname{Div}^0(T) \to E$, which identifies E as the Jacobian of T.

Other notation and conventions

Let K be a number field. We refer to K as a global field, and the completion K_v at a place v, as a local field. We abbreviate G_v for G_{K_v}. If $v = \mathfrak{p}$ is a prime we write $\operatorname{ord}_\mathfrak{p} : K_\mathfrak{p}^* \to \mathbf{Z}$ for the normalised valuation and $\mathcal{O}_\mathfrak{p}$ for the ring of integers. An object is said to be unramified if the inertia subgroup $I_\mathfrak{p} \subset G_\mathfrak{p}$ acts trivially.

We write $\zeta = \zeta_m$ for a primitive mth root of unity, so that ζ^ν runs over μ_m as ν runs over $\mathbf{Z}/m\mathbf{Z}$. In the case $m = 4$ we usually write i instead of ζ_4. In the case $m = 5$ we write $\phi = 1 + \zeta + \zeta^4$ for the golden ratio, and $\overline{\phi}$ for its conjugate. The minimal polynomials for $\zeta\overline{\phi}$ and $\zeta\phi$ are

$$\begin{array}{rcccl} f(t) & = & t^4 + 3t^3 + 4t^2 + 2t + 1 & = & ((t+1)^5 + 1)/(t+2) \\ g(t) & = & t^4 - 2t^3 + 4t^2 - 3t + 1 & = & ((t-1)^5 + t^5)/(2t-1). \end{array} \qquad (4)$$

In §2 we define a number of pairings taking values in $\mathbf{Q}/\mathbf{Z}$. We write $\operatorname{Ind}_\zeta : \mu_m \to \mathbf{Q}/\mathbf{Z}$ for the map $\zeta \mapsto 1/m$. When making explicit computations we do not hesitate to identify $\mathbf{Z}/m\mathbf{Z}$ with the subgroup $\frac{1}{m}\mathbf{Z}/\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z}$.

Finally, many of our results are stated for an arbitrary point on the modular curve $X_1(m)$ or $X(m)$. Even when not explicitly stated, we assume that this point is not a cusp.

1. SOME DESCENT CALCULATIONS

Let K a number field and let $m = 3, 4$ or 5. We discuss descent by m-isogeny for some elliptic curves parametrised by $X_1(m)$ and $X(m)$.

1.1. Elliptic curves parametrised by $X_1(m)$

Let $\phi : C \to D$ be an isogeny of elliptic curves over K with $C[\phi] \simeq \mu_m$ and $D[\widehat{\phi}] \simeq \mathbf{Z}/m\mathbf{Z}$ as Galois modules. We identify $H^1(K, C[\phi]) = K^*/K^{*m}$ and $H^1(K, D[\widehat{\phi}]) = \mathrm{Hom}(G_K, \mathbf{Z}/m\mathbf{Z})$. In order to compute the Selmer groups attached to ϕ and $\widehat{\phi}$ we must describe the images of the local connecting maps

$$\delta_v = \delta_{\phi,v} : D(K_v) \longrightarrow K_v^*/K_v^{*m}. \tag{5}$$

We consider the elliptic curves $D = D_\lambda$ with Weierstrass equations

$$\begin{array}{lrcl} m = 3 & y^2 + xy + \lambda y & = & x^3 \\ m = 4 & y^2 + xy + \lambda y & = & x^3 + \lambda x^2 \\ m = 5 & y^2 + (1 - \lambda)xy - \lambda y & = & x^3 - \lambda x^2. \end{array}$$

In each case $(x, y) = (0, 0)$ is a rational point of order m. By [Si1, Exercise 8.13] these are the universal families of elliptic curves over $\overline{K}$ with a specified rational point of order m. Thus our parameter λ is a co-ordinate on $X_1(m) \simeq \mathbf{P}^1$. For $m = 4$ or 5 the universal property also holds over K. However for $m = 3$ we have in effect excluded the infinitely many curves

$$y^2 = x^3 + d^2 \tag{6}$$

above $\lambda = \infty$. These curves have complex multiplication by $\mathbf{Z}[\zeta_3]$. We find the cusps on $X_1(m)$ by computing the discriminant $\Delta(D_\lambda)$.

	$\Delta(D_\lambda)$	cusps	η
$m = 3$	$\lambda^3(27\lambda - 1)$	$0, 1/27$	$\lambda \mapsto 1/27 - \lambda$
$m = 4$	$-\lambda^4(16\lambda - 1)$	$0, 1/16, \infty$	$\lambda \mapsto 1/16 - \lambda$
$m = 5$	$\lambda^5(\lambda^2 - 11\lambda - 1)$	$0, \infty, \phi^5, \overline{\phi^5}$	$\lambda \mapsto (\phi^5\lambda + 1)/(\lambda - \phi^5)$

In each case η is an involution of $X_1(m)$, permuting the cusps, such that

$$(\mu_m \hookrightarrow C_\lambda) \;\simeq\; (\mathbf{Z}/m\mathbf{Z} \hookrightarrow D_{\eta(\lambda)}) \quad \text{over } \mathbf{Q}(\mu_m). \tag{7}$$

There is also an action of $(\mathbf{Z}/m\mathbf{Z})^*/\{\pm 1\}$ on $X_1(m)$ given by relabelling torsion. For $m = 3$ or 4 this action is trivial. For $m = 5$ we obtain an involution

$$\lambda \mapsto -1/\lambda. \tag{8}$$

Following Vélu [V] the elliptic curves C_λ isogenous to D_λ have Weierstrass equations

$$\begin{array}{rcl} y^2+xy+\lambda y &=& x^3-5\lambda x-\lambda(7\lambda+1) \\ y^2+xy+\lambda y &=& x^3+\lambda x^2-5\lambda(\lambda+1)x+\lambda(3\lambda^2-12\lambda-1) \\ y^2+(1-\lambda)xy-\lambda y &=& x^3-\lambda x^2-5\lambda(\lambda^2+2\lambda-1)x \\ && \quad -\lambda(\lambda^4+10\lambda^3-5\lambda^2+15\lambda-1). \end{array}$$

Lemma 1.1. *Let $m=3,4$ or 5. The image of $D_\lambda[\widehat{\phi}]\simeq \mathbf{Z}/m\mathbf{Z}$ under the connecting map $\delta=\delta_\phi : D_\lambda(K)\to K^*/K^{*m}$ is generated by λ.*

Proof. The connecting map δ is given by a rational function $f\in K(D_\lambda)$ with $\operatorname{div}(f)=m.(0,0)-m.0$. The formal group [Si1, Chapter IV] may be used to resolve the issue of scaling. We find

$$f(x,y)=\begin{cases} y & m=3 \\ -y+x^2 & m=4 \\ xy+y-x^2 & m=5. \end{cases}$$

Computing f on multiples of $(0,0)$ we obtain powers of λ as claimed. ∎

We describe the image of the local connecting map (5). For $v=\mathfrak{p}$ a prime of bad reduction, the answer depends on which cusp we obtain as the reduction of λ mod $\mathfrak{p}$. We do not cover certain cases where $\mathfrak{p}\,|\,m$.

Proposition 1.2. *Let $m=3$. If $\operatorname{ord}_\mathfrak{p}(\lambda)\ge 0$ then*

$$\operatorname{im}\delta_\mathfrak{p}=\begin{cases} K_\mathfrak{p}^*/K_\mathfrak{p}^{*3} & \text{if } \operatorname{ord}_\mathfrak{p}(\lambda)>0 \\ \mathcal{O}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^{*3} & \text{if } \lambda(27\lambda-1)\not\equiv 0 \pmod{\mathfrak{p}} \\ 1 & \text{if } 27\lambda-1\equiv 0 \pmod{\mathfrak{p}}. \end{cases}$$

If $\operatorname{ord}_\mathfrak{p}(\lambda)<0$ and $\mathfrak{p}\nmid 3$ then

$$\operatorname{im}\delta_\mathfrak{p}=\begin{cases} \mathcal{O}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^{*3} & \text{if } 3\,|\operatorname{ord}_\mathfrak{p}(\lambda) \\ \langle\lambda\rangle & \text{otherwise.} \end{cases}$$

We see that the point $\lambda=\infty$, corresponding to the infinitely many curves (6), behaves to some extent as if it were a cusp.

Proposition 1.3. *Let $m=4$. If $\operatorname{ord}_\mathfrak{p}(\lambda)\ge 0$ then*

$$\operatorname{im}\delta_\mathfrak{p}=\begin{cases} K_\mathfrak{p}^*/K_\mathfrak{p}^{*4} & \text{if } \operatorname{ord}_\mathfrak{p}(\lambda)>0 \\ \mathcal{O}_\mathfrak{p}^*/\mathcal{O}_\mathfrak{p}^{*4} & \text{if } \lambda(16\lambda-1)\not\equiv 0 \pmod{\mathfrak{p}} \\ 1 \text{ or } \langle -4\rangle & \text{if } 16\lambda-1\equiv 0 \pmod{\mathfrak{p}}. \end{cases}$$

If $\operatorname{ord}_\mathfrak{p}(\lambda)<0$ and $\mathfrak{p}\nmid 2$ then

$$\operatorname{im}\delta_\mathfrak{p}=\begin{cases} K_\mathfrak{p}^{*2}/K_\mathfrak{p}^{*4} & \text{if } \lambda\in K_\mathfrak{p}^{*2} \\ \langle\lambda\rangle & \text{if } \operatorname{ord}_\mathfrak{p}(\lambda) \text{ is odd} \\ \langle\lambda,\mathcal{O}_\mathfrak{p}^{*2}\rangle & \text{otherwise.} \end{cases}$$

Moreover at a real place v, $\operatorname{im}\delta_v$ is trivial if and only if $16\lambda-1>0$.

If $\mu_4 \subset K_{\mathfrak{p}}$ then the inelegant $\langle -4 \rangle$ appearing in Proposition 1.3 vanishes. Indeed $-4 = (1+i)^4$, so $\langle -4 \rangle \subset K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*4}$ is trivial.

Proposition 1.4. *Let $m = 5$. Then*

$$\operatorname{im} \delta_{\mathfrak{p}} = \begin{cases} K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*5} & \text{if } \operatorname{ord}_{\mathfrak{p}}(\lambda) \neq 0 \\ \mathcal{O}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^{*5} & \text{if } \lambda(\lambda^2 - 11\lambda - 1) \not\equiv 0 \pmod{\mathfrak{p}} \\ 1 & \text{if } \lambda^2 - 11\lambda - 1 \equiv 0 \pmod{\mathfrak{p}} \text{ and } \mathfrak{p} \nmid 5. \end{cases}$$

The automorphism (8) of $X_1(5)$ reduces the number of cases to consider both for the statement and for the proof of Proposition 1.4.

Remark. If $\mu_m \subset K_{\mathfrak{p}}$ then we may identify

$$H^1(K_{\mathfrak{p}}, C[\phi]) = H^1(K_{\mathfrak{p}}, D[\widehat{\phi}]) = K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*m}.$$

Tate local duality (see §2.1) tells us that $\operatorname{im} \delta_{\phi,\mathfrak{p}}$ and $\operatorname{im} \delta_{\widehat{\phi},\mathfrak{p}}$ are exact annihilators with respect to the Hilbert norm residue symbol. It is instructive to check that replacing λ by $\eta(\lambda)$ in Propositions 1.2–1.4 has the effect of replacing $\delta_{\mathfrak{p}}$ by its exact annihilator.

1.2. Torsors with a diagonal action of μ_m.

In this section we prove Propositions 1.2–1.4. Following [F1] we consider certain smooth curves of genus 1 in $\mathbf{P}^{m-1}$. Specifically for $\tau_0, \tau_1, \ldots, \tau_{m-1}$ non-zero elements of K we define $T = T[\tau_0, \tau_1, \ldots, \tau_{m-1}] \subset \mathbf{P}^{m-1}$ via

$$\begin{array}{ll} m = 3 & \{ \tau_0 x_0^3 + \tau_1 x_1^3 + \tau_2 x_2^3 - x_0 x_1 x_2 = 0 \} \subset \mathbf{P}^2 \\ m = 4 & \left\{ \begin{array}{l} \tau_0 x_0^2 + x_1 x_3 - \tau_2 x_2^2 = 0 \\ \tau_1 x_1^2 + x_0 x_2 - \tau_3 x_3^2 = 0 \end{array} \right\} \subset \mathbf{P}^3 \\ m = 5 & \{ \tau_\nu x_\nu^2 + x_{\nu-1} x_{\nu+1} - \tau_{\nu-2}\tau_{\nu+2} x_{\nu-2} x_{\nu+2} = 0 \} \subset \mathbf{P}^4 \end{array}$$

where ν runs over $\mathbf{Z}/5\mathbf{Z}$, so that the curve in $\mathbf{P}^4$ is defined by 5 quadrics. In each case $T \subset \mathbf{P}^{m-1}$ is a curve of degree m, invariant under the diagonal action of μ_m given by $x_\nu \mapsto \zeta^\nu x_\nu$. The claims we make about these curves for $m = 3$ and 4 are easy to check directly. For $m = 5$ we refer to [F1].

Rescaling our co-ordinates $x_0, x_1, \ldots, x_{m-1}$ on $\mathbf{P}^{m-1}$ we see that the geometry of $T[\tau_0, \ldots, \tau_{m-1}]$ only depends on $\lambda := \prod \tau_\nu$. It may be shown that the elliptic curves C_λ introduced in §1.1 have equations

$$\begin{array}{lll} m = 3 & T[\lambda, 1, 1] & 0 = (0 : 1 : -1) \\ m = 4 & T[\lambda, 1, 1, 1] & 0 = (0 : 1 : 1 : 1) \\ m = 5 & T[\lambda, 1, 1, 1, 1] & 0 = (0 : 1 : 1 : -1 : -1). \end{array}$$

Thus $T[\tau_0, \ldots, \tau_{m-1}]$ is a smooth curve of genus 1, provided $\lambda = \prod \tau_\nu$ is not a cusp of $X_1(m)$. At the cusps we obtain collections of lines arranged in an m-gon. For example $T[\frac{1}{3}, \frac{1}{3}, \frac{1}{3}]$ has equation

$$(x_0 + x_1 + x_2)(x_0 + \zeta x_1 + \zeta^2 x_2)(x_0 + \zeta^2 x_1 + \zeta x_2) = 0.$$

With reference to the exact sequence (2) we define $C_{\lambda,\theta}$ to be the torsor under C_λ described by $\theta \in K^*/K^{*m}$.

LEMMA 1.5. *Let $\tau_0, \dots, \tau_{m-1}$ be non-zero elements of K with*

$$\prod \tau_\nu = \lambda \quad \textit{and} \quad \prod \tau_\nu^\nu \equiv \theta \mod K^{*m}. \tag{9}$$

Then $T[\tau_0, \dots, \tau_{m-1}] \simeq C_{\lambda,\theta}$ and $T[\tau_0, \dots, \tau_{m-1}]$ meets the co-ordinate hyperplane $\{x_\nu = 0\}$ in m points, each with field of definition $K(\sqrt[m]{\lambda^{-\nu}\theta})$.

Proof. An isomorphism between $T[\tau_0, \dots, \tau_{m-1}]$ and $C_\lambda = T[\lambda, 1, \dots, 1]$ is given by rescaling co-ordinates over $\overline{K}$. Comparing this isomorphism with its Galois conjugates we obtain a cocycle taking values in μ_m. This cocycle corresponds[1] to θ^{-1} under $H^1(K, \mu_m) \simeq K^*/K^{*m}$. The final statement follows by direct calculation. ∎

We outline the proof of Propositions 1.2–1.4. First by (2) we know that $\theta \in \operatorname{im} \delta_v$ if and only if $C_{\lambda,\theta}(K_v) \neq \emptyset$. We also know that $\operatorname{im} \delta_v$ is a group and by Lemma 1.1 it contains λ. These observations reduce us to considering a handful of cases depending on λ and θ. In each case we choose $\tau_0, \dots, \tau_{m-1}$ satisfying (9). Then Lemma 1.5 provides equations for $C_{\lambda,\theta}$ as a curve in $\mathbf{P}^{m-1}$. If $v = \mathfrak{p}$ is a prime we reduce these equations mod $\mathfrak{p}$ to help us decide whether $C_{\lambda,\theta}(K_\mathfrak{p}) \neq \emptyset$.

We summarise the proof of Proposition 1.2 in a table. We write k for the residue field mod $\mathfrak{p}$ and n for a negative integer. We abbreviate $\operatorname{ord}_\mathfrak{p}(\tau_\nu) := (\operatorname{ord}_\mathfrak{p}(\tau_0), \dots, \operatorname{ord}_\mathfrak{p}(\tau_{m-1}))$.

	Condition on λ	$\operatorname{ord}_\mathfrak{p}(\theta)$	$\operatorname{ord}_\mathfrak{p}(\tau_\nu)$	Reduction mod $\mathfrak{p}$
(a)	$\operatorname{ord}_\mathfrak{p}(\lambda) > 0$	—	all ≥ 0	rational curves defined over k
(b)	$\operatorname{ord}_\mathfrak{p}(\lambda) = 0$	1	$(-1, 0, 1)$	—
(c)	$\lambda(27\lambda - 1) \not\equiv 0$	0	$(0, 0, 0)$	smooth curve of genus 1
(d)	$27\lambda - 1 \equiv 0$	0	$(0, 0, 0)$	3 lines defined over $k(\sqrt[3]{\theta})$
(e)	$\operatorname{ord}_\mathfrak{p}(\lambda) = 3n$	1	$(n-1, n, n+1)$	—
(f)	$\operatorname{ord}_\mathfrak{p}(\lambda) = 3n$	0	(n, n, n)	smooth curve of genus 1
(g)	$\operatorname{ord}_\mathfrak{p}(\lambda) = 3n + \varepsilon$ $\varepsilon = 1$ or 2	0	$(n + \varepsilon, n, n)$	3 lines defined over $k(\sqrt[3]{\theta})$

In cases (a), (c), (f) we may pick a smooth k-point on the reduction. Hensel's lemma then shows that $C_{\lambda,\theta}(K_\mathfrak{p}) \neq \emptyset$. In cases (b) and (e) we

[1]Let us note that $C_{\lambda,\theta}$ and $C_{\lambda,\theta^{-1}}$ are isomorphic as curves, but not as torsors.

assume there is a $K_\mathfrak{p}$-point $(x_0 : x_1 : x_2)$ with $\min \mathrm{ord}_\mathfrak{p}(x_\nu) = 0$ and proceed to a contradiction by repeated use of the ultrametric law.

In cases (d) and (g) the reduction is a collection of 3 distinct lines each defined over $k(\sqrt[3]{\theta})$. The lines are distinct since by assumption $\mathfrak{p} \nmid 3$. We claim $C_{\lambda,\theta}(K_\mathfrak{p}) \neq \emptyset$ if and only if θ is a cube, equivalently θ is a cube mod $\mathfrak{p}$. So suppose given a $K_\mathfrak{p}$-point on $C_{\lambda,\theta}$. If it reduces to a smooth point, then one of our lines is defined over k, and θ is a cube as required. It remains to consider the singular points of the reduction, *i.e.* where the three lines meet. In case (d) the lines are arranged in a triangle. If a vertex is k-rational, then so is the opposite side and we are done. In case (g) all 3 lines pass through $(1 : 0 : 0)$. But if the $K_\mathfrak{p}$-point $(x_0 : x_1 : x_2)$ has reduction $(1 : 0 : 0)$ then $\mathrm{ord}_\mathfrak{p}(x_0) = 0$, $\mathrm{ord}_\mathfrak{p}(x_1) > 0$ and $\mathrm{ord}_\mathfrak{p}(x_2) > 0$. So

$$\mathrm{ord}_\mathfrak{p}(\tau_1 x_1^3),\ \mathrm{ord}_\mathfrak{p}(\tau_2 x_2^3),\ \mathrm{ord}_\mathfrak{p}(x_0 x_1 x_2) \geq n + 3$$

yet $\mathrm{ord}_\mathfrak{p}(\tau_0 x_0^3) = n + \varepsilon$, and this contradicts the ultrametric law. So there are no $K_\mathfrak{p}$-points above the singular point, and our claim follows as before. This completes the proof of Proposition 1.2.

Again we draw up a table for the proof of Proposition 1.3. We take n, n_0, n_1 negative integers with $n = n_0 + n_1$.

	Condition on λ	$\mathrm{ord}_\mathfrak{p}(\theta)$	$\mathrm{ord}_\mathfrak{p}(\tau_\nu)$	Reduction mod $\mathfrak{p}$
(a)	$\mathrm{ord}_\mathfrak{p}(\lambda) > 0$	—	all ≥ 0	rational curves defined over k
(b)	$\mathrm{ord}_\mathfrak{p}(\lambda) = 0$	2	$(-2, 0, 0, 2)$	—
(c)	$\lambda(16\lambda - 1) \not\equiv 0$	0	$(0, 0, 0, 0)$	smooth curve of genus 1
(d)	$16\lambda - 1 \equiv 0$	0	$(0, 0, 0, 0)$	4 lines defined over $k(\sqrt[4]{\theta})$
(e)	$\mathrm{ord}_\mathfrak{p}(\lambda) = 2n$	1	$(n-1, 0, n, 1)$	—
(f)	$\mathrm{ord}_\mathfrak{p}(\lambda) = 2n$	0	$(0, n, 0, n)$	2 conics defined over $k(\sqrt{\theta})$
		$2n_0$	(n_0, n_1, n_0, n_1)	4 lines defined over $k(\sqrt{\theta}, \sqrt{\lambda\theta})$
		$2n$	$(n, 0, n, 0)$	2 conics defined over $k(\sqrt{\lambda\theta})$
(g)	$\mathrm{ord}_\mathfrak{p}(\lambda) = 2n + 1$	0	$(1, n, 0, n)$	4 lines defined over $k(\sqrt[4]{\theta})$

All except cases (d) and (f) go through as before. In these cases our assumptions give $\mathfrak{p} \nmid 2$. In case (d) the reduction is a collection of 4 lines arranged in a quadrilateral. Each line has field of definition $k(\sqrt[4]{\theta})$. It follows by elementary Galois theory that each vertex has field of definition $k(\sqrt[4]{-4\theta})$. So if $C_{\lambda,\theta}(K_\mathfrak{p}) \neq \emptyset$ then either $\theta \in K_\mathfrak{p}^{*4}$ or $-4\theta \in K_\mathfrak{p}^{*4}$. Thus $\mathrm{im}\,\delta_\mathfrak{p} = 1$ or $\langle -4 \rangle$. In fact the theory of the Néron model provides a formula for $|\operatorname{im}\delta_{\mathfrak{p}}|$. By [Sc1, Lemma 3.8] and Tate's algorithm [Si2, IV.9] we deduce

$$\operatorname{im}\delta_{\mathfrak{p}} = \begin{cases} 1 & \text{if } \operatorname{ord}_{\mathfrak{p}}(16\lambda-1) \text{ is odd} \\ \langle -4 \rangle & \text{if } \operatorname{ord}_{\mathfrak{p}}(16\lambda-1) \text{ is even.} \end{cases}$$

In case (f) we have $\operatorname{ord}_{\mathfrak{p}}(\lambda) = 2n$ for some $n < 0$. We write $n = n_0 + n_1$ with $n_0, n_1 \le 0$. We assume that $\operatorname{ord}_{\mathfrak{p}}(\theta)$ is even. If θ satisfies one of the following conditions, then our table shows that $C_{\lambda,\theta}(K_{\mathfrak{p}}) \neq \emptyset$

(i) $\theta \in K_{\mathfrak{p}}^{*2}$ and $\operatorname{ord}_{\mathfrak{p}}(\theta) \equiv 0 \pmod 4$
(ii) $\theta \in K_{\mathfrak{p}}^{*2}$ and $\lambda\theta \in K_{\mathfrak{p}}^{*2}$
(iii) $\lambda\theta \in K_{\mathfrak{p}}^{*2}$ and $\operatorname{ord}_{\mathfrak{p}}(\lambda\theta) \equiv 0 \pmod 4$.

Conversely, we must show that if $C_{\lambda,\theta}(K_{\mathfrak{p}}) \neq \emptyset$ then at least one of the conditions (i), (ii) or (iii) is satisfied. We write $C_{\lambda,\theta}$ in the form $T[\tau_0, \ldots, \tau_3]$ with $\operatorname{ord}_{\mathfrak{p}}(\tau_\nu) = (n_0, n_1, n_0, n_1)$. Replacing θ by $\lambda\theta$ if necessary, we may suppose $\lambda\theta \notin K_{\mathfrak{p}}^{*2}$ and $n_0 < 0$. We take $(x_0 : \ldots : x_3)$ a $K_{\mathfrak{p}}$-point with $\min\{\operatorname{ord}_{\mathfrak{p}}(x_\nu)\} = 0$ and recall the equations

$$\begin{aligned} \tau_0 x_0^2 + x_1 x_3 - \tau_2 x_2^2 &= 0 \qquad (10) \\ \tau_1 x_1^2 + x_0 x_2 - \tau_3 x_3^2 &= 0. \qquad (11) \end{aligned}$$

Since $\tau_0/\tau_2 \notin K_{\mathfrak{p}}^{*2}$ the equation (10) tells us $\operatorname{ord}_{\mathfrak{p}}(x_0), \operatorname{ord}_{\mathfrak{p}}(x_2) > 0$. Next by (11) we have $\tau_1/\tau_3 \in K_{\mathfrak{p}}^{*2}$ and $\operatorname{ord}_{\mathfrak{p}}(x_1) = \operatorname{ord}_{\mathfrak{p}}(x_3) = 0$. Again using (10) we see that n_0 is even. So condition (i) holds and we our done.

To complete the proof of Proposition 1.3, it only remains to consider v a real place. If $\theta < 0$ we may write $C_{\lambda,\theta}$ in the form

$$\begin{aligned} (16\lambda - 1)x_0^2 + (x_0 + x_2)^2 + (x_1 + x_3)^2 &= 0 \\ (16\lambda - 1)x_0^2 + (x_0 - x_2)^2 - (x_1 - x_3)^2 &= 0. \end{aligned}$$

It is readily seen that $C_{\lambda,\theta}(\mathbf{R}) = \emptyset$ if and only if $16\lambda - 1 > 0$. This is then the condition for $\operatorname{im}\delta_v$ to be trivial.

Finally Proposition 1.4 is a restatement of [F1, Proposition 2.15]. We therefore omit details of the proof, which is in any case similar to the above.

1.3. Elliptic curves parametrised by $X(m)$

We recall that the K-points of the modular curve $Y(m)$ correspond to isomorphism classes of triples (E, P, Q) where E/K is an elliptic curve, $P, Q \in E[m]$, $e_m(P,Q) = \zeta$ and $Q \in E(K)$. For $m = 3, 4$ or 5 it follows by Lemma 1.1 that $X(m) \simeq \mathbf{P}^1$. We make a choice of co-ordinate t on $X(m)$ by writing

$m = 3$	$E_t = C_{t^3/27}$	$X(3)$ has cusps at $t = 0, 1, \zeta, \zeta^2$
$m = 4$	$E_t = C_{t^4/16}$	$X(4)$ has cusps at $t = 0, \infty, \pm 1, \pm i$
$m = 5$	$E_t = C_{t^5}$	$X(5)$ has cusps at $t = 0, \infty, \zeta^\nu\phi, \zeta^\nu\overline{\phi}$.

The configuration of these cusps was described in the introduction. The work of §1.2 allows us to identify E_t as the Jacobian of X_t, where X_t has equations

$$\begin{array}{ll} m=3 & \{\, t(x_0^3+x_1^3+x_2^3)-3x_0x_1x_2=0 \,\} \subset \mathbf{P}^2 \\ m=4 & \left\{ \begin{array}{l} t(x_0^2+x_2^2)+2x_1x_3=0 \\ t(x_1^2+x_3^2)+2x_0x_2=0 \end{array} \right\} \subset \mathbf{P}^3 \\ m=5 & \{\, tx_\nu^2+x_{\nu-1}x_{\nu+1}-t^2x_{\nu-2}x_{\nu+2}=0 \,\} \subset \mathbf{P}^4 \end{array}$$

These curves are taken from [H, Chapter III]. They are invariant under the action of the Heisenberg group, generated by $\sigma_P : x_\nu \mapsto \zeta^\nu x_\nu$ and $\sigma_Q : x_\nu \mapsto x_{\nu-1}$. We write P_t, Q_t for the basis of $E_t[m]$ determined by σ_P, σ_Q. Computing the commutator of σ_P and σ_Q shows that $e_m(P_t,Q_t)=\zeta$. We may therefore take (E_t,P_t,Q_t) as our triple above t. In the cases $m=3$ and 5, it is possible to identify $E_t=X_t$ via $0=(0:1:-1)$ and $0=(0:t:1:-1:-t)$ respectively.

Let $S=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ and $T=\begin{pmatrix}1&1\\0&1\end{pmatrix}$ be the usual generators for $\mathrm{SL}_2(\mathbf{Z})$. We use the same letters to denote their images in $\mathrm{PSL}_2(\mathbf{Z}/m\mathbf{Z})$. Writing M^* for $(M^T)^{-1}$ we have $S^*=S$ and $T^*=STS$.

PROPOSITION 1.6. *There is an action of* $\mathrm{PSL}_2(\mathbf{Z}/m\mathbf{Z})$ *on* $X(m)$ *via*

$$\begin{pmatrix}a&b\\c&d\end{pmatrix} : (E,P,Q) \mapsto (E, aP+bQ, cP+dQ).$$

In terms of our co-ordinate t *on* $X(m)$ *it is given by*

$$\begin{array}{lll} m=3 & S: t\mapsto (-t+1)/(2t+1) & T^*: t\mapsto \zeta t \\ m=4 & S: t\mapsto (-t+1)/(t+1) & T^*: t\mapsto \zeta t \\ m=5 & S: t\mapsto (\phi t+1)/(t-\phi) & T^*: t\mapsto \zeta t. \end{array}$$

Proof. (i) There is an isomorphism $X_t \simeq X_{\zeta t}$ given by

$$\begin{array}{lll} (x_0:x_1:x_2) & \mapsto & (\zeta_3 x_0 : x_1 : x_2) \\ (x_0:x_1:x_2:x_3) & \mapsto & (x_0 : \zeta_8 x_1 : -x_2 : \zeta_8 x_3) \\ (x_0:x_1:x_2:x_3:x_4) & \mapsto & (\zeta_5^3 x_0 : \zeta_5 x_1 : x_2 : x_3 : \zeta_5 x_4). \end{array}$$

where $\zeta_8^2=\zeta_4$. Passing to the Jacobian we obtain an isomorphism $(E_t,P_t,Q_t) \simeq (E_{\zeta t}, P_{\zeta t}, P_{\zeta t}+Q_{\zeta t})$. It follows that $T^*: t\mapsto \zeta t$ as claimed.
(ii) For suitable t', an isomorphism $X_{t'} \simeq X_t$ is given by

$$(x_0:x_1:\ldots:x_{m-1}) \mapsto (\textstyle\sum x_\nu : \sum \zeta^\nu x_\nu : \ldots : \sum \zeta^{(m-1)\nu} x_\nu) \qquad (12)$$

where each sum runs over $\nu \in \mathbf{Z}/m\mathbf{Z}$. Passing to the Jacobian we obtain an isomorphism $(E_{t'},P_{t'},Q_{t'}) \simeq (E_t,-Q_t,P_t)$. It follows that $S: t\mapsto t'$.

Finally we compute t' by substituting (12) into the equations for X_t. For $m=3$ or 5 a number of short-cuts are available since $E_t = X_t$. ∎

Let $E = E_t$ for some $t \in K$. Then $E[m] \simeq \mu_m \times \mathbf{Z}/m\mathbf{Z}$ as a Galois module. We write E' (respectively E'') for the elliptic curve isogenous to E obtained as the quotient by μ_m (respectively $\mathbf{Z}/m\mathbf{Z}$). The isogenies

$$\alpha : E \to E' \quad \text{and} \quad \beta : E'' \to E$$

are both of the form $\phi : C_\lambda \to D_\lambda$ but for different values of $\lambda \in K$. In order to apply Propositions 1.2–1.4 we record these values of λ. In the case $m=5$ the answer involves the polynomials $f(t)$ and $g(t)$ defined by (4).

	$m=3$		$m=4$		$m=5$	
	λ	$27\lambda - 1$	λ	$16\lambda - 1$	λ	$\lambda^2 - 11\lambda - 1$
α	$t^3/27$	$t^3 - 1$	$t^4/16$	$t^4 - 1$	t^5	$(t^2 - t - 1)f(t)g(t)$
β	$\frac{t(t^2+t+1)}{3(2t+1)^3}$	$\left(\frac{t-1}{2t+1}\right)^3$	$\frac{t(t^2+1)}{2(t+1)^4}$	$\left(\frac{t-1}{t+1}\right)^4$	$tf(t)/g(t)$	$(t^2 - t - 1)^5/g(t)^2$

The entries for the isogeny α are immediate from the definition of E_t. The entries for the isogeny β follow from Proposition 1.6 and the involution η on $X_1(m)$ defined in §1.1. For example, taking $m=3$ there is an isomorphism

$$(\mu_3 \times \mathbf{Z}/3\mathbf{Z} \hookrightarrow E_t) \simeq (\mathbf{Z}/3\mathbf{Z} \times \mu_3 \hookrightarrow E_{t'})$$

where $t' = (-t+1)/(2t+1)$. So the required value of λ is $\eta((t')^3/27) = t(t^2+t+1)/(3(2t+1)^3)$.

Proposition 1.7. *Let $m = 3, 4$ or 5. Let $\mathfrak{p}$ be a prime of bad reduction for $E = E_t$. Suppose that $\mu_m \subset K_\mathfrak{p}$ and $\mathfrak{p} \nmid m$. Then t reduces to a cusp mod $\mathfrak{p}$ and the local connecting maps have images*

$m=3$	$t \bmod \mathfrak{p}$	0	ζ, ζ^2	1
	$\operatorname{im} \delta_{\alpha,\mathfrak{p}}$	$K_\mathfrak{p}^*/K_\mathfrak{p}^{*3}$	1	1
	$\operatorname{im} \delta_{\beta,\mathfrak{p}}$	$K_\mathfrak{p}^*/K_\mathfrak{p}^{*3}$	$K_\mathfrak{p}^*/K_\mathfrak{p}^{*3}$	1

$m=4$	$t \bmod \mathfrak{p}$	0	∞	$\pm i$	-1	1
	$\operatorname{im} \delta_{\alpha,\mathfrak{p}}$	$K_\mathfrak{p}^*/K_\mathfrak{p}^{*4}$	$K_\mathfrak{p}^{*2}/K_\mathfrak{p}^{*4}$	1	1	1
	$\operatorname{im} \delta_{\beta,\mathfrak{p}}$	$K_\mathfrak{p}^*/K_\mathfrak{p}^{*4}$	$K_\mathfrak{p}^*/K_\mathfrak{p}^{*4}$	$K_\mathfrak{p}^*/K_\mathfrak{p}^{*4}$	$K_\mathfrak{p}^{*2}/K_\mathfrak{p}^{*4}$	1

$m=5$	$t \bmod \mathfrak{p}$	0	$\zeta^\nu \phi, \zeta^\nu \overline{\phi}$ $(\nu \neq 0)$	$\phi, \overline{\phi}$
	$\operatorname{im} \delta_{\alpha,\mathfrak{p}}$	$K_\mathfrak{p}^*/K_\mathfrak{p}^{*5}$	1	1
	$\operatorname{im} \delta_{\beta,\mathfrak{p}}$	$K_\mathfrak{p}^*/K_\mathfrak{p}^{*5}$	$K_\mathfrak{p}^*/K_\mathfrak{p}^{*5}$	1

Proof. This follows from Propositions 1.2–1.4 and the table above. The assumption $\mu_m \subset K_\mathfrak{p}$ is made purely to simplify the statement of the proposition in the case $m=4$. ∎

1.4. Large Tate-Shafarevich groups

Let $E = E_t$ as above. There are exact sequences

$$0 \longrightarrow S^{(\alpha)}(E/K) \longrightarrow S^{(m)}(E/K) \xrightarrow{\alpha} S^{(\widehat{\alpha})}(E'/K) \tag{13}$$

$$0 \longrightarrow S^{(\widehat{\beta})}(E/K) \longrightarrow S^{(m)}(E/K) \xrightarrow{\widehat{\beta}} S^{(\beta)}(E''/K). \tag{14}$$

Propositions 1.2–1.4 allow us the estimate the Selmer groups attached to $\alpha, \widehat{\alpha}, \beta$ and $\widehat{\beta}$. We show that for a careful choice of t the group $S^{(\widehat{\alpha})}(E'/K)$ may be large compared to both $S^{(\widehat{\beta})}(E/K)$ and $S^{(\beta)}(E''/K)$. It follows that Ш(E'/K) may become arbitrarily large. More precisely we prove

THEOREM 1. *Let K a number field and let $m = 3, 4$ or 5. Then the Tate-Shafarevich group of an elliptic curve over K may contain arbitrarily many elements of order m.*

We stress that our theorem applies to *any* number field K, for example $K = \mathbf{Q}$. We give details of the proof.

LEMMA 1.8. *We may choose $\mathcal{S}_1$ and $\mathcal{S}_2$ finite disjoint set of primes, and $X \subset H^1(K, \mathbf{Z}/m\mathbf{Z})$ a finite subgroup such that*
(i) Each prime $\mathfrak{p} \in \mathcal{S}_1 \cup \mathcal{S}_2$ satisfies $\operatorname{Norm} \mathfrak{p} \equiv 1 \pmod{m}$.
(ii) The map $X \to \prod_{\mathfrak{p} \in \mathcal{S}_1} H^1(K_\mathfrak{p}, \mathbf{Z}/m\mathbf{Z})$ is injective.
(iii) X is unramified outside $\mathcal{S}_2$.
(iv) X contains arbitrarily many elements of order m.

Proof. By class field theory there exists L/K an abelian extension whose Galois group contains arbitrarily many elements of order m, and that is unramified outside a finite set of primes $\mathcal{S}_2$ satisfying (i). We may suppose $L \cap K(\mu_m) = K$ and take $X = \operatorname{Hom}(\operatorname{Gal}(L/K), \mathbf{Z}/m\mathbf{Z})$. By the Tchebotarev density theorem there exists a finite set of primes $\mathcal{S}_1$ satisfying the remaining conditions. ∎

With $\mathcal{S}_1$, $\mathcal{S}_2$ and X as above, we impose congruence conditions on t.

$$\begin{array}{lrll}
m = 3 & t^2 + t + 1 \equiv 0 & \pmod{\mathfrak{p}} & \text{for all } \mathfrak{p} \in \mathcal{S}_1 \\
 & t - 1 \equiv 0 & \pmod{\mathfrak{p}} & \text{for all } \mathfrak{p} \in \mathcal{S}_2 \\
m = 4 & t^2 + 1 \equiv 0 & \pmod{\mathfrak{p}} & \text{for all } \mathfrak{p} \in \mathcal{S}_1 \\
 & t - 1 \equiv 0 & \pmod{\mathfrak{p}} & \text{for all } \mathfrak{p} \in \mathcal{S}_2 \\
m = 5 & t^4 + 3t^3 + 4t^2 + 2t + 1 \equiv 0 & \pmod{\mathfrak{p}} & \text{for all } \mathfrak{p} \in \mathcal{S}_1 \\
 & t^2 - t - 1 \equiv 0 & \pmod{\mathfrak{p}} & \text{for all } \mathfrak{p} \in \mathcal{S}_2
\end{array}$$

By Lemma 1.8(i) and the Chinese Remainder Theorem these conditions may be replaced by a single linear congruence. Now let $t \in K$ be an algebraic integer satisfying this congruence and write $\mathcal{S}$ for the set of primes dividing m and t together with the infinite places. By Dirichlet's theorem on primes in arithmetic progression (or perhaps a weaker result) we may assume that $|\mathcal{S}|$ is bounded by a constant only depending on K.

Propositions 1.2–1.4 and Tate local duality (see §2.1) now give

(a) If $\mathfrak{p} \notin \mathcal{S}$ then $\operatorname{im} \delta_{\alpha,\mathfrak{p}} \subset \mathcal{O}_{\mathfrak{p}}^{*}/\mathcal{O}_{\mathfrak{p}}^{*m}$ and $\operatorname{im} \delta_{\widehat{\alpha},\mathfrak{p}} \supset \operatorname{Hom}(G_{\mathfrak{p}}/I_{\mathfrak{p}}, \mathbf{Z}/m\mathbf{Z})$.
(b) If $\mathfrak{p} \in \mathcal{S}_1 \cup \mathcal{S}_2$ then $\operatorname{im} \delta_{\alpha,\mathfrak{p}} = 1$ and $\operatorname{im} \delta_{\widehat{\alpha},\mathfrak{p}} = \operatorname{Hom}(G_{\mathfrak{p}}, \mathbf{Z}/m\mathbf{Z})$.
(c) If $\mathfrak{p} \in \mathcal{S}_1$ then $\operatorname{im} \delta_{\beta,\mathfrak{p}} = K_{\mathfrak{p}}^{*}/K_{\mathfrak{p}}^{*m}$ and $\operatorname{im} \delta_{\widehat{\beta},\mathfrak{p}} = 0$.
(d) If $\mathfrak{p} \in \mathcal{S}_2$ then $\operatorname{im} \delta_{\beta,\mathfrak{p}} = 1$ and $\operatorname{im} \delta_{\widehat{\beta},\mathfrak{p}} = \operatorname{Hom}(G_{\mathfrak{p}}, \mathbf{Z}/m\mathbf{Z})$.

We make two claims, namely that the groups $X/(X \cap S^{(\widehat{\alpha})}(E'/K))$ and $X \cap \alpha S^{(m)}(E/K)$ are bounded by constants only depending on K. By (a), (b) and Lemma 1.8(iii) we have

$$\begin{array}{rcl} X \cap S^{(\widehat{\alpha})}(E'/K) & = & \{\, x \in X \mid x_v \in \operatorname{im} \delta_{\widehat{\alpha},v} \text{ for all places } v \,\} \\ & \supset & \{\, x \in X \mid x_v = 0 \text{ for all } v \in \mathcal{S} \,\}. \end{array}$$

Our first claim follows from our assumption on $|\mathcal{S}|$.

Now let $Y = \alpha^{-1} X \cap S^{(m)}(E/K)$. By (a) we know that $S^{(\alpha)}(E/K)$ is unramified outside $\mathcal{S}$. Then (13) and Lemma 1.8(iii) show that Y is unramified outside $\mathcal{S} \cup \mathcal{S}_2$. Next (c) and Lemma 1.8(ii) give $S^{(\widehat{\beta})}(E/K) \cap X = 0$. From the exact sequence (14) we learn that Y injects into $S^{(\beta)}(E''/K)$. But (d) tells us that this Selmer group is unramified at all primes in $\mathcal{S}_2$. We deduce that Y is unramified outside $\mathcal{S}$. So Y is bounded by a constant only depending on K. Our second claim follows.

Finally the cokernel of the map $S^{(m)}(E/K) \to S^{(\widehat{\alpha})}(E'/K)$ injects into $Ш(E'/K)$ and we have shown that this cokernel may contain arbitrarily many elements of order m. This completes the proof of the theorem.

Remark. To establish the existence of arbitrarily large Selmer groups, a lesser assumption on the torsion is required. In particular for $m = 3, 5$ or 7 we have $X_1(m) \simeq \mathbf{P}^1$, and $S^{(m)}(E/K)$ may become arbitrarily large. We refer to [F1], [Kl] or [Sc2] for details. Kloosterman [Kl] also treats the case $m = 13$ using the fact $X_0(13) \simeq \mathbf{P}^1$.

2. THE CASSELS-TATE PAIRING

We give a survey of duality results for elliptic curves, and in particular the Cassels-Tate pairing. One reason for including this material is that we could not find a clear reference for our Theorem 3 in the existing literature, although a proof conditional on the finiteness of Ш appears in the work of Cassels [CaVIII, Corollary to Theorem 1.2]. In a number of proofs it is tacitly assumed that the divisors chosen have disjoint supports. We also leave it to the reader to check that certain *a priori* infinite sums are in fact finite.

2.1. Local duality theorems

Let K be a local field. Let M be a finite G_K-module. We define the Cartier dual $M^\vee = \mathrm{Hom}(M, \overline{K}^*)$. The (local) Tate pairing

$$H^1(K,M) \times H^1(K,M^\vee) \to \mathbf{Q}/\mathbf{Z} \tag{15}$$

is defined as the cup product map induced by the canonical pairing $M \times M^\vee \to \overline{K}^*$ followed by the invariant map $\mathrm{Br}(K) \to \mathbf{Q}/\mathbf{Z}$. As a special case we take $\phi : C \to D$ an isogeny of elliptic curves and $M = C[\phi]$.

$$H^1(K,C[\phi]) \times H^1(K,D[\widehat{\phi}]) \to \mathbf{Q}/\mathbf{Z} \tag{16}$$

In terms of cocycles $a = \{a_\sigma\}_\sigma$ and $b = \{b_\sigma\}_\sigma$ this pairing is given by

$$(a,b) \mapsto \mathrm{inv}\{e_\phi(a_\sigma, \sigma b_\tau)\}_{\sigma,\tau}$$

Now let E be an elliptic curve over K. Taking Galois cohomology of the exact sequence

$$0 \to \overline{K}(E)^*/\overline{K}^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(E) \xrightarrow{\mathrm{sum}} E \to 0$$

we obtain

$$H^1(K,E) \xrightarrow{\delta} H^2(K, \overline{K}(E)^*/\overline{K}^*) \xrightarrow{\mathrm{div}} H^2(K, \mathrm{Div}^0(E)).$$

There is another local pairing due to Tate

$$E(K) \times H^1(K,E) \to \mathbf{Q}/\mathbf{Z}\,; \quad (x,y) \mapsto -\mathrm{inv} f(\mathfrak{x}) \tag{17}$$

where $\mathrm{sum}(\mathfrak{x}) = x$ and $f = \delta(y)$. Weil reciprocity [Si1, Exercise 2.11] shows that this pairing is well defined. Indeed if $\mathfrak{x} = \mathrm{div}(g)$ for some g in $\overline{K}(E)$, then

$$f(\mathfrak{x}) = f(\mathrm{div}\, g) = g(\mathrm{div}\, f) = 0.$$

PROPOSITION 2.1. *The Tate pairings (16) and (17) are compatible with the Kummer exact sequence (2). In other words, if $a \in H^1(K, C[\phi])$ and $b \in H^1(K, D[\widehat{\phi}])$ with $\delta_\phi : x \mapsto a$ and $\iota_{\widehat{\phi}} : b \mapsto y$ then $(a,b) = (x,y)$.*

Proof. Let $b = \{b_\sigma\}_\sigma$ and let $\mathfrak{x}$, $\mathfrak{b}_\sigma \in \mathrm{Div}^0(D)$ with $\mathrm{sum}(\mathfrak{x}) = x$ and $\mathrm{sum}(\mathfrak{b}_\sigma) = b_\sigma$. We choose rational functions $f_{\sigma,\tau} \in \overline{K}(D)$ and $g_\sigma \in \overline{K}(C)$ with

$$\mathrm{div}(f_{\sigma,\tau}) = \sigma\mathfrak{b}_\tau - \mathfrak{b}_{\sigma\tau} + \mathfrak{b}_\sigma \qquad \mathrm{div}(g_\sigma) = \phi^*\mathfrak{b}_\sigma$$

and scale such that $f_{\sigma,\tau} \circ \phi = (\sigma g_\tau)\, g_{\sigma\tau}^{-1}\, g_\sigma$. We also choose $\mathfrak{x}_1 \in \mathrm{Div}^0(C)$ with $\phi\,\mathfrak{x}_1 = \mathfrak{x}$. Then $a = \{a_\sigma\}_\sigma$ with $a_\sigma = \mathrm{sum}(\sigma\mathfrak{x}_1 - \mathfrak{x}_1)$. The product of the cocycles

$$e_\phi(a_\sigma, \sigma b_\tau) = \frac{\sigma(g_\tau\,\mathfrak{x}_1)}{(\sigma g_\tau)\,\mathfrak{x}_1} \quad \text{and} \quad f_{\sigma,\tau}(\mathfrak{x}) = (f_{\sigma,\tau} \circ \phi)\,\mathfrak{x}_1 = \frac{(\sigma g_\tau)\,\mathfrak{x}_1 \;\; g_\sigma\,\mathfrak{x}_1}{g_{\sigma\tau}\,\mathfrak{x}_1}$$

is a coboundary. Thus $(a,b) = (x,y)$ as required. ∎

PROPOSITION 2.2. *The Tate pairings (15) and (17) are*[2] *non-degenerate.*

Proof. This is due to Tate [T1], [T2]. See [Si1, §17] for a detailed statement. In fact the non-degeneracy of (15) follows from local class field theory [Se1, XIV]. The non-degeneracy of (17) may then be deduced using Proposition 2.1 and a counting argument [Mi, I.3.2]. ∎

LEMMA 2.3. *Let K be a finite extension of $\mathbf{Q}_p$. Let M be an unramified finite G_K-module of order prime to p. Then the unramified subgroups are exact annihilators with respect to the Tate pairing* (15).

Proof. See [Se2, II.5.5]. ∎

The next result is often referred to simply as *Tate local duality.*

LEMMA 2.4. *Let K be a local field. Let $\phi : C \to D$ be an isogeny of elliptic curves over K. Then $\operatorname{im}\delta_\phi$ and $\operatorname{im}\delta_{\widehat{\phi}}$ are exact annihilators with respect to the Tate pairing.*

Proof. This follows easily from Propositions 2.1 and 2.2. ∎

We end this section with one global result. For K a number field there is a well known exact sequence

$$0 \longrightarrow \operatorname{Br}(K) \longrightarrow \oplus_v \operatorname{Br}(K_v) \stackrel{\sum \operatorname{inv}_v}{\longrightarrow} \mathbf{Q}/\mathbf{Z} \longrightarrow 0. \tag{18}$$

It follows that all pairings discussed in this section satisfy a product formula. For example if $a \in H^1(K, C[\phi])$ and $b \in H^1(K, D[\widehat{\phi}])$ then we have

$$\textstyle\sum_v (a_v, b_v)_v \quad = \quad 0 \tag{19}$$

where $(\cdot,\cdot)_v$ is the Tate pairing (16) at K_v.

2.2. Global duality theorems

From now on let K be a number field. Let E/K be an elliptic curve. We review the pairing on $\text{Ш}(E/K)$ due to Cassels [CaIV]. We do not discuss the extension to abelian varieties, due to Tate, details of which may be found in [Mi].

THEOREM 2. *There is an alternating bilinear pairing*

$$\text{Ш}(E/K) \times \text{Ш}(E/K) \to \mathbf{Q}/\mathbf{Z} \tag{20}$$

whose kernel is the subgroup of infinitely divisible elements.

We outline two different definitions of the pairing. In the language of [PS] these are the *homogeneous space definition* and the *Weil pairing definition.* Both appear in Cassels' original paper [CaIV].

[2] In the case $K = \mathbf{R}$ or $\mathbf{C}$ we must replace $E(K)$ by its group of connected components.

Homogeneous space definition. Let $x, y \in Ш(E/K)$. Then x corresponds to a torsor T under E. There is an exact sequence of G_K-modules

$$0 \longrightarrow \overline{K}^* \longrightarrow \overline{K}(T)^* \xrightarrow{\text{div}} \text{Div}^0(T) \xrightarrow{\text{sum}} E \longrightarrow 0.$$

Splitting into short exact sequences and passing to the long exact sequence of Galois cohomology we obtain a diagram, which we consider both in its own right and with K replaced by K_v

$$\begin{array}{ccccc} & & & & \text{Br}(K) = H^2(K, \overline{K}^*) \\ & & & & \downarrow \iota \\ & & & & H^2(K, \overline{K}(T)^*) \\ & & & & \downarrow \\ H^1(K, \text{Div}^0(T)) & \xrightarrow{\text{sum}} & H^1(K, E) & \xrightarrow{\delta} & H^2(K, \overline{K}(T)^*/\overline{K}^*) \\ & & & & \downarrow \\ & & & & H^3(K, \overline{K}^*) = 0. \end{array}$$

We choose $f \in H^2(K, \overline{K}(T)^*)$ such that f and y have the same image in $H^2(K, \overline{K}(T)^*/\overline{K}^*)$. Since y is locally trivial $f_v = \iota(\varepsilon_v)$ for some $\varepsilon_v \in \text{Br}(K_v)$. We define

$$\langle x, y \rangle \quad = \quad \textstyle\sum_v \text{inv}_v(\varepsilon_v). \tag{21}$$

Remarks. (i) The global element f exists since $H^3(K, \overline{K}^*) = 0$. Cassels [CaIV, §3] avoids appealing to this fact by relaxing the condition that f is represented by a cocycle.
(ii) The definition is independent of the choice of f by (18).
(iii) Since $T(K_v) \neq \emptyset$ the map $\iota : \text{Br}(K_v) \to H^2(K_v, \overline{K}_v(T)^*)$ has a section. It follows that our choice of element ε_v is forced.
(iv) Linearity in the second argument is clear. For linearity in the first argument we refer to Cassels [CaIV, §3].
(v) The pairing is alternating, *i.e.* $\langle x, x \rangle = 0$ for all $x \in Ш(E/K)$. To see this let T as above and pick $P \in T(\overline{K})$. Then the cocycle $\sigma P - P$ defines an element $\mathfrak{x}$ of $H^1(K, \text{Div}^0(T))$ with $\text{sum}(\mathfrak{x}) = x$. The exact row of our diagram shows $\delta(x) = 0$. It follows that $\langle x, x \rangle = 0$ as claimed.

The non-degeneracy statement of Theorem 2 follows from

THEOREM 3. *Let $\phi : C \to D$ be an isogeny of elliptic curves over K. Then there is a map $\phi : Ш(C/K) \to Ш(D/K)$, and $x \in Ш(D/K)$ belongs to the image of ϕ if and only if $\langle x, y \rangle = 0$ for all $y \in Ш(D/K)[\widehat{\phi}]$.*

At this point we need an alternative definition of the pairing.

Weil pairing definition. Let $x, y \in Ш(D/K)$. Suppose that x lifts to an element $x_1 \in H^1(K, C)$ with $\phi x_1 = x$, and that $y \in Ш(D/K)[\widehat{\phi}]$. Since x is locally trivial we may choose $\xi_v \in H^1(K_v, C[\phi])$ such that $-\xi_v$ and x_1 have the same image in $H^1(K_v, C)$. Let $b \in S^{(\widehat{\phi})}(D/K)$ with $\iota_{\widehat{\phi}} : b \mapsto y$. We define

$$\langle x, y \rangle \quad = \quad \textstyle\sum_v (\xi_v, b_v)_v \tag{22}$$

where $(\cdot, \cdot)_v$ is the local Tate pairing (16).

Remarks. (i) The definition is independent of the choices of x_1 and b by the product formulae for the pairings (16) and (17) respectively.
(ii) The definition is independent of the choice of ξ_v by Tate local duality.
(iii) Linearity in both arguments is clear.
(iv) If $x = \phi x_1$ for some $x_1 \in Ш(C/K)$ it is clear that $\langle x, y \rangle = 0$.

PROPOSITION 2.5. *The global pairings (21) and (22) are compatible.*

Proof. Let x, x_1, y, and b be as in the Weil pairing definition. Then x_1 and x correspond to torsors T_1 and T under C and D respectively. There is a commutative diagram

$$\begin{tikzcd} T_1 \arrow[r, "\phi"] \arrow[d, phantom, "\wr"] & T \arrow[d, phantom, "\wr"] \arrow[dr] & \\ C \arrow[r, "\phi"] & D \arrow[r, "\widehat{\phi}"] & C \end{tikzcd}$$

with non-vertical maps defined over K. Let $b = \{b_\sigma\}_\sigma$ and let $\mathfrak{b}_\sigma \in \mathrm{Div}^0(T)$ with $\mathrm{sum}(\mathfrak{b}_\sigma) = b_\sigma$. We choose rational functions $f_{\sigma,\tau} \in \overline{K}(T)$ and $g_\sigma \in \overline{K}(T_1)$ with

$$\mathrm{div}(f_{\sigma,\tau}) = \sigma\mathfrak{b}_\tau - \mathfrak{b}_{\sigma\tau} + \mathfrak{b}_\sigma \qquad\qquad \mathrm{div}(g_\sigma) = \phi^*\mathfrak{b}_\sigma$$

and scale such that $f_{\sigma,\tau} \circ \phi \;=\; (\sigma g_\tau)\, g_{\sigma\tau}^{-1}\, g_\sigma$. At each place v we choose $P \in T(K_v)$ and $P_1 \in T_1(\overline{K}_v)$ with $\phi(P_1) = P$. Then the cocycle $\sigma P_1 - P_1$ defines an element $-\xi_v$ in $H^1(K_v, C[\phi])$. Following the proof of Proposition 2.1 the cocycles

$$e_\phi(\sigma P_1 - P_1, \sigma b_\tau)^{-1} \quad \text{and} \quad f_{\sigma,\tau}(P) = (f_{\sigma,\tau} \circ \phi)\, P_1$$

are cobounding. Thus $(\xi_v, b_v)_v = \varepsilon_v$ for all v and the pairings (21) and (22) agree. ∎

For the proof of Theorem 3 we need an approximation theorem in the style of [CaIV, Lemma 6.2]. We temporarily suspend our convention that $(*)_v$ is the local object corresponding to $(*)$.

Lemma 2.6. *Let M be a finite G_K-module. For each place v we fix $W_v(M) \subset H^1(K_v, M)$ and write $W_v(M^\vee) \subset H^1(K_v, M^\vee)$ for its exact annihilator with respect to the Tate pairing. Suppose that $W_v(M)$ and $W_v(M^\vee)$ are the unramified subgroups for all but finitely many v. Then given $\xi_v \in H^1(K_v, M)$ there exists $\xi \in H^1(K, M)$ with $\xi \equiv \xi_v \mod W_v(M)$ for all v, if and only if*
(i) ξ_v is unramified for all but finitely many v,
(ii) $\sum_v (\xi_v, b_v)_v = 0$ for all $b \in H^1(K, M^\vee)$ with $b_v \in W_v(M^\vee)$.

Proof. Necessity of (i) and (ii) is clear, the latter from the product formula. Sufficiency is a consequence of the Cassels-Poitou-Tate exact sequence. We refer to [CS, §1] or [Mi, I.4.10, I.6.15] for details. ∎

We now give the proof of Theorem 3 under the assumption

$$x \in Ш(D/K) \ \text{ lifts to } \ x_1 \in H^1(K, C) \ \text{ with } \ \phi x_1 = x. \tag{23}$$

Under this assumption, x is in the image of $\phi : Ш(C/K) \to Ш(D/K)$ if and only if we can find $\xi \in H^1(K, C[\phi])$ such that $x_1 + \iota_\phi(\xi)$ is everywhere locally trivial. We choose local elements $\xi_v \in H^1(K_v, C[\phi])$ such that $-\xi_v$ and x_1 have the same image in $H^1(K_v, C)$. Lemma 2.6 with $M = C[\phi]$ and $W_v(M) = \operatorname{im} \delta_{\phi,v}$ tells us that the ξ_v may be chosen coming from a global element $\xi \in H^1(K, C[\phi])$ if and only if

$$\textstyle\sum_v (\xi_v, b_v)_v = 0 \quad \text{ for all } b \in S^{(\widehat{\phi})}(D/K). \tag{24}$$

According to the Weil pairing definition, (24) is precisely the condition $\langle x, y \rangle = 0$ for all $y \in Ш(D/K)[\widehat{\phi}]$. This completes the proof of Theorem 3 under the assumption (23).

The existence of a global lifting (23) is assured if for $M = C[\phi]$ the natural map

$$H^2(K, M) \longrightarrow \textstyle\prod_v H^2(K_v, M) \quad \text{ is injective.} \tag{25}$$

Indeed there is an exact sequence

$$H^1(K, C) \longrightarrow H^1(K, D) \longrightarrow H^2(K, C[\phi])$$

and by assumption x is everywhere locally trivial.

Lemma 2.7. *Let $M = C[\phi]$ with either $\deg \phi = p$ or $\phi = [p]$ for p a prime. Then the Hasse Principle (25) holds.*

Proof. First suppose $\deg \phi = p$. A field extension of degree prime to p reduces us to the case $M = \mu_p$ and we are done by (18). The case $\phi = [p]$ is due to Tate [CaIV, Lemma 5.1]. See [Mi, I.9.2] for a more general statement. A counter-example for arbitrary finite M may be found in [Se2, III.4.7]. ∎

We now have a proof of Theorem 3 in the case $\phi = [p]$. As Cassels [CaIV, §4] explains, this is sufficient to prove Theorem 2. To complete the proof of Theorem 3 we argue by induction on the degree of the isogeny ϕ. We factor $\phi = \phi_1\phi_2$ with ϕ_2 satisfying one of the conditions of Lemma 2.7. Say

$$C \xrightarrow{\phi_2} E \xrightarrow{\phi_1} D.$$

We are given $x \in Ш(D/K)$ with $\langle x, y\rangle = 0$ for all $y \in Ш(D/K)[\widehat{\phi}]$. Since $\deg \phi_1 < \deg \phi$ our induction hypothesis shows that there exists $x_1 \in Ш(E/K)$ with $\phi_1 x_1 = x$. Then by Lemma 2.7 there exists $x_2 \in H^1(K, C)$ with $\phi_2 x_2 = x_1$. Thus $\phi x_2 = x$. Our earlier proof of Theorem 3 under the assumption (23) now applies.

LEMMA 2.8. *Let $\phi : C \to D$ be an isogeny of elliptic curves over K. Then the maps $\phi : Ш(C/K) \to Ш(D/K)$ and $\widehat{\phi} : Ш(D/K) \to Ш(C/K)$ are adjoints with respect to the Cassels-Tate pairing.*

Proof. See [CaVIII, §2] where this result is readily deduced from the homogeneous space definition. This lemma gives yet another proof of the easier implication of Theorem 3. ∎

Remark. The Weil pairing definition may be used more generally by relaxing the condition that x_1 is represented by a cocycle. See [Mi, I.6.9] or [PS, §12.2] for details. If we then check that the definition does not depend on our choice of isogeny ϕ, we may avoid the homogeneous space definition altogether.

Remark. The homogeneous space definition has been used for explicit computations by McGuinness [McG]. The Weil pairing definition has been used by McCallum [McC] and Beaver [Be] in the split torsion case. Variants of the Weil pairing definition have been used by Cassels [CaI], [Ca98] to treat diagonal cubics and 2-descents respectively.

2.3. Split torsion and local pairings

We write the Cassels-Tate pairing in a form expounded by Cassels [CaI], [Ca98], and then recall from [McC] a condition for this pairing to be written as a sum of local pairings.

PROPOSITION 2.9. *(i) Let $\phi : C \to D$ be an isogeny of elliptic curves over K with $m = \deg \phi$. There is an alternating bilinear pairing*

$$S^{(\widehat{\phi})}(D/K) \times S^{(\widehat{\phi})}(D/K) \to \mathbf{Q}/\mathbf{Z} \tag{26}$$

whose kernel is precisely the image of $S^{(m)}(C/K)$.
(ii) If the exact sequence of Galois modules $0 \to C[\phi] \to C[m] \to D[\widehat{\phi}] \to 0$

splits then the global pairing (26) is a sum of local pairings

$$\langle \cdot, \cdot \rangle_{\widehat{\phi},v} : \operatorname{im} \delta_{\widehat{\phi},v} \times \operatorname{im} \delta_{\widehat{\phi},v} \to \mathbf{Q}/\mathbf{Z}. \tag{27}$$

Proof. (i) The Cassels-Tate pairing on $Ш(D/K)[\widehat{\phi}]$ lifts to a pairing on $S^{(\widehat{\phi})}(D/K)$. The description of the kernel is immediate from Theorem 3.
(ii) Let s be a Galois equivariant section of the map $\phi : C[m] \to D[\widehat{\phi}]$. Then s may be used to make the lifting (23) automatic. Working over the local field K_v we drop the subscripts v from our local connecting maps. There is a commutative diagram

$$\begin{array}{ccccc}
C(K_v) & \xrightarrow{\phi} & D(K_v) & \xrightarrow{\delta_\phi} & H^1(K_v, C[\phi]) \\
|| & & \downarrow \widehat{\phi} & & \downarrow \iota \\
C(K_v) & \xrightarrow{[m]} & C(K_v) & \xrightarrow{\delta_m} & H^1(K_v, C[m]) \\
\downarrow \phi & & || & & \downarrow \phi \\
D(K_v) & \xrightarrow{\widehat{\phi}} & C(K_v) & \xrightarrow{\delta_{\widehat{\phi}}} & H^1(K_v, D[\widehat{\phi}]).
\end{array} \tag{28}$$

Given $a, b \in \operatorname{im} \delta_{\widehat{\phi}}$ we choose $P \in C(K_v)$ with $\delta_{\widehat{\phi}}(P) = a$. Then there exists $\xi \in H^1(K_v, C[\phi])$ with $\delta_m(P) = \iota(\xi) + s(a)$. We define

$$\langle a, b \rangle_{\widehat{\phi},v} = (\xi, b)_v \tag{29}$$

where $(\cdot, \cdot)_v$ is the Tate pairing. By Tate local duality this definition does not depend on the choices of P and ξ. The Weil pairing definition shows that the Cassels-Tate pairing on $S^{(\widehat{\phi})}(D/K)$ is the sum of these local pairings. ∎

Since $\operatorname{im} \delta_m \subset H^1(K_v, C[m])$ is an isotropic subspace with respect to the Tate pairing, we find

LEMMA 2.10. *The local pairings $\langle \cdot, \cdot \rangle_{\widehat{\phi},v}$ are skew-symmetric.*

Proof. See [McC, Lemma 1.10]. ∎

In the setting of Proposition 2.9(ii) we have $C[m] = C[\phi] \times sD[\widehat{\phi}]$. It is helpful to make some changes to our notation. We write $\alpha : E \to E'$ instead of $\phi : C \to D$, and $\widehat{\beta} : E \to E''$ for the isogeny with kernel $sD[\widehat{\phi}]$. Then it is natural to identify $E[\alpha] = E''[\beta] = M$ (say), $E[\widehat{\beta}] = E'[\widehat{\alpha}] = M^\vee$ and $E[m] = M \times M^\vee$.

Again we work over the local field K_v and drop the subscripts v from our local connecting maps. From the commutative diagram

$$\begin{array}{ccccc}
E(K_v) & \xrightarrow{\alpha} & E'(K_v) & \xrightarrow{\delta_\alpha} & H^1(K_v, M) \\
\downarrow \widehat{\beta} & & \downarrow \widehat{\alpha} & & || \\
E''(K_v) & \xrightarrow{\beta} & E(K_v) & \xrightarrow{\delta_\beta} & H^1(K_v, M) \\
\downarrow \delta_{\widehat{\beta}} & & \downarrow \delta_{\widehat{\alpha}} & & \\
H^1(K_v, M^\vee) & = & H^1(K_v, M^\vee) & &
\end{array} \tag{30}$$

it is clear that $\operatorname{im}\delta_\alpha \subset \operatorname{im}\delta_\beta$ and $\operatorname{im}\delta_{\widehat{\beta}} \subset \operatorname{im}\delta_{\widehat{\alpha}}$. The next proposition shows that $\operatorname{im}\delta_\alpha = \operatorname{im}\delta_\beta$ if and only if $\operatorname{im}\delta_{\widehat{\beta}} = \operatorname{im}\delta_{\widehat{\alpha}}$. We call v a *switching place* if these equalities do not hold. For all but finitely many primes $\mathfrak{p}$ we know that $\operatorname{im}\delta_\alpha = \operatorname{im}\delta_\beta$ is the unramified subgroup of $H^1(K_\mathfrak{p}, M)$. So the set of switching places is finite.

LEMMA 2.11. *(i) The subgroup* $\operatorname{im}\delta_m \subset H^1(K_v, E[m])$ *may be viewed as a relation on* $H^1(K_v, M) \times H^1(K_v, M^\vee)$*. It induces an isomorphism*

$$\operatorname{im}\delta_\beta / \operatorname{im}\delta_\alpha \;\simeq\; \operatorname{im}\delta_{\widehat{\alpha}} / \operatorname{im}\delta_{\widehat{\beta}}. \tag{31}$$

(ii) The Tate pairing (15) induces a non-degenerate pairing

$$(\cdot,\cdot)_v : \operatorname{im}\delta_\beta / \operatorname{im}\delta_\alpha \times \operatorname{im}\delta_{\widehat{\alpha}} / \operatorname{im}\delta_{\widehat{\beta}} \to \mathbf{Q}/\mathbf{Z}.$$

Combining (i) and (ii) we obtain the local pairings of Proposition 2.9. More precisely, if we write both the isomorphism (31) and its inverse as $a \mapsto \overline{a}$*, then* $\langle a, b\rangle_{\widehat{\alpha},v} = (\overline{a}, b)_v$ *and* $\langle a, b\rangle_{\beta,v} = -(a, \overline{b})_v$*. In particular the switching places are precisely the places for which the local pairings are non-zero.*

Proof. (i) The diagram (30) shows

$$\operatorname{im}\delta_\beta / \operatorname{im}\delta_\alpha \quad\simeq\quad \frac{E(K_v)}{\widehat{\alpha}E'(K_v)\,\beta E''(K_v)} \quad\simeq\quad \operatorname{im}\delta_{\widehat{\alpha}} / \operatorname{im}\delta_{\widehat{\beta}}.$$

(ii) The non-degeneracy is a consequence of Tate local duality.
The description of $\langle\cdot,\cdot\rangle_{\widehat{\alpha},v}$ follows from the proof of Proposition 2.9 on noting that our identifications suppress the maps ι and s. The description of $\langle\cdot,\cdot\rangle_{\beta,v}$ follows by the symmetry properties of the pairings. The final statement is clear. ∎

Remark. By Lemma 2.10 we know that $\operatorname{im}\delta_\beta / \operatorname{im}\delta_\alpha$ has order either a square or twice a square. Taking $M = \mu_4$ and following the proof of Proposition 1.7 (with $\mu_4 \not\subset K_v$) we may give examples of the latter. We deduce that the local pairings need not be alternating.

Following Beaver [Be] we give a formula for the local pairings in terms of the Hilbert norm residue symbol. We suppose

$$M \simeq M^\vee \simeq \mathbf{Z}/m\mathbf{Z} \quad \text{as } G_v\text{-modules}. \tag{32}$$

In particular $\mu_m \subset K_v$. We fix $P \in M$ and $Q \in M^\vee$ with $e_m(P, Q) = \zeta$. The maps $x \mapsto e_m(P, x)$ and $x \mapsto e_m(Q, x)$ induce isomorphisms

$$\begin{aligned} j_P : H^1(K_v, M^\vee) &\simeq K_v^*/K_v^{*m} \\ j_Q : H^1(K_v, M) &\simeq K_v^*/K_v^{*m}. \end{aligned}$$

Let $a \in H^1(K_v, M)$ and $b \in H^1(K_v, M^\vee)$. By [McC, Lemma 2.7]

$$(a, b)_v = -\operatorname{Ind}_\zeta(j_Q a, j_P b)_v \tag{33}$$

where $(\cdot,\cdot)_v$ on the left is the Tate pairing and $(\cdot,\cdot)_v$ on the right is the Hilbert norm residue symbol. Under the assumption (32) we have $H^1(K_v, E[m]) = \mathrm{Hom}(G_v, \langle P, Q\rangle)$.

PROPOSITION 2.12. *Let v be a place of K satisfying (32) and*

$$\operatorname{im}\delta_m = \mathrm{Hom}(G_v, \langle rP + sQ\rangle) \tag{34}$$

for some $(r : s) \in \mathbf{P}^1(\mathbf{Z}/m\mathbf{Z})$. Then
(i) $\operatorname{im}\delta_{\widehat{\alpha}} = \mathrm{Hom}(G_v, \langle sQ\rangle)$ and $\langle sa, sb\rangle_{\widehat{\alpha},v} = rs\,\mathrm{Ind}_\zeta(j_P a, j_P b)_v$
(ii) $\operatorname{im}\delta_\beta = \mathrm{Hom}(G_v, \langle rP\rangle)$ and $\langle ra, rb\rangle_{\beta,v} = -rs\,\mathrm{Ind}_\zeta(j_Q a, j_Q b)_v$.

Proof. (i) We compute

$$\begin{aligned}
\langle sa, sb\rangle_{\widehat{\alpha},v} &= (\overline{sa}, sb)_v && \text{by Lemma 2.11}\\
&= -\mathrm{Ind}_\zeta(j_Q(\overline{sa}), j_P(sb))_v && \text{by (33)}\\
&= \mathrm{Ind}_\zeta(j_P(ra), j_P(sb))_v && \text{by (34)}\\
&= rs\,\mathrm{Ind}_\zeta(j_P a, j_P b)_v.
\end{aligned}$$

(ii) This follows on interchanging P and Q. Although both pairings are skew symmetric a minus sign is introduced since we have taken $e_m(P,Q) = \zeta$. ∎

2.4. A description of the ratio $(r : s)$.

Let $m = 3$, 4 or 5. Let E/K be an elliptic curve with $E[m] \simeq \mu_m \times \mathbf{Z}/m\mathbf{Z}$. In the notation of §1.3 we have $E = E_t$ for some $t \in K$. In the notation of §2.3 we have taken $M = \mu_m$. We aim to compute the local pairings $\langle\cdot,\cdot\rangle_{\widehat{\alpha},v}$ and $\langle\cdot,\cdot\rangle_{\beta,v}$.

We treat an important special case, namely when $v = \mathfrak{p}$ is a prime with $\operatorname{Norm}\mathfrak{p} \equiv 1 \pmod m$, equivalently $\mathfrak{p} \nmid m$ and $\mu_m \subset K_\mathfrak{p}$. For these primes our hypothesis (32) is satisfied. In fact E has split multiplicative reduction at $\mathfrak{p}$. As Beaver [Be] explains the Tate parametrisation may then be used to establish (34). Instead we make use of the action of $\mathrm{PSL}_2(\mathbf{Z}/m\mathbf{Z})$ on $X(m)$. Our method gives a simple way of computing the ratio $(r : s)$.

PROPOSITION 2.13. *Let $(E, P, Q) = (E_t, P_t, Q_t)$ with $t \in K$. Let $\mathfrak{p}$ be a prime of bad reduction for E with $\operatorname{Norm}\mathfrak{p} \equiv 1 \pmod m$. Then hypotheses (32) and (34) are satisfied for the following values of $(r : s)$*

$$\begin{array}{lll}
m = 3 & \left\{\begin{array}{l} t \equiv 0 \pmod{\mathfrak{p}} \\ t \equiv \zeta^\nu \pmod{\mathfrak{p}} \end{array}\right. & \begin{array}{l} (1:0) \\ (\nu:1) \end{array} \\[2ex]
m = 4 & \left\{\begin{array}{l} t \equiv 0 \pmod{\mathfrak{p}} \\ t \equiv i^\nu \pmod{\mathfrak{p}} \\ t \equiv \infty \pmod{\mathfrak{p}} \end{array}\right. & \begin{array}{l} (1:0) \\ (\nu:1) \\ (1:2) \end{array} \\[2ex]
m = 5 & \left\{\begin{array}{l} t \equiv 0, \infty \pmod{\mathfrak{p}} \\ t \equiv \zeta^\nu\phi, \zeta^\nu\overline{\phi} \pmod{\mathfrak{p}} \end{array}\right. & \begin{array}{l} (1:0) \\ (\nu:1). \end{array}
\end{array}$$

Proof. Since $\mathfrak{p} \nmid m$ the cusps of $X(m)$ are distinct when we reduce mod $\mathfrak{p}$. We first consider the case $t \equiv 0 \pmod{\mathfrak{p}}$. Proposition 1.7 and Tate local duality give $\operatorname{im} \delta_{\alpha,\mathfrak{p}} = K_{\mathfrak{p}}^* / K_{\mathfrak{p}}^{*m}$ and $\operatorname{im} \delta_{\widehat{\alpha},\mathfrak{p}} = 0$. The diagram (28) shows that there is an exact sequence

$$0 \longrightarrow \operatorname{im} \delta_{\alpha,\mathfrak{p}} \longrightarrow \operatorname{im} \delta_{m,\mathfrak{p}} \longrightarrow \operatorname{im} \delta_{\widehat{\alpha},\mathfrak{p}} \longrightarrow 0.$$

We deduce $\operatorname{im} \delta_{m,\mathfrak{p}} = \operatorname{Hom}(G_{\mathfrak{p}}, \langle P \rangle)$. So the hypothesis (34) is satisfied with $(r:s) = (1:0)$. We use the action of $\mathrm{PSL}_2(\mathbf{Z}/m\mathbf{Z})$ on $X(m)$ to extend to the general case. Indeed if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} : t_1 \mapsto t_2$, then in an obvious notation

$$\begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \begin{pmatrix} r_1 \\ s_1 \end{pmatrix} = \begin{pmatrix} r_2 \\ s_2 \end{pmatrix}.$$

It only remains to describe the action of $\mathrm{PSL}_2(\mathbf{Z}/m\mathbf{Z})$ on the cusps, and this may be read off from Proposition 1.6. ∎

Remark. The last two propositions give an alternative and perhaps more natural proof of Proposition 1.7.

COROLLARY 2.14. *Let $(E,P,Q) = (E_t, P_t, Q_t)$ with $t \in K$. Let $\mathfrak{p}$ be a prime with* $\operatorname{Norm} \mathfrak{p} \equiv 1 \pmod{m}$. *Suppose* $t \equiv \zeta^\nu \pmod{\mathfrak{p}}$ *(for $m = 3$, 4), respectively* $t \equiv \zeta^\nu \phi, \zeta^\nu \overline{\phi} \pmod{\mathfrak{p}}$ *(for $m = 5$), for some ν prime to m. Then*

$$\langle a,b \rangle_{\widehat{\alpha},\mathfrak{p}} = \nu \operatorname{Ind}_\zeta (j_P a, j_P b)_{\mathfrak{p}} \tag{35}$$
$$\langle a,b \rangle_{\beta,\mathfrak{p}} = -1/\nu \operatorname{Ind}_\zeta (j_Q a, j_Q b)_{\mathfrak{p}}. \tag{36}$$

Proof. This is the case $(r:s) = (\nu:1)$ of the last two propositions. ∎

Remark. Beaver [Be] obtained the formula (36) in the case $m = 5$. In her notation $\lambda_v = 1/\nu$ is computed in terms of the Tate parametrisation.

We give an alternative approach to Corollary 2.14 that avoids both the Tate parametrisation and the action of $\mathrm{PSL}_2(\mathbf{Z}/m\mathbf{Z})$. Putting our equations for $E = E_t$ into Weierstrass form and using Lemma 1.1 we blast out the identities

$$j_P \delta_{\widehat{\alpha}}(Q) = \begin{cases} \zeta(t-\zeta)(t-\zeta^2)^2 & m = 3 \\ -(t-i)(t+1)^2(t+i)^3 & m = 4 \\ \prod_\nu \left((t-\zeta^\nu \overline{\phi})/(t-\zeta^\nu \phi) \right)^\nu & m = 5 \end{cases}$$

$$j_Q \delta_\beta(Q)^{-1} = \begin{cases} t(t^2+t+1)/3 & m = 3 \\ t(t^2+1)/2 & m = 4 \\ tf(t)/g(t) & m = 5 \end{cases}$$

where $f(t)$ and $g(t)$ are given by (4). For ν as in Corollary 2.14 it follows

$$\operatorname{ord}_{\mathfrak{p}}(j_Q \delta_\beta(Q)) \equiv -\nu \operatorname{ord}_{\mathfrak{p}}(j_P \delta_{\widehat{\alpha}}(Q)) \pmod{m}. \tag{37}$$

We check (35) in the case $a = \delta_{\widehat{\alpha}}(Q)$ and $\operatorname{ord}_{\mathfrak{p}}(j_P b) \equiv 0$. Indeed

$$\begin{aligned} \langle \delta_{\widehat{\alpha}}(Q), b \rangle_{\widehat{\alpha},\mathfrak{p}} &= (\delta_\beta(Q), b)_{\mathfrak{p}} && \text{by Lemma 2.11} \\ &= -\operatorname{Ind}_\zeta(j_Q \delta_\beta(Q), j_P b)_{\mathfrak{p}} && \text{by (33)} \\ &= \nu \operatorname{Ind}_\zeta(j_P \delta_{\widehat{\alpha}}(Q), j_P b)_{\mathfrak{p}} && \text{by (37).} \end{aligned}$$

Similarly we may check (36) in the case $\operatorname{ord}_{\mathfrak{p}}(j_Q a) \equiv 0$ and $b = \delta_\beta(Q)$.

$$\begin{aligned} \langle a, \delta_\beta(Q) \rangle_{\beta,\mathfrak{p}} &= -(a, \delta_{\widehat{\alpha}}(Q))_{\mathfrak{p}} && \text{by Lemma 2.11} \\ &= \operatorname{Ind}_\zeta(j_Q a, j_P \delta_{\widehat{\alpha}}(Q))_{\mathfrak{p}} && \text{by (33)} \\ &= -1/\nu \operatorname{Ind}_\zeta(j_Q a, j_Q \delta_\beta(Q))_{\mathfrak{p}} && \text{by (37).} \end{aligned}$$

Under the hypotheses of Corollary 2.14 the pairings $\langle \cdot, \cdot \rangle_{\widehat{\alpha},v}$ and $\langle \cdot, \cdot \rangle_{\beta,v}$ are, at the level of abelian groups, just skew symmetric pairings

$$(\mathbf{Z}/m\mathbf{Z})^2 \times (\mathbf{Z}/m\mathbf{Z})^2 \to \mathbf{Q}/\mathbf{Z}.$$

Thus for m odd the formulae (35) and (36) may be established by checking at a single pair of non-trivial values. The above calculations do this whenever $\operatorname{ord}_{\mathfrak{p}}(j_Q \delta_\beta(Q)) \not\equiv 0 \pmod{m}$.

2.5. An example without split torsion

We compute the Cassels-Tate pairing for one of the curves found in [F1]. This section and §3 may be read in either order.

Let $m = 5$ and $\lambda = 100/9$. The curve C_λ defined in §1.1 is labelled 570L4 in Cremona's tables [Cr1]. In [F1] we saw

$$S^{(\phi)}(C_\lambda/\mathbf{Q}) \simeq (\mathbf{Z}/5\mathbf{Z})^3 \quad \text{and} \quad S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q}) = 0.$$

Descent by 2-isogeny [Cr1], or equally an L-value computation, shows that $C_\lambda(\mathbf{Q})$ has rank 0. We were able to deduce $Ш(C_\lambda/\mathbf{Q})[5] \simeq (\mathbf{Z}/5\mathbf{Z})^2$. In this section we prove

Proposition 2.15. *Let $m = 5$ and $\lambda = 100/9$. Then $S^{(\phi)}(C_\lambda/\mathbf{Q}) \subset \mathbf{Q}^*/\mathbf{Q}^{*5}$ is generated by the primes 2, 3 and 5. The Cassels-Tate pairing on this Selmer group is given by*

	2	3	5
2	0	3	3
3	2	0	3
5	2	2	0

Not only does this give another proof that $C_\lambda(\mathbf{Q})$ has rank 0, but we also learn that $Ш(C_\lambda/\mathbf{Q})$ contains no element of order 25.

The idea is that we use our work in the split torsion case to give a formula for the Cassels-Tate pairing over a certain subfield $F \subset \mathbf{Q}(D_\lambda[5])$. We must therefore explain the relationship between the Cassels-Tate pairing over $\mathbf{Q}$ and the Cassels-Tate pairing over F.

PROPOSITION 2.16. *Let L/K be a finite extension of number fields. Let E/K be an elliptic curve. Then the restriction map $Ш(E/K) \to Ш(E/L)$ and the corestriction map $Ш(E/L) \to Ш(E/K)$ are adjoints with respect to the Cassels-Tate pairing.*

Proof. We recall [Se1, VII.7] that corestriction is the map on cohomology corresponding to the norm in dimension 0. Let v be a place of K. For any discrete G_K-module A and any $q \geq 0$ there is commutative diagram

$$\begin{array}{ccc} H^q(L,A) & \longrightarrow & \oplus_{w|v} H^q(L_w,A) \\ \downarrow \mathrm{Cor} & & \downarrow \sum \mathrm{Cor} \\ H^q(K,A) & \longrightarrow & H^q(K_v,A) \end{array}$$

Indeed for $q=0$ this expresses a well-known property of the norm, and the general case follows by dimension shifting. In particular the corestriction map $H^1(L,E) \to H^1(K,E)$ preserves local triviality. We obtain a map on Tate-Shafarevich groups as claimed.

We give one further preliminary to our calculation. Let $w|v$ be places of L and K and let $n = [L_w : K_v]$. There are commutative diagrams

$$\begin{array}{ccc} \mathrm{Br}(K_v) & \xrightarrow{\mathrm{inv}} & \mathbf{Q}/\mathbf{Z} \\ \downarrow \mathrm{Res} & & \downarrow \times n \\ \mathrm{Br}(L_w) & \xrightarrow{\mathrm{inv}} & \mathbf{Q}/\mathbf{Z} \end{array} \qquad\qquad \begin{array}{ccc} \mathrm{Br}(K_v) & \xrightarrow{\mathrm{inv}} & \mathbf{Q}/\mathbf{Z} \\ \uparrow \mathrm{Cor} & & \| \\ \mathrm{Br}(L_w) & \xrightarrow{\mathrm{inv}} & \mathbf{Q}/\mathbf{Z}. \end{array}$$

The diagram on the left is well-known [CF, VI.1]. Since the restriction map $\mathrm{Br}(K_v) \to \mathrm{Br}(L_w)$ is surjective and $\mathrm{Cor} \circ \mathrm{Res} = n$, the diagram on the right is a formal consequence.

Now let $x \in Ш(E/K)$ and $y \in Ш(E/L)$. Following the homogeneous space definition, x corresponds to a torsor T defined over K. Then $\mathrm{Res}\, x$ corresponds to T viewed as a curve over L. We choose $f \in H^2(L, \overline{K}(T)^*)$ such that f and y have the same image in $H^2(L, \overline{K}(T)^*/\overline{K}^*)$. Writing $f_w = \iota(\varepsilon_w)$ we have $(\mathrm{Cor}\, f)_v = \iota \sum_{w|v} \mathrm{Cor}\, \varepsilon_w$. Finally we compute

$$\langle x, \mathrm{Cor}\, y \rangle = \textstyle\sum_v \mathrm{inv}(\sum_{w|v} \mathrm{Cor}\, \varepsilon_w) = \sum_w \mathrm{inv}(\varepsilon_w) = \langle \mathrm{Res}\, x, y \rangle.$$

∎

We return to our numerical example. By Lemma 1.1 and (7) we have $\mathbf{Q}(D_\lambda[5]) = \mathbf{Q}(\mu_5, \sqrt[5]{\eta(\lambda)})$. We put $\tau = \sqrt[5]{\eta(\lambda)}$ and $t = (\phi\tau + 1)/(\tau - \phi)$. Then t is a root of $tf(t) - \lambda g(t) = 0$ where $f(t)$ and $g(t)$ are the quartics (4). We work over $F = \mathbf{Q}(t)$, a non-Galois degree 5 subfield of $\mathbf{Q}(D_\lambda[5])$.

LEMMA 2.17. *Let* $\lambda = 100/9$. *Then*

$$\begin{array}{rcl} S^{(\phi)}(C_\lambda/\mathbf{Q}) & = & \{\,\theta \in \mathbf{Q}^*/\mathbf{Q}^{*5} \mid \mathrm{ord}_p(\theta) \equiv 0 \pmod 5 \textit{ for all } p \neq 2,3,5\} \\ S^{(\phi)}(C_\lambda/F) & = & \{\,\theta \in F^*/F^{*5} \mid \mathrm{ord}_{\mathfrak{p}}(\theta) \equiv 0 \pmod 5 \textit{ for all } \mathfrak{p} \nmid 2,3,5\}. \end{array}$$

The Cassels-Tate pairings on these Selmer groups are related via

$$\langle \mathrm{Norm}_{F/\mathbf{Q}}\, x, y\rangle_{\mathbf{Q}} = \langle x, y\rangle_F \qquad \textit{for } x \in S^{(\phi)}(C_\lambda/F),\ y \in S^{(\phi)}(C_\lambda/\mathbf{Q}).$$

Proof. The description of the Selmer groups is immediate from Proposition 1.4. Let us note that $\lambda^2 - 11\lambda - 1 = 19/81$ and that $\mathcal{O}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^{*5}$ is trivial for $\mathfrak{p} \mid 19$. The relationship between the Cassels-Tate pairings is a restatement of Proposition 2.16. ∎

We are fortunate in our example to find that t, $t-1$ and $t-2$ belong to $S^{(\phi)}(C_\lambda/F)$ and that their norms generate $S^{(\phi)}(C_\lambda/\mathbf{Q})$. So it only remains to compute the Cassels-Tate pairing on $S^{(\phi)}(C_\lambda/F)$. The primes of $\mathbf{Q}(\mu_5)$ above 2, 3 and 5 are (2), (3) and $\mathfrak{l} = (1-\zeta_5)$. In each case $\eta(\lambda) = (\phi^5\lambda + 1)/(\lambda - \phi^5)$ is locally a 5th power. So these primes split in $\mathbf{Q}(D_\lambda[5])/\mathbf{Q}(\mu_5)$. We label the primes upstairs

$$\begin{array}{rcll} (2) & = & \mathfrak{P}_0\mathfrak{P}_1\ldots\mathfrak{P}_4 & \text{with } \tau \equiv \zeta^\nu\overline{\phi} \pmod{\mathfrak{P}_\nu} \\ (3) & = & \mathfrak{Q}_0\mathfrak{Q}_1\ldots\mathfrak{Q}_4 & \text{with } \tau \equiv \zeta^\nu\phi \pmod{\mathfrak{Q}_\nu} \\ \mathfrak{l} & = & \mathfrak{L}_0\,\mathfrak{L}_1\,\ldots\,\mathfrak{L}_4 & \text{with } \tau \equiv \zeta^\nu\overline{\phi} \pmod{\mathfrak{L}_\nu^2}. \end{array}$$

Our treatment of the primes above 5 makes use of [CF, Exercise 2].

LEMMA 2.18. *Let* $(E,P,Q) = (E_t,P_t,Q_t)$ *with* t *as above. The primes* $\mathfrak{P}_\nu, \mathfrak{Q}_\nu, \mathfrak{L}_\nu$ *of* $\mathbf{Q}(D_\lambda[5])$ *above* 2, 3 *and* 5 *satisfy the hypotheses (32) and (34) with* $(r:s) = (-1:\nu)$.

Proof. We closely follow the proof of Proposition 2.13. Since $(t) = \mathfrak{P}_0^2\mathfrak{Q}_0^{-2}\mathfrak{L}_0^2$ the case $\nu = 0$ may be deduced from Proposition 1.4. We then use the action of $\mathrm{Gal}(\mathbf{Q}(D_\lambda[5])/\mathbf{Q}(\mu_5))$ to extend to the general case. In the notation of Proposition 1.6, $S : \tau \mapsto t$. So we obtain $(r:s) = (-1:\nu)$ rather than $(\nu:1)$. ∎

LEMMA 2.19. *The Cassels-Tate pairing on* $S^{(\phi)}(C_\lambda/F)$ *is given by*

$$\langle a, b\rangle = \mathrm{Ind}_\zeta (a,b)_{\mathfrak{P}_1}(a,b)_{\mathfrak{Q}_1}(a,b)_{\mathfrak{L}_1}. \tag{38}$$

Proof. As in §1.3 we identify $\phi : C_\lambda \to D_\lambda$ with $\beta : E'' \to E$. We have already seen

$$\mathrm{im}\,\delta_{\beta,\mathfrak{p}} = \begin{cases} F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*5} & \text{if } \mathfrak{p} \mid 2,3,5 \\ \mathcal{O}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^{*5} & \text{otherwise.} \end{cases}$$

The Cassels-Tate pairing is a sum of local pairings $\langle\cdot,\cdot\rangle_{\beta,\mathfrak{p}}$. By Lemmas 2.10 and 2.11 we need only consider the local pairings at the primes above 2, 3 and 5. We have $(2) = \mathfrak{p}\mathfrak{p}'$ with $\mathfrak{p} = \mathfrak{P}_0$ and $\mathfrak{p}' = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4$. Since

$\mathrm{ord}_{\mathfrak{p}}(t) \neq 0$ we know that $\mathrm{im}\,\delta_{\alpha,\mathfrak{p}} = F_{\mathfrak{p}}/F_{\mathfrak{p}}^{*5}$ and so $\mathfrak{p}$ is not a switching prime. On the other hand $\mathfrak{p}'$ splits in $\mathbf{Q}(D_\lambda[5])/F$. By Proposition 2.12(ii) we have

$$\langle a,b\rangle_{\beta,\mathfrak{p}'} = \langle a,b\rangle_{\beta,\mathfrak{P}_1} = \mathrm{Ind}_\zeta(a,b)_{\mathfrak{P}_1}$$

where in accordance with Lemma 2.17 we have suppressed the map j_Q. Repeating for the primes above 3 and 5 we arrive at the formula (38). ∎

Finally we use the congruences

$$\begin{array}{llcll}
\tau \equiv \zeta\overline{\phi} & (\mathrm{mod}\ \mathfrak{P}_1) & \Longrightarrow & t \equiv \zeta^4\overline{\phi} & (\mathrm{mod}\ \mathfrak{P}_1) \\
\tau \equiv \zeta\phi & (\mathrm{mod}\ \mathfrak{Q}_1) & \Longrightarrow & t \equiv \zeta^4\phi & (\mathrm{mod}\ \mathfrak{Q}_1) \\
\tau \equiv \zeta\overline{\phi} & (\mathrm{mod}\ \mathfrak{L}_1^2) & \Longrightarrow & t \equiv \zeta^4\overline{\phi} & (\mathrm{mod}\ \mathfrak{L}_1^6)
\end{array}$$

to reduce the proof of Proposition 2.15 to a calculation of Hilbert norm residue symbols at the primes of $\mathbf{Q}(\mu_5)$ above 2, 3 and 5. We assume that the reader is familiar with the rules for manipulating these symbols, in particular the product formula, the relationship with the power residue symbol, and Euler's criterion. A good reference is [CF, Exercises 1 and 2]. We further make the observation that if $a \equiv 1 \pmod{\mathfrak{l}^2}$ then $(a,b)_{\mathfrak{l}} = 1$ for all $b \in \mathbf{Z}_5^*$. This observation is useful since $\phi \equiv \overline{\phi} \pmod{\mathfrak{l}^2}$.

(i) $\mathrm{Norm}_{F/\mathbf{Q}}(t) = 100/9$. We have

$$\langle 100/9, b\rangle = \mathrm{Ind}_\zeta(\zeta^4\overline{\phi}, b)_2(\zeta^4\phi, b)_3(\zeta^4\overline{\phi}, b)_{\mathfrak{l}}.$$

Since $\zeta^4\overline{\phi}$ and $\zeta^4\phi$ are units it follows

$$\langle 100/9, 2\rangle = \langle 100/9, 3\rangle = \langle 100/9, 5\rangle = 0. \tag{39}$$

(ii) $\mathrm{Norm}_{F/\mathbf{Q}}(t-1) = 1/9$. We have

$$\langle 1/9, b\rangle = \mathrm{Ind}_\zeta(\zeta^4\overline{\phi}-1, b)_2(\zeta^4\phi-1, b)_3(\zeta^4\overline{\phi}-1, b)_{\mathfrak{l}}.$$

Now $\zeta^4\overline{\phi}-1 = -(2+\zeta^3)$ is a prime above 11, whereas $\zeta^4\phi - 1 = -\zeta\phi$ is a unit. We compute

$$\begin{array}{lclcl}
\langle 1/9, 2\rangle & = & \mathrm{Ind}_\zeta(2/2+\zeta^3) & = & 1 \\
\langle 1/9, 3\rangle & = & 0 & & \\
\langle 1/9, 5\rangle & = & \mathrm{Ind}_\zeta(5/2+\zeta^3) & = & 4.
\end{array} \tag{40}$$

(iii) $\mathrm{Norm}_{F/\mathbf{Q}}(t-2) = 2/9$. We have

$$\langle 2/9, b\rangle = \mathrm{Ind}_\zeta(\zeta^4\overline{\phi}-2, b)_2(\zeta^4\phi-2, b)_3(\zeta^4\overline{\phi}-2, b)_{\mathfrak{l}}.$$

Now $\zeta^4\overline{\phi}-2 = -(3+\zeta^3)$ is a prime above 61, whereas $\zeta^4\phi-2 = -\zeta\phi(2+\zeta^3)$ is a prime above 11. We compute

$$\begin{array}{lclcl}
\langle 2/9, 2\rangle & = & \mathrm{Ind}_\zeta(2/3+\zeta^3) & = & 1 \\
\langle 2/9, 3\rangle & = & \mathrm{Ind}_\zeta(3/2+\zeta^3) & = & 3 \\
\langle 2/9, 5\rangle & = & \mathrm{Ind}_\zeta(5/3+\zeta^3) & = & 2.
\end{array} \tag{41}$$

Proposition 2.15 now follows from (39), (40) and (41) together with linearity of $\langle \cdot, \cdot \rangle$ in the first argument. In fact our calculations are overkill, since we know ahead of time that $\langle \cdot, \cdot \rangle$ is skew-symmetric and that $\lambda = 100/9$ lies in the kernel. So it would have sufficed to compute a single non-zero value of the pairing.

Remark. The Hasse norm theorem guarantees that the elements of $S^{(\phi)}(C_\lambda/\mathbf{Q})$ are norms from F^*/F^{*5}. However we cannot always expect the elements upstairs to belong to $S^{(\phi)}(C_\lambda/F)$. So although the above method applies to several more of the examples in [F1], including some with $m = 7$, we do not claim that it is a general method. Imposing local conditions on the elements upstairs is also undesirable for computations. By comparison with [CaI, Appendix B] we believe that there must be a more general formula for the Cassels-Tate pairing on $S^{(\phi)}(C_\lambda/\mathbf{Q})$ that does not rely on Proposition 2.16.

3. EXAMPLES OVER $\mathbf{Q}$

Let $E/\mathbf{Q}$ be an elliptic curve with $E[m] \simeq \mu_m \times \mathbf{Z}/m\mathbf{Z}$ as a Galois module. We write

$$E'' \xrightarrow{\beta} E \xrightarrow{\alpha} E'$$

for the isogenies with $E[\alpha] = E''[\beta] = \mu_m$ and $E'[\widehat{\alpha}] = E[\widehat{\beta}] = \mathbf{Z}/m\mathbf{Z}$. We may estimate the Mordell-Weil rank using either (i) the pair of isogenies α and $\widehat{\alpha}$, or (ii) the pair of isogenies β and $\widehat{\beta}$, or (iii) the multiplication-by-m map on E. Theorem 4 below makes these estimates explicit in the cases $m = 3$ and 5.

The reader will notice that we have dropped from discussion the case $m = 4$. We believe that the analogue of Theorem 4 in that case would be considerably more complicated. Not least, a proper treatment would need to explain the relationship between the Selmer groups attached to many different isogenies. Let us also note that the elliptic curves $E/\mathbf{Q}$ with $E[4] \simeq \mu_4 \times \mathbf{Z}/4\mathbf{Z}$ are just rather special cases of (1).

3.1. Statement of the main theorem

Let $m = 3$ or 5. Let $E/\mathbf{Q}$ be an elliptic curve with $E[m] \simeq \mu_m \times \mathbf{Z}/m\mathbf{Z}$. Then $E = E_t$ for some $t \in \mathbf{Q}$. We recall from §1.3 that E_t has equations

$$\begin{aligned} m = 3 \qquad & \{\ t(x_0^3 + x_1^3 + x_2^3) - 3x_0x_1x_2 = 0\ \} \subset \mathbf{P}^2 \\ m = 5 \quad & \{\ tx_\nu^2 + x_{\nu-1}x_{\nu+1} - t^2x_{\nu-2}x_{\nu+2} = 0\ \} \subset \mathbf{P}^4 \end{aligned} \tag{42}$$

with $0 = (0:1:-1)$ and $0 = (0:t:1:-1:-t)$ respectively. Alternatively, an equation for E_t in Weierstrass form is given by substituting $\lambda = t^3/27$, respectively $\lambda = t^5$, into the equations for C_λ appearing in §1.1.

In the case $m = 3$ the modular curve $X(3)$ has cusps at $t = 0, 1, \zeta, \zeta^2$. For $t \neq 0, 1$ a rational number we define finite disjoint sets of rational primes

$$
\begin{aligned}
\mathcal{P} &= \{\, p \text{ prime} \mid \operatorname{ord}_p(t/3) > 0 \,\} \\
\mathcal{Q} &= \left\{ p \text{ prime} \;\middle|\; \begin{array}{c} t^2 + t + 1 \equiv 0 \pmod{p} \text{ and } p \equiv 1 \pmod{3} \\ \text{or} \quad p = 3 \text{ and } \operatorname{ord}_3(t+1) \neq 0 \end{array} \right\} \\
\mathcal{R} &= \left\{ p \text{ prime} \;\middle|\; \begin{array}{c} t - 1 \equiv 0 \pmod{p} \text{ and } p \equiv 1 \pmod{3} \\ \text{or} \quad p = 3 \text{ and } t \equiv 1 \text{ or } 4 \pmod{9} \end{array} \right\}.
\end{aligned}
$$

In the case $m = 5$ the modular curve $X(5)$ has cusps at $t = 0, \infty, \zeta^\nu \phi, \zeta^\nu \overline{\phi}$, where ν runs over $\mathbf{Z}/5\mathbf{Z}$. For $t \neq 0$ a rational number we define finite disjoint sets of rational primes

$$
\begin{aligned}
\mathcal{P} &= \{\, p \text{ prime} \mid \operatorname{ord}_p(t) \neq 0 \,\} \\
\mathcal{Q} &= \{\, p \text{ prime} \mid f(t)g(t) \equiv 0 \pmod{p} \text{ and } p \equiv 1 \pmod{5} \,\} \\
\mathcal{R} &= \left\{ p \text{ prime} \;\middle|\; \begin{array}{c} t^2 - t - 1 \equiv 0 \pmod{p} \text{ and } p \equiv 1 \pmod{5} \\ \text{or} \quad p = 5 \text{ and } t \equiv 3 \pmod{5} \end{array} \right\}
\end{aligned}
$$

where $f(t)$ and $g(t)$ are the polynomials (4).

Each prime $p \in \mathcal{Q} \cup \mathcal{R}$ satisfies either $p \equiv 1 \pmod{m}$ or $p = m$. So we may choose non-trivial characters

$$\chi_p : (\mathbf{Z}/p\mathbf{Z})^* \to \mathbf{Z}/m\mathbf{Z}, \text{ respectively } \chi_m : (\mathbf{Z}/m^2\mathbf{Z})^* \to \mathbf{Z}/m\mathbf{Z}.$$

We write $[\mathcal{A}, \mathcal{B}]$ for the matrix with entries $(\chi_q(p))_{p \in \mathcal{A}, q \in \mathcal{B}}$ and define

$$\Xi_\alpha = \begin{pmatrix} [\mathcal{P}, \mathcal{Q}] & [\mathcal{P}, \mathcal{R}] \end{pmatrix} \qquad \Xi_\beta = \begin{pmatrix} [\mathcal{P}, \mathcal{R}] \\ [\mathcal{Q}, \mathcal{R}] \end{pmatrix}$$

$$\Xi_m = \begin{pmatrix} 0 & [\mathcal{P}, \mathcal{Q}] & [\mathcal{P}, \mathcal{R}] \\ -[\mathcal{P}, \mathcal{Q}]^T & [\mathcal{Q}, \mathcal{Q}] - [\mathcal{Q}, \mathcal{Q}]^T & [\mathcal{Q}, \mathcal{R}] \\ -[\mathcal{P}, \mathcal{R}]^T & -[\mathcal{Q}, \mathcal{R}]^T & 0 \end{pmatrix}.$$

It is to be understood that Ξ_m is a skew-symmetric matrix, and that the diagonal entries are therefore zero.

THEOREM 4. *Let $m = 3$ or 5. Let $E/\mathbf{Q}$ be an elliptic curve with $E[m] \simeq \mu_m \times \mathbf{Z}/m\mathbf{Z}$. Then $E \simeq E_t$ for some $t \in \mathbf{Q}$ and t determines matrices Ξ_α, Ξ_β and Ξ_m as above.*
(i) The Selmer groups attached to α and $\widehat{\alpha}$ are $S^{(\alpha)}(E/\mathbf{Q}) \simeq \ker_L(\Xi_\alpha)$ and $S^{(\widehat{\alpha})}(E'/\mathbf{Q}) \simeq \ker_R(\Xi_\alpha)$. The corresponding estimate for rank $E(\mathbf{Q})$ *is*

$$r_\alpha = |\mathcal{P}| + |\mathcal{Q}| + |\mathcal{R}| - 1 - 2\operatorname{rank}(\Xi_\alpha).$$

(ii) The Selmer groups attached to β and $\widehat{\beta}$ are $S^{(\beta)}(E''/\mathbf{Q}) \simeq \ker_L(\Xi_\beta)$ *and* $S^{(\widehat{\beta})}(E/\mathbf{Q}) \simeq \ker_R(\Xi_\beta)$. *The corresponding estimate for* $\operatorname{rank} E(\mathbf{Q})$ *is*

$$r_\beta = |\mathcal{P}| + |\mathcal{Q}| + |\mathcal{R}| - 1 - 2\operatorname{rank}(\Xi_\beta).$$

(iii) Suppose that the characters χ_p for $p \in \mathcal{Q}$ are compatible *in a sense to be defined below. Then* $S^{(m)}(E/\mathbf{Q}) \simeq \ker(\Xi_m)$ *and the corresponding estimate for* $\operatorname{rank} E(\mathbf{Q})$ *is*

$$r_m = |\mathcal{P}| + |\mathcal{Q}| + |\mathcal{R}| - 1 - \operatorname{rank}(\Xi_m).$$

Remarks. (i) The estimates r_α, r_β and r_m are upper bounds which, granted the finiteness of $\text{Ш}(E/\mathbf{Q})$, differ from $\operatorname{rank} E(\mathbf{Q})$ by an even integer. Some authors call these Selmer ranks.
(ii) The choice of characters χ_p does not affect the rank of Ξ_α or Ξ_β, but may affect the rank of Ξ_m. So in computing r_m a further condition on the characters is essential.
(iii) It is clear both from theory and our explicit recipes that $r_m \leq \min\{r_\alpha, r_\beta\}$. In §3.4 and §3.5 we give some examples where this inequality is strict.
(iv) The estimates r_α, r_β and r_m all have the same parity. By Tate's algorithm [Si2, IV.9] together with [R], [Co] it may be checked that the set of places for which E has root number -1 is $\mathcal{P} \cup \mathcal{Q} \cup \mathcal{R} \cup \{\infty\}$. The parity result so obtained is a special case of a theorem of Monsky [Mo].
(v) In the case $m = 5$ we have $E_t \simeq E_{-1/t}$. It is instructive to check that replacing t by $-1/t$ does not alter our estimates r_α, r_β and r_m.

We specify a preferred choice of characters χ_p for primes $p \in \mathcal{Q}$. By definition of $\mathcal{Q}$ we have either $p \equiv 1 \pmod{m}$ or $p = m = 3$. If $p \equiv 1 \pmod{m}$ we may choose[3] $\zeta \in (\mathbf{Z}/p\mathbf{Z})^*$ an element of order m. According as $m = 3$ or 5 we have either $t \equiv \zeta^\nu \pmod{p}$ or $t \equiv \zeta^\nu\phi, \zeta^\nu\overline{\phi} \pmod{p}$ for some $\nu \in (\mathbf{Z}/m\mathbf{Z})^*$. The character

$$\chi_p : (\mathbf{Z}/p\mathbf{Z})^* \to \mathbf{Z}/m\mathbf{Z}\,; \quad x \mapsto x^{(p-1)/m} \text{ followed by } \zeta^\nu \mapsto 1 \tag{43}$$

is independent of our choice of ζ. If $p = m = 3$ we define

$$\chi_3 : (\mathbf{Z}/9\mathbf{Z})^* \to \mathbf{Z}/3\mathbf{Z}\,; \quad 2 \mapsto \left\{ \begin{array}{ll} 1 & \text{if } \operatorname{ord}_3(t+1) < 0 \\ 2 & \text{if } \operatorname{ord}_3(t+1) > 0. \end{array} \right. \tag{44}$$

The case $p = m = 5$ does not occur. We say that the characters χ_p for $p \in \mathcal{Q}$ are *compatible* if they are all chosen to be the same scalar multiple of the characters (43) and (44).

Remark. It would be interesting to understand the relationship between our Theorem 4 and [CSS, Proposition 1.2.3] which express the 2-Selmer group for the curves (1) as the kernel of a (skew-)symmetric pairing.

[3] It is equivalent to choose a prime $\mathfrak{p}$ of $\mathbf{Q}(\mu_m)$ above p.

3.2. Proof of the main theorem

We begin the proof of Theorem 4 by computing the images of the local connecting maps attached to $\alpha : E \to E'$ and $\beta : E'' \to E$. Since m is odd we need only concern ourselves with the finite places.

PROPOSITION 3.1. *Let $E = E_t$ for some $t \in \mathbf{Q}$. Then*

$$\operatorname{im}\delta_{\alpha,p} = \begin{cases} \mathbf{Q}_p^*/\mathbf{Q}_p^{*m} & \text{if } p \in \mathcal{P} \\ \mathbf{Z}_p^*/\mathbf{Z}_p^{*m} & \text{if } p \notin \mathcal{P}\cup\mathcal{Q}\cup\mathcal{R} \\ 1 & \text{if } p \in \mathcal{Q}\cup\mathcal{R} \end{cases}$$

$$\operatorname{im}\delta_{\beta,p} = \begin{cases} \mathbf{Q}_p^*/\mathbf{Q}_p^{*m} & \text{if } p \in \mathcal{P}\cup\mathcal{Q} \\ \mathbf{Z}_p^*/\mathbf{Z}_p^{*m} & \text{if } p \notin \mathcal{P}\cup\mathcal{Q}\cup\mathcal{R} \\ 1 & \text{if } p \in \mathcal{R}. \end{cases}$$

Proof. Assume first that $p \neq m$. We apply Propositions 1.2 and 1.4 for the two values of λ given in the table of §1.3, noting that $\mathbf{Z}_p/\mathbf{Z}_p^{*m}$ is trivial if $p \not\equiv 1 \pmod m$. The case $p = m = 3$ is postponed to §3.3. The remaining details in the case $m = 5$ are recalled from [F1]. ∎

As in §1.3 we take $(E, P, Q) = (E_t, P_t, Q_t)$, so that $e_m(P, Q) = \zeta$ and $Q \in E(\mathbf{Q})$. In the notation of §2.3 we have taken $M = \mu_m$ generated by P and $M^\vee = \mathbf{Z}/m\mathbf{Z}$ generated by Q. The maps $x \mapsto e_m(Q, x)$ and $Q \mapsto 1$ allow us to identify

$$\begin{array}{rclcl} H^1(\mathbf{Q}, M) & = & H^1(\mathbf{Q}, \mu_m) & = & \mathbf{Q}^*/\mathbf{Q}^{*m} \\ H^1(\mathbf{Q}, M^\vee) & = & H^1(\mathbf{Q}, \mathbf{Z}/m\mathbf{Z}) & = & \operatorname{Hom}(G_{\mathbf{Q}}, \mathbf{Z}/m\mathbf{Z}). \end{array} \tag{45}$$

Let $\mathcal{A}$ and $\mathcal{B}$ be finite sets of rational primes and suppose that $\mathcal{B}$ consists of primes p with $p \equiv 1 \pmod m$ or $p = m$. We define

$$\begin{array}{rcl} [\mathcal{A}] & = & \{\theta \in \mathbf{Q}^*/\mathbf{Q}^{*m} \mid \operatorname{ord}_p(\theta) \equiv 0 \pmod m \text{ for all } p \notin \mathcal{A}\} \\ \langle\mathcal{B}\rangle & = & \{\chi \in \operatorname{Hom}(G_{\mathbf{Q}}, \mathbf{Z}/m\mathbf{Z}) \mid \chi_p \text{ is unramified at all } p \notin \mathcal{B}\}. \end{array}$$

Then $[\mathcal{A}]$ has basis $\mathcal{A}$. For each prime $p \in \mathcal{B}$ we choose $p^\vee \in \operatorname{Hom}(G_{\mathbf{Q}}, \mathbf{Z}/m\mathbf{Z})$ a non-trivial element ramified only at p. By class field theory, specifically the Kronecker-Weber theorem, such an element exists and is unique up to scalars. Now $\langle\mathcal{B}\rangle$ has basis $\{p^\vee | p \in \mathcal{B}\}$.

By Proposition 3.1 and Tate local duality we have

$$\begin{array}{rcl} S^{(\alpha)}(E/\mathbf{Q}) & = & \{\, x \in H^1(\mathbf{Q}, M) \mid x_p \in \operatorname{im}\delta_{\alpha,p} \text{ for all primes } p \,\} \\ & = & \{\, x \in [\mathcal{P}] \mid x_p = 0 \text{ for all } p \in \mathcal{Q}\cup\mathcal{R} \,\} \\ S^{(\widehat{\alpha})}(E'/\mathbf{Q}) & = & \{\, x \in H^1(\mathbf{Q}, M^\vee) \mid x_p \in \operatorname{im}\delta_{\widehat{\alpha},p} \text{ for all primes } p \,\} \\ & = & \{\, x \in \langle\mathcal{Q}\cup\mathcal{R}\rangle \mid x_p = 0 \text{ for all } p \in \mathcal{P} \,\}. \end{array}$$

As in [F1, §2.4] we identify $S^{(\alpha)}(E/\mathbf{Q})$ and $S^{(\widehat{\alpha})}(E'/\mathbf{Q})$ as the left and right kernels of a pairing

$$\begin{array}{rcl} [\mathcal{P}] \times \langle\mathcal{Q}\cup\mathcal{R}\rangle & \to & \mathbf{Z}/m\mathbf{Z} \\ (x, y) & \mapsto & \sum_{p\in\mathcal{Q}\cup\mathcal{R}} (x, y)_p \end{array}$$

where $(\cdot,\cdot)_p$ is the Tate pairing. In terms of the bases $\{p\}$ and $\{p^\vee\}$ this pairing is represented by the matrix Ξ_α. We note that the arbitrary choice of characters χ_p corresponds to the arbitrary choice of elements $p^\vee$. Specifically we have taken

$$\chi_p : \mathbf{Z}_p^* \to \mathbf{Z}/m\mathbf{Z}\,; \quad x \mapsto (x, p^\vee)_p. \tag{46}$$

Since $E(\mathbf{Q})[\alpha] = 0$ and $E'(\mathbf{Q})[\widehat{\alpha}] = \mathbf{Z}/m\mathbf{Z}$ it follows from the exact sequence (3) with $\phi = \alpha$ and $\phi = \widehat{\alpha}$ that

$$\begin{aligned} \operatorname{rank} E(\mathbf{Q}) + 1 + \dim_m \text{Ш}(E/\mathbf{Q})[\alpha] + \dim_m \text{Ш}(E'/\mathbf{Q})[\widehat{\alpha}] & \\ = \; |\mathcal{P}| + |\mathcal{Q} \cup \mathcal{R}| - 2\operatorname{rank}(\Xi_\alpha).& \end{aligned}$$

This furnishes the estimate r_α of Theorem 4(i) and granted Proposition 3.1 the proof of Theorem 4(ii) is entirely analogous. Theorem 4(iii) will follow from

Proposition 3.2. *Let $m = 3$ or 5. Let $E = E_t$ for some $t \in \mathbf{Q}$ and suppose that the characters χ_p for $p \in \mathcal{Q}$ are compatible.*
(i) The Cassels-Tate pairing on $S^{(\widehat{\alpha})}(E'/\mathbf{Q})$ is represented by

$$\Xi' = -\begin{pmatrix} [\mathcal{Q},\mathcal{Q}] - [\mathcal{Q},\mathcal{Q}]^T & [\mathcal{Q},\mathcal{R}] \\ -[\mathcal{Q},\mathcal{R}]^T & 0 \end{pmatrix}.$$

(ii) The Cassels-Tate pairing on $S^{(\beta)}(E''/\mathbf{Q})$ is represented by

$$\Xi'' = -\begin{pmatrix} 0 & [\mathcal{P},\mathcal{Q}] \\ -[\mathcal{P},\mathcal{Q}]^T & [\mathcal{Q},\mathcal{Q}] - [\mathcal{Q},\mathcal{Q}]^T \end{pmatrix}.$$

Proof. (i) We read off from Proposition 3.1 that $\mathcal{Q}$ is the set of switching primes. We define some global pairings by summing the local pairings of Proposition 2.9.

$$\begin{aligned} \langle\cdot,\cdot\rangle_{\widehat{\alpha}} \; &: \; \langle \mathcal{Q}\cup\mathcal{R}\rangle \times \langle \mathcal{Q}\cup\mathcal{R}\rangle \to \mathbf{Z}/m\mathbf{Z}\,; \qquad (x,y) \mapsto \textstyle\sum_{p\in\mathcal{Q}} \langle x_p, y_p\rangle_{\widehat{\alpha},p} \\ \langle\cdot,\cdot\rangle_{\beta} \; &: \; [\mathcal{P}\cup\mathcal{Q}] \times [\mathcal{P}\cup\mathcal{Q}] \to \mathbf{Z}/m\mathbf{Z}\,; \qquad (x,y) \mapsto \textstyle\sum_{p\in\mathcal{Q}} \langle x_p, y_p\rangle_{\beta,p} \end{aligned}$$

The Cassels-Tate pairings on $S^{(\widehat{\alpha})}(E'/\mathbf{Q})$ and $S^{(\beta)}(E''/\mathbf{Q})$ are *restrictions* of these pairings. For $p \in \mathcal{Q}$ we now make our choice of global element $p^\vee \in H^1(\mathbf{Q}, M^\vee)$ such that locally at p the isomorphism (31) satisfies

$$H^1(\mathbf{Q}_p, M) \to H^1(\mathbf{Q}_p, M^\vee)\,; \quad p \mapsto p^\vee \tag{47}$$

Later we will check that this choice means the characters χ_p defined by (46) are compatible in the sense of §3.1. Subject to this, we complete the proof of Proposition 3.2 by showing that Ξ' and Ξ'' represent the pairings $\langle\cdot,\cdot\rangle_{\widehat{\alpha}}$

and $\langle\cdot,\cdot\rangle_\beta$ with respect to the bases $\{p\}$ and $\{p^\vee\}$.
(i) For $p, q \in \mathcal{Q}$ distinct primes we compute

$$\begin{array}{rcll} \langle p^\vee, q^\vee\rangle_{\widehat{\alpha}} & = & \langle p^\vee, q^\vee\rangle_{\widehat{\alpha},p} - \langle q^\vee, p^\vee\rangle_{\widehat{\alpha},q} & \text{by Lemma 2.10} \\ & = & (p, q^\vee)_p - (q, p^\vee)_q & \text{by Lemma 2.11 and (47)} \\ & = & -(p, q^\vee)_q + (q, p^\vee)_p & \text{by the product formula} \\ & = & -\chi_q(p) + \chi_p(q) & \text{by (46).} \end{array}$$

The other cases (say with $p \in \mathcal{Q}$ and $q \in \mathcal{R}$) are similar.
(ii) For $p, q \in \mathcal{Q}$ distinct primes we compute

$$\begin{array}{rcll} \langle p, q\rangle_\beta & = & -\langle q, p\rangle_{\beta,p} + \langle p, q\rangle_{\beta,q} & \text{by Lemma 2.10} \\ & = & (q, p^\vee)_p - (p, q^\vee)_q & \text{by Lemma 2.11 and (47)} \\ & = & \chi_p(q) - \chi_q(p) & \text{by (46).} \end{array}$$

The other cases are similar. ∎

To explain how Theorem 4(iii) follows from Proposition 3.2 we need a lemma from linear algebra.

LEMMA 3.3. *Let V be a finite dimensional vector space over a field F. Let $V = U \oplus W$ and write $pr : V \to W$ for the projection map. Let $\langle\cdot,\cdot\rangle$ be a skew-symmetric pairing on V and suppose that U is an isotropic subspace,* i.e. $\langle u, u'\rangle = 0$ *for all $u, u' \in U$. Let $W_1 = W \cap U^\perp$. Then*

$$pr(V^\perp) = W_1 \cap W_1^\perp.$$

Proof. Let $v = u + w \in V^\perp$ with $u \in U$ and $w \in W$. Then $w \in W_1$ since U is isotropic, and $w \in W_1^\perp$ since u, $v \in W_1^\perp$. Thus $pr(V^\perp) \subset W_1 \cap W_1^\perp$.

Conversely, given $w \in W_1 \cap W_1^\perp$ we seek $u \in U$ such that $u + w \in V^\perp$. But for any choice of u, we have $u + w \in U^\perp$, since U is isotropic and $w \in W_1$. Thus it suffices to find $u \in U$ such that $u + w \in W^\perp$. We write $\psi : V \to W^*$ for the linear map induced by $\langle\cdot,\cdot\rangle$. We must show $\psi(w) \in \psi(U)$. By counting dimensions we have $\psi(U) = (W/W_1)^*$. Finally the assumption $w \in W_1^\perp$ implies $\psi(w)$ is trivial on W_1 and we are done. ∎

We apply Lemma 3.3 with $U = [\mathcal{P}]$, $W = \langle \mathcal{Q} \cup \mathcal{R}\rangle$ and $\langle\cdot,\cdot\rangle$ the pairing represented by Ξ_m with respect to the bases $\{p\}$ and $\{p^\vee\}$. By Theorem 4(i) we have $S^{(\alpha)}(E/\mathbf{Q}) = U \cap V^\perp$ and $S^{(\widehat{\alpha})}(E'/\mathbf{Q}) = W_1$. Then Propositions 2.9(i) and 3.2(i) give $\alpha S^{(m)}(E/\mathbf{Q}) = W_1 \cap W_1^\perp$. So Lemma 3.3 allows us to identify the exact sequences

$$0 \longrightarrow S^{(\alpha)}(E/\mathbf{Q}) \longrightarrow S^{(m)}(E/\mathbf{Q}) \xrightarrow{\ \alpha\ } S^{(\widehat{\alpha})}(E'/\mathbf{Q})$$

and

$$0 \longrightarrow U \cap V^\perp \longrightarrow V^\perp \xrightarrow{\ pr\ } W_1.$$

In particular $S^{(m)}(E/\mathbf{Q}) = V^\perp = \ker(\Xi_m)$. Since $E(\mathbf{Q})[m] \simeq \mathbf{Z}/m\mathbf{Z}$ it follows from the exact sequence (3) with $\phi = [m]$ that

$$\operatorname{rank} E(\mathbf{Q}) + 1 + \dim_m Ш(E/\mathbf{Q})[m] = |\mathcal{P} \cup \mathcal{Q} \cup \mathcal{R}| - \operatorname{rank}(\Xi_m).$$

This furnishes the estimate r_m for $\operatorname{rank} E(\mathbf{Q})$.

Remark. Theorem 4(iii) equally follows from Proposition 3.2(ii) and the exact sequence

$$0 \longrightarrow S^{(\widehat{\beta})}(E/\mathbf{Q}) \longrightarrow S^{(m)}(E/\mathbf{Q}) \xrightarrow{\widehat{\beta}} S^{(\beta)}(E''/\mathbf{Q}).$$

In this case we apply Lemma 3.3 with $U = \langle \mathcal{R} \rangle$ and $W = [\mathcal{P} \cup \mathcal{Q}]$.

It remains to examine our choice of characters χ_p for $p \in \mathcal{Q}$. We recall that either $p \equiv 1 \pmod m$ or $p = m = 3$. If $p \equiv 1 \pmod m$ then $\mu_m \subset \mathbf{Q}_p$ and we may apply Corollary 2.14. The identifications (45) suppress the map j_Q. For $x \in \mathbf{Z}_p^*$ we compute

$$\begin{array}{rcll} \chi_p(x) & = & (x, p^\vee)_p & \text{by (46)} \\ & = & -\langle x, p \rangle_{\beta,p} & \text{by Lemma 2.11 and (47)} \\ & = & 1/\nu \ \mathrm{Ind}_\zeta(x,p)_p & \text{by Corollary 2.14} \\ & = & \mathrm{Ind}_{\zeta^\nu}(x/p). & \end{array}$$

But Euler's criterion tells us $(x/p) \equiv x^{(p-1)/m} \pmod p$. So χ_p is the character specified in §3.1. The case $p = m = 3$ is the subject of the next section.

3.3. Further calculations with $p = m = 3$

To complete the proof of Proposition 3.1 we must show

PROPOSITION 3.4. *Let $m = 3$ and $E = E_t$ as in §1.3. Then*

$$\mathrm{im}\, \delta_{\alpha,3} = \left\{ \begin{array}{cl} \mathbf{Q}_3^*/\mathbf{Q}_3^{*3} & \text{if } t \equiv 0 \pmod 9 \\ \mathbf{Z}_3^*/\mathbf{Z}_3^{*3} & \text{if } t \equiv 3,6,7 \pmod 9 \\ 1 & \text{if } t \equiv 1,4 \pmod 9 \text{ or } \mathrm{ord}_3(t+1) \neq 0 \end{array} \right.$$

$$\mathrm{im}\, \delta_{\beta,3} = \left\{ \begin{array}{cl} \mathbf{Q}_3^*/\mathbf{Q}_3^{*3} & \text{if } t \equiv 0 \pmod 9 \text{ or } \mathrm{ord}_3(t+1) \neq 0 \\ \mathbf{Z}_3^*/\mathbf{Z}_3^{*3} & \text{if } t \equiv 3,6,7 \pmod 9 \\ 1 & \text{if } t \equiv 1,4 \pmod 9. \end{array} \right.$$

Proof. (i) Let $\lambda = t^3/27$. Then for $\mathrm{ord}_3(t) > 0$ our description of $\mathrm{im}\, \delta_{\alpha,3}$ follows from Proposition 1.2. We must modify the proof to treat the case $\mathrm{ord}_3(t) \leq 0$. We find $\mathrm{im}\, \delta_{\alpha,3} \subset \mathbf{Z}_3^*/\mathbf{Z}_3^{*3}$ with equality if and only if the congruence

$$x_0^3 + 4x_1^3 + 7x_2^3 - 3t^{-1}x_0x_1x_2 \equiv 0 \pmod{27}$$

is soluble for $x_0, x_1, x_2 \in \mathbf{Z}_3$ not all divisible by 3. Writing $x_\nu = 1 + 3a_\nu$ this is equivalent to $t \equiv 7 \pmod 9$.
(ii) We first make the claim that if $\mathrm{ord}_3(\lambda) = -1$ then $\mathrm{im}\, \delta_{\phi,3} = \mathbf{Q}_3^*/\mathbf{Q}_3^{*3}$. For any $\theta \in \mathbf{Q}_3^*/\mathbf{Q}_3^{*3}$ we may arrange $C_{\lambda,\theta} \simeq T[\tau_0, \tau_1, \tau_2]$ with $\mathrm{ord}_p(\tau_\nu) = (1, -1, -1)$. So our assertion is that for any $b, c \in \mathbf{Z}_3^*$ the equation

$$9x_0^3 + bx_1^3 + cx_2^3 - 3x_0x_1x_2 = 0$$

is soluble over $\mathbf{Z}_3$. Taking $x_1, x_2 = \pm 1$ gives a solution mod 3. We then use Hensel's lemma to solve for $x_0 \in \mathbf{Z}_3$. This proves our claim.

Now let $\lambda = t(t^2+t+1)/(3(2t+1)^3)$. If $\operatorname{ord}_3(t) > 0$ then $\operatorname{ord}_3(\lambda) \geq 0$ and our description of $\operatorname{im}\delta_{\beta,3}$ follows from Proposition 1.2. If $\operatorname{ord}_3(t+1) \neq 0$, then $\operatorname{ord}_3(\lambda) = -1$ and we are done by the above claim. It remains to consider the case $t \equiv 1 \pmod 3$. We recall from §1.3 the identity

$$27\lambda - 1 = \left(\frac{t-1}{2t+1}\right)^3.$$

If $t \equiv 1$ or $4 \pmod 9$ then $\operatorname{ord}_3(27\lambda - 1) \neq 0$. It follows that $\lambda = \tau^3/27$ for some $\tau \in \mathbf{Q}_3$ with either $\operatorname{ord}_3(\tau) < 0$ or $\tau \equiv 1 \pmod 9$. We are done by (i). Finally if $t \equiv 7 \pmod 9$ then $27\lambda \equiv 2 \pmod 3$. By case (e) of the proof of Proposition 1.2 we have $\operatorname{im}\delta_{\beta,3} \subset \mathbf{Z}_3^*/\mathbf{Z}_3^{*3}$. Then Lemma 1.1 shows that we have equality. ∎

Now suppose that 3 is a switching prime, *i.e.* $\operatorname{ord}_3(t+1) \neq 0$. In §3.2 we defined a character

$$\chi_3 : (\mathbf{Z}/9\mathbf{Z})^* \to \mathbf{Z}/3\mathbf{Z}\,; \quad x \mapsto (x, 3^\vee)_3 \tag{48}$$

where $3^\vee \in H^1(\mathbf{Q}, \mathbf{Z}/3\mathbf{Z})$ is unramified outside 3 and satisfies (47). To complete the proof of Theorem 4 it remains to give an explicit description of this character. We make use of the explicit calculations at the end of §2.4. We recall

$$\begin{array}{rcl} j_P\delta_{\widehat{\alpha}}(Q) & = & \zeta(t-\zeta)/(t-\zeta^2) \\ j_Q\delta_\beta(Q)^{-1} & = & t(t^2+t+1)/3. \end{array}$$

The identifications (45) suppress the map j_Q. Since $\langle \cdot, \cdot \rangle_{\beta,3}$ is alternating it is clear that for $x \in \mathbf{Z}_3^*$ we have

$$\langle x, 3 \rangle_{\beta,3} = \langle x, \delta_\beta(Q) \rangle_{\beta,3}. \tag{49}$$

Let $\mathfrak{p} = (1 - \zeta_3)$ be the prime of $\mathbf{Q}(\mu_3)$ above 3. For $x \in \mathbf{Z}_3^*$ we compute

$$\begin{array}{rcll} \chi_3(x) & = & (x, 3^\vee)_3 & \text{by (48)} \\ & = & (x, \delta_{\widehat{\alpha}}(Q))_3 & \text{by Lemma 2.11 and (49)} \\ & = & -(x, \delta_{\widehat{\alpha}}(Q))_{\mathfrak{p}} & \text{since } [\mathbf{Q}(\mu_3)_{\mathfrak{p}} : \mathbf{Q}_3] = 2 \\ & = & \operatorname{Ind}_\zeta(x, j_P\delta_{\widehat{\alpha}}(Q))_{\mathfrak{p}} & \text{by (33)} \\ & = & \left\{ \begin{array}{ll} \operatorname{Ind}_\zeta(x, \zeta)_{\mathfrak{p}} & \text{if } \operatorname{ord}_3(t+1) < 0 \\ \operatorname{Ind}_\zeta(x, \zeta^2)_{\mathfrak{p}} & \text{if } \operatorname{ord}_3(t+1) > 0. \end{array} \right. & \end{array}$$

But $(2, \zeta)_{\mathfrak{p}} = (\zeta/2) = \zeta$. So χ_3 is the character specified in §3.1. The proof of Theorem 4 is now complete.

3.4. Examples with $E[3] \simeq \mu_3 \times \mathbf{Z}/3\mathbf{Z}$

We apply Theorem 4 to all elliptic curves $E/\mathbf{Q}$ with $E[3] \simeq \mu_3 \times \mathbf{Z}/3\mathbf{Z}$ and conductor $N \leq 10^4$. With the help of Cremona's tables [Cr2] we know that there are 264 such curves. All but 4 satisfy one of

(i) $Ш(E/\mathbf{Q})(3) = Ш(E'/\mathbf{Q})(3) = Ш(E''/\mathbf{Q})(3) = 0$
(ii) $Ш(E/\mathbf{Q})(3) = Ш(E'/\mathbf{Q})(3) = 0$ and $Ш(E''/\mathbf{Q})(3) \simeq (\mathbf{Z}/3\mathbf{Z})^2$
(iii) $Ш(E/\mathbf{Q})(3) = Ш(E''/\mathbf{Q})(3) = 0$ and $Ш(E'/\mathbf{Q})(3) \simeq (\mathbf{Z}/3\mathbf{Z})^2$.

We record, against the rank, the frequency with which these possibilities occur.

	(i)	(ii)	(iii)	other
$\operatorname{rank} E(\mathbf{Q}) = 0$	84	58	5	4
$\operatorname{rank} E(\mathbf{Q}) = 1$	103	5	0	0
$\operatorname{rank} E(\mathbf{Q}) = 2$	5	0	0	0

The exceptional curves are $E = E_t$ for $t = 1/9, -1/31, 18/17$ and $105/104$. Their behaviour is illustrated in Examples 1 and 2 below. Table 1 in §3.6 gives data for the first 40 of the 264 curves.

Example 1. Let $E = E_t$ and $t = 1/9$. Then E, E', E'' are labelled 4914N2,1,3 in Cremona's tables. We have $\mathcal{P} = \emptyset$, $\mathcal{Q} = \{3, 7, 13\}$ and $\mathcal{R} = \emptyset$. A compatible choice of characters is

$$\begin{array}{ll} \chi_3 : (\mathbf{Z}/9\mathbf{Z})^* \to \mathbf{Z}/3\mathbf{Z}\,; & x \mapsto x^2 \text{ followed by } 4 \mapsto 1 \\ \chi_7 : (\mathbf{Z}/7\mathbf{Z})^* \to \mathbf{Z}/3\mathbf{Z}\,; & x \mapsto x^2 \text{ followed by } 4 \mapsto 1 \\ \chi_{13} : (\mathbf{Z}/13\mathbf{Z})^* \to \mathbf{Z}/3\mathbf{Z}\,; & x \mapsto x^4 \text{ followed by } 3 \mapsto 1. \end{array}$$

The matrix Ξ_3 has entries in $\mathbf{Z}/3\mathbf{Z}$

	3	7	13
3	0	1	2
7	2	0	2
13	1	1	0

Theorem 4 gives $r_\alpha = r_\beta = 2$ and $r_3 = 0$. So $E(\mathbf{Q})$ has rank 0 and

$$\begin{array}{lcl} Ш(E/\mathbf{Q})(3) & = & 0 \\ Ш(E'/\mathbf{Q})(3) & \simeq & (\mathbf{Z}/3\mathbf{Z})^2 \\ Ш(E''/\mathbf{Q})(3) & \simeq & (\mathbf{Z}/3\mathbf{Z})^2. \end{array}$$

Example 2. Let $E = E_t$ and $t = 18/17$. Then E, E', E'' are labelled 5514A2,1,3 in Cremona's tables. We have $\mathcal{P} = \{2, 3\}$, $\mathcal{Q} = \{919\}$ and $\mathcal{R} = \emptyset$. But $2^{306} \equiv 3^{306} \equiv 1 \pmod{919}$. So Ξ_3 is the zero matrix and Theorem 4 gives $r_\alpha = r_\beta = r_3 = 2$. Cremona's tables tell us that $E(\mathbf{Q})$ has rank 0. We deduce

$$Ш(E''/\mathbf{Q})[\beta] = Ш(E''/\mathbf{Q})[3] \simeq (\mathbf{Z}/3\mathbf{Z})^2.$$

By Proposition 3.2(ii) the Cassels-Tate pairing on this space is trivial. Theorem 3 applied to the multiplication-by-3 map on E'' then shows that $\text{Ш}(E''/\mathbf{Q})$ contains an element of order 9.

We give an example beyond the range of Cremona's tables.

EXAMPLE 3. Let $E = E_t$ and $t = 124/167$. We have $\mathcal{P} = \{2, 31\}$, $\mathcal{Q} = \{3, 7, 13, 19, 37\}$ and $\mathcal{R} = \{43\}$. Making a compatible choice of characters the matrix Ξ_3 is

	2	31	3	7	13	19	37	43
2	0	0	2	2	1	1	1	0
31	0	0	1	1	0	0	0	1
3	1	2	0	2	0	1	2	1
7	1	2	1	0	2	1	0	2
13	2	0	0	1	0	0	1	2
19	2	0	2	2	0	0	2	1
37	2	0	1	0	2	1	0	1
43	0	2	2	1	1	2	2	0

We find $r_\alpha = 3$, $r_\beta = 5$ and $r_3 = 1$. Let $\lambda = t(t^2 + t + 1)/(3(2t + 1)^3) = 2^2.31.3^2.7.13.19.37/1245^3$ and $\theta = 3534 = 2.31.3.19$. By Lemma 1.5 the torsor $C_{\lambda,\theta}$ has equation

$$x_0^3 + 3534x_1^3 + 20202x_2^3 - 1245x_0x_1x_2 = 0.$$

A solution is $(x_0 : x_1 : x_2) = (12 : 1 : -1)$. Thus $E(\mathbf{Q})$ has rank 1 and

$$\begin{array}{lcl} \text{Ш}(E/\mathbf{Q})(3) & = & 0 \\ \text{Ш}(E'/\mathbf{Q})(3) & \simeq & (\mathbf{Z}/3\mathbf{Z})^2 \\ \text{Ш}(E''/\mathbf{Q})(3) & \simeq & (\mathbf{Z}/3\mathbf{Z})^4. \end{array}$$

3.5. Examples with $E[5] \simeq \mu_5 \times \mathbf{Z}/5\mathbf{Z}$

Cremona's tables [Cr2] tell us that there are only 3 elliptic curves $E/\mathbf{Q}$ with $E[5] \simeq \mu_5 \times \mathbf{Z}/5\mathbf{Z}$ and conductor $N \leq 10^4$. Instead we search over all $E = E_t$ with $t = a/b$, a, b coprime integers and $|a|, |b| \leq 10^3$. Table 2 gives data for the first 40 of these curves, ordered by conductor. We give further details for some of the curves on our list, beginning with the example considered by Beaver [Be]. Let us note that $E = E_{-5}$ has *non-split* multiplicative reduction at $p = 29$.

EXAMPLE 4. Let $E = E_t$ and $t = -5$. We have $\mathcal{P} = \{5\}$, $\mathcal{Q} = \{11, 31, 991\}$ and $\mathcal{R} = \emptyset$. Beaver made a compatible choice of characters

$$\begin{array}{ll} \chi_{11} : (\mathbf{Z}/11\mathbf{Z})^* \to \mathbf{Z}/5\mathbf{Z}\,; & x \mapsto x^2 \text{ followed by } 5 \mapsto 1 \\ \chi_{31} : (\mathbf{Z}/31\mathbf{Z})^* \to \mathbf{Z}/5\mathbf{Z}\,; & x \mapsto x^6 \text{ followed by } 16 \mapsto 1 \\ \chi_{991} : (\mathbf{Z}/991\mathbf{Z})^* \to \mathbf{Z}/5\mathbf{Z}\,; & x \mapsto x^{198} \text{ followed by } 799 \mapsto 1. \end{array}$$

The matrix Ξ_5 has entries in $\mathbf{Z}/5\mathbf{Z}$

	5	11	31	991
5	0	2	0	2
11	3	0	0	3
31	0	0	0	0
991	3	2	0	0

Theorem 4 gives $r_\alpha = r_5 = 1$ and $r_\beta = 3$. An L-value computation, details of which appear in [Be], shows that $E(\mathbf{Q})$ has rank 1. We deduce

$$Ш(E/\mathbf{Q})(5) = Ш(E'/\mathbf{Q})(5) = 0 \quad \text{and} \quad Ш(E''/\mathbf{Q})(5) \simeq (\mathbf{Z}/5\mathbf{Z})^2.$$

As Beaver conjectured the hypothesis "$\lambda_{11} \neq 0$" of [Be, Corollary 1.3] is unnecessary.

COROLLARY 3.5. *Let $E = E_t$ with $t \in \mathbf{Z}$, $\mathrm{ord}_5(t) > 0$, $\mathrm{ord}_{11}(t) = 0$ and $t^2 - t - 1$ not divisible by any prime congruent to 1 mod 5. Then $Ш(E''/\mathbf{Q})$ contains a subgroup isomorphic to $(\mathbf{Z}/5\mathbf{Z})^2$.*

Proof. Since $(t^2 - t - 1)f(t)g(t) = t^{10} - 11t^5 - 1$ it is clear[4] that 11 always belongs to one of the sets $\mathcal{P}$, $\mathcal{Q}$ or $\mathcal{R}$. Our hypotheses now give $5 \in \mathcal{P}$, $11 \in \mathcal{Q}$ and $\mathcal{R} = \emptyset$. Then Theorem 4(ii) and Proposition 3.2(ii) tell us that the Cassels-Tate pairing on $S^{(\beta)}(E''/\mathbf{Q})$ is non-zero. The result follows. ∎

In fact Beaver only considered the case $\mathrm{ord}_5(t) > 0$. So the next two examples are new.

EXAMPLE 5. Let $E = E_t$ and $t = 7$. We have $\mathcal{P} = \{7\}$, $\mathcal{Q} = \{11, 31, 61, 331\}$ and $\mathcal{R} = \{41\}$. Making a compatible choice of characters the matrix Ξ_5 is

	7	11	31	61	331	41
7	0	4	3	2	1	1
11	1	0	1	2	2	2
31	2	4	0	2	1	2
61	3	3	3	0	2	1
331	4	3	4	3	0	0
41	4	3	3	4	0	0

Theorem 4 gives $r_\alpha = r_\beta = 3$ and $r_5 = 1$. Table 4 in §3.6 exhibits a rational point of infinite order. Thus $E(\mathbf{Q})$ has rank 1 and

$$\begin{aligned} Ш(E/\mathbf{Q})(5) &= 0 \\ Ш(E'/\mathbf{Q})(5) &\simeq (\mathbf{Z}/5\mathbf{Z})^2 \\ Ш(E''/\mathbf{Q})(5) &\simeq (\mathbf{Z}/5\mathbf{Z})^2. \end{aligned}$$

[4] Alternatively, applying Hasse's bounds to the reduction of E at a prime of $\mathbf{Q}(\mu_5)$ above 11, we see that E must have bad reduction at 11.

EXAMPLE 6. Let $E = E_t$ and $t = 5/4$. We have $\mathcal{P} = \{2,5\}$, $\mathcal{Q} = \{521, 4621\}$ and $\mathcal{R} = \{11\}$. Making a compatible choice of characters the matrix Ξ_5 is

	2	5	521	4621	11
2	0	0	2	2	1
5	0	0	3	3	4
521	3	2	0	4	2
4621	3	2	1	0	0
11	4	1	3	0	0

Theorem 4 gives $r_\alpha = r_\beta = r_5 = 2$. According to `pari` $L(E,1) \neq 0$. By the work of Kolyvagin, $E(\mathbf{Q})$ has rank 0. We deduce

$$Ш(E''/\mathbf{Q})[\beta] = Ш(E''/\mathbf{Q})[5] \simeq (\mathbf{Z}/5\mathbf{Z})^2.$$

By Proposition 3.2(ii) the Cassels-Tate pairing on this space is trivial. It follows that $Ш(E''/\mathbf{Q})$ contains an element of order 25.

3.6. Tables

Tables 1 and 2. We apply Theorem 4 to the first 40 elliptic curves $E/\mathbf{Q}$ with $E[m] \simeq \mu_m \times \mathbf{Z}/m\mathbf{Z}$, ordered by conductor. In the case $m = 3$ our list is extracted from Cremona's tables [Cr2] and so guaranteed to be complete. In the case $m = 5$ we have checked that there are no gaps within the range of Table 6. Table 1 ($m = 3$) lists our parameter t, the conductor N, the Cremona labels # for E, E', E'', the sets of primes $\mathcal{P}, \mathcal{Q}, \mathcal{R}$, the estimates r_α, r_β, r_3 and finally $r = \operatorname{rank} E(\mathbf{Q})$ taken directly from Cremona's tables. Table 2 ($m = 5$) has the same column headings, except that we omit the Cremona labels, and the entry $r = \operatorname{rank} E(\mathbf{Q})$ remains to be justified below. It is unconditional in all cases except $t = -8$.

Tables 3 and 4. The curves listed in Table 2 are nearly all beyond the range of Cremona's tables. We perform some further computations whenever $r_5 > 0$. Theorem 4 suggests that $C_{\lambda,\theta}(\mathbf{Q}) \neq \emptyset$ for $\lambda = tf(t)/g(t)$ and certain $\theta \in \mathbf{Q}^*/\mathbf{Q}^{*5}$. Lemma 1.5 provides equations for $C_{\lambda,\theta}$ in the form $T[\tau_0, \ldots, \tau_4]$, and we may arrange for the τ_ν to be coprime. We write $\tau_\nu = a_\nu/b_\nu$ with a_ν, b_ν coprime integers and $b_\nu > 0$. Putting $x_\nu = b_\nu X_\nu$ we arrive at the equations

$$\{ \; a_\nu b_\nu X_\nu^2 + b_{\nu-1} b_{\nu+1} X_{\nu-1} X_{\nu+1} - a_{\nu-2} a_{\nu+2} X_{\nu-2} X_{\nu+2} = 0 \; \} \subset \mathbf{P}^4$$

where as usual ν runs over $\mathbf{Z}/5\mathbf{Z}$. Table 3 records when a search for $\mathbf{Q}$-points was successful. Next we use the degree 5 map $C_{\lambda,\theta} \to D_\lambda$, given in [F0, Appendix C], to determine rational points of infinite order on E. We record these solutions to (42) in Table 4, together with their canonical height. In accordance with [Cr1, §3.4] our heights are twice those computed by `pari`. We note that cyclically permuting the x_ν corresponds to addition of 5-torsion. So no essentially new solutions are obtained in this way. Similarly, reversing the order of the x_ν corresponds to the map $[-1]$.

We justify the entries $r = \operatorname{rank} E(\mathbf{Q})$ in Table 2. In the cases where Table 4 fails to exhibit sufficient points of infinite order, we make use of the following implications due to Wiles, Kolyvagin, Gross and Zagier.

$$\begin{array}{lcl} \operatorname{ord}_{s=1} L(E,s) = 0 & \Longrightarrow & \operatorname{rank} E(\mathbf{Q}) = 0 \\ \operatorname{ord}_{s=1} L(E,s) = 1 & \Longrightarrow & \operatorname{rank} E(\mathbf{Q}) = 1. \end{array} \tag{50}$$

We also make use of the program `bg.gp` written by T. Womack [W] that computes $L^{(r)}(E,1)$ using the Buhler-Gross algorithm.

If $r_5 = 1$ then Remark (iv) of §3.1 tells us that $\operatorname{ord}_{s=1} L(E,s)$ is odd. Running `bg.gp` we find $L'(E,1) \neq 0$. By (50) we have $r = 1$. Our 5-descent then gives $\text{Ш}(E/\mathbf{Q})(5) = 0$, and assuming $\text{Ш}(E/\mathbf{Q}) = 0$, the Birch Swinnerton-Dyer conjecture predicts the minimal height of a rational point of infinite order. To the accuracy of T. Womack's program this agrees with the heights of the points listed in Table 4.

If $r_5 = 2$ then Remark (iv) of §3.1 tells us that $\operatorname{ord}_{s=1} L(E,s)$ is even. The case $t = 5/4$ was treated in Example 6 of §3.5. In the remaining cases, Table 4 lists at least one point of infinite order. By (50) we have $L(E,1) = 0$. Running `bg.gp` we find $L''(E,1) \neq 0$. Assuming the weak Birch Swinnerton-Dyer conjecture it follows that $r = 2$. Our 5-descent then gives $\text{Ш}(E/\mathbf{Q})(5) = 0$, and assuming $\text{Ш}(E/\mathbf{Q}) = 0$, the Birch Swinnerton-Dyer conjecture predicts a value for the regulator

t	-6	-8	$-9/2$	-12
Regulator	12.686	196.322	41.688	76.056

In the cases $t = -6, -9/2, -12$, Table 4 lists two independent points of infinite order. They generate a subgroup with the predicted regulator. In the case $t = -8$ we have found only one of the generators. The claim $r = 2$ remains conditional on either the weak Birch Swinnerton-Dyer conjecture, or equally on the finiteness of $\text{Ш}(E/\mathbf{Q})(5)$. The predicted value of the regulator suggests that we are looking for a second generator whose height is approximately 66.

Tables 5 and 6. Finally we apply Theorem 4 for all rational numbers t of the form a/b with a, b coprime integers and $|a|, |b| \leq 10^3$. For $m = 3$ we obtain data for $1\,216\,765 \approx 2.10^6(6/\pi^2)$ curves. For $m = 5$ we ignore repeats of the form t and $-1/t$, and so obtain data for $608\,383 \approx 10^6(6/\pi^2)$ curves. Tables 5 and 6 give a frequency count for each of the estimates r_α, r_β, $\min\{r_\alpha, r_\beta\}$ and r_m. The second number in each column is a percentage. For example, in the case $m = 3$, we find $4\,101$ curves with $\min\{r_\alpha, r_\beta\} = 4$. These amount to $4\,101/1\,216\,765 \times 100\% \approx 0.34\%$ of the curves considered. We see that the estimate r_m is often an improvement on both r_α and r_β. We also see that r_β is usually much larger than r_α. It is therefore somewhat perverse that our proof of Theorem 1 works by showing that $r_\alpha - r_\beta$ may become arbitrarily large.

Table 1 Elliptic curves $E/\mathbf{Q}$ with $E[3] \simeq \mu_3 \times \mathbf{Z}/3\mathbf{Z}$

t	N	#	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{R}$	r_α	r_β	r_3	r
-3	14	A1, 4, 3	$\emptyset$	$\{7\}$	$\emptyset$	0	0	0	0
$3/5$	14	A2, 6, 5	$\emptyset$	$\{7\}$	$\emptyset$	0	0	0	0
$3/2$	19	A1, 3, 2	$\emptyset$	$\{19\}$	$\emptyset$	0	0	0	0
3	26	A1, 3, 2	$\emptyset$	$\{13\}$	$\emptyset$	0	0	0	0
∞	27	A1, 3, 2	$\emptyset$	$\{3\}$	$\emptyset$	0	0	0	0
$-1/2$	27	A3, 4, 1	$\emptyset$	$\emptyset$	$\{3\}$	0	0	0	0
$-3/2$	35	A1, 3, 2	$\emptyset$	$\{7\}$	$\emptyset$	0	0	0	0
$3/4$	37	B1, 3, 2	$\emptyset$	$\{37\}$	$\emptyset$	0	0	0	0
$-3/5$	38	A1, 3, 2	$\emptyset$	$\{19\}$	$\emptyset$	0	0	0	0
-1	54	A1, 3, 2	$\emptyset$	$\{3\}$	$\emptyset$	0	0	0	0
-2	54	B1, 3, 2	$\{2\}$	$\emptyset$	$\emptyset$	0	0	0	0
$-3/8$	77	B1, 3, 2	$\emptyset$	$\{7\}$	$\emptyset$	0	0	0	0
$-3/4$	91	B2, 1, 3	$\emptyset$	$\{13\}$	$\{7\}$	1	1	1	1
$-4/5$	126	A3, 5, 1	$\{2\}$	$\{7\}$	$\{3\}$	0	0	0	0
$2/11$	126	A4, 6, 2	$\{2\}$	$\{7\}$	$\{3\}$	0	0	0	0
$3/7$	158	D1, 3, 2	$\emptyset$	$\{79\}$	$\emptyset$	0	0	0	0
$-1/8$	171	B2, 3, 1	$\emptyset$	$\{19\}$	$\{3\}$	1	1	1	1
$6/5$	182	B2, 1, 3	$\{2\}$	$\{7, 13\}$	$\emptyset$	0	2	0	0
$1/2$	189	B2, 1, 3	$\emptyset$	$\{3, 7\}$	$\emptyset$	1	1	1	1
$1/4$	189	C1, 3, 2	$\emptyset$	$\{7\}$	$\emptyset$	0	0	0	0
$-2/7$	234	E2, 3, 1	$\{2\}$	$\{13\}$	$\{3\}$	0	0	0	0
$6/7$	254	A2, 1, 3	$\{2\}$	$\{127\}$	$\emptyset$	1	1	1	1
$-3/13$	278	B1, 3, 2	$\emptyset$	$\{139\}$	$\emptyset$	0	0	0	0
$-5/4$	315	A2, 3, 1	$\{5\}$	$\{7\}$	$\{3\}$	0	0	0	0
$3/11$	326	C1, 3, 2	$\emptyset$	$\{163\}$	$\emptyset$	0	0	0	0
$1/10$	333	A2, 3, 1	$\emptyset$	$\{37\}$	$\{3\}$	1	1	1	1
-8	342	A2, 3, 1	$\{2\}$	$\{19\}$	$\{3\}$	0	0	0	0
$-3/7$	370	C1, 3, 2	$\emptyset$	$\{37\}$	$\emptyset$	0	0	0	0
2	378	A2, 1, 3	$\{2\}$	$\{3, 7\}$	$\emptyset$	0	2	0	0
$-1/5$	378	B1, 3, 2	$\emptyset$	$\{7\}$	$\emptyset$	0	0	0	0
4	378	E1, 3, 2	$\{2\}$	$\{7\}$	$\{3\}$	0	0	0	0
$-1/3$	378	F2, 1, 3	$\emptyset$	$\{3, 7\}$	$\emptyset$	1	1	1	1
$-9/7$	402	D2, 1, 3	$\{3\}$	$\{67\}$	$\emptyset$	1	1	1	1
6	430	C2, 1, 3	$\{2\}$	$\{43\}$	$\emptyset$	1	1	1	1
-6	434	B2, 1, 3	$\{2\}$	$\{31\}$	$\{7\}$	0	0	0	0
$3/8$	485	A1, 3, 2	$\emptyset$	$\{97\}$	$\emptyset$	0	0	0	0
9	546	D2, 1, 3	$\{3\}$	$\{7, 13\}$	$\emptyset$	0	2	0	0
$9/8$	651	E2, 1, 3	$\{3\}$	$\{7, 31\}$	$\emptyset$	0	2	0	0
$-6/5$	682	A2, 1, 3	$\{2\}$	$\{31\}$	$\emptyset$	1	1	1	1
$11/2$	693	C2, 3, 1	$\{11\}$	$\{7\}$	$\{3\}$	0	0	0	0

Table 2 Elliptic curves $E/\mathbf{Q}$ with $E[5] \simeq \mu_5 \times \mathbf{Z}/5\mathbf{Z}$

t	N	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{R}$	r_α	r_β	r_5	r
1	11	$\emptyset$	$\{11\}$	$\emptyset$	0	0	0	0
-2	550	$\{2\}$	$\{11\}$	$\{5\}$	0	0	0	0
2	1 342	$\{2\}$	$\{11, 61\}$	$\emptyset$	0	2	0	0
3	33 825	$\{3\}$	$\{11, 41\}$	$\{5\}$	1	1	1	1
$3/2$	165 066	$\{2, 3\}$	$\{11, 41, 61\}$	$\emptyset$	0	4	0	0
-3	185 163	$\{3\}$	$\{31, 181\}$	$\{11\}$	1	1	1	1
-4	192 698	$\{2\}$	$\{11, 461\}$	$\emptyset$	0	2	0	0
$-3/2$	861 366	$\{2, 3\}$	$\{31, 421\}$	$\{11\}$	0	2	0	0
$-4/3$	2 032 734	$\{2, 3\}$	$\{11, 1621\}$	$\emptyset$	1	3	1	1
4	2 074 622	$\{2\}$	$\{181, 521\}$	$\{11\}$	1	1	1	1
$4/3$	2 097 150	$\{2, 3\}$	$\{11, 31, 41\}$	$\{5\}$	1	3	1	1
$5/3$	20 301 765	$\{3, 5\}$	$\{11, 41, 3001\}$	$\emptyset$	0	4	0	0
5	48 656 245	$\{5\}$	$\{11, 101, 461\}$	$\emptyset$	1	3	1	1
-5	48 999 995	$\{5\}$	$\{11, 31, 991\}$	$\emptyset$	1	3	1	1
$-8/3$	68 986 434	$\{2, 3\}$	$\{11, 101, 131\}$	$\emptyset$	0	4	0	0
$5/2$	86 646 010	$\{2, 5\}$	$\{421, 1871\}$	$\{11\}$	0	2	0	0
$-5/2$	108 646 010	$\{2, 5\}$	$\{11, 151, 211\}$	$\{31\}$	1	3	1	1
$7/4$	257 915 350	$\{2, 7\}$	$\{11, 31, 2161\}$	$\{5\}$	1	3	1	1
$5/4$	264 829 510	$\{2, 5\}$	$\{521, 4621\}$	$\{11\}$	2	2	2	0
$-5/3$	270 895 515	$\{3, 5\}$	$\{11, 211, 251\}$	$\{31\}$	1	3	1	1
6	362 283 834	$\{2, 3\}$	$\{11, 191, 991\}$	$\emptyset$	0	4	0	0
-6	363 310 266	$\{2, 3\}$	$\{11, 31, 61, 71\}$	$\{41\}$	2	4	2	2
-7	395 724 175	$\{7\}$	$\{311, 661\}$	$\{5, 11\}$	2	0	0	0
8	429 352 550	$\{2\}$	$\{661, 1181\}$	$\{5, 11\}$	2	0	0	0
$-5/4$	439 170 490	$\{2, 5\}$	$\{11, 31, 4441\}$	$\emptyset$	0	4	0	0
$8/5$	624 238 010	$\{2, 5\}$	$\{11, 31, 61, 3001\}$	$\emptyset$	1	5	1	1
$9/4$	1 538 513 394	$\{2, 3\}$	$\{11, 181, 4441\}$	$\emptyset$	0	4	0	0
7	1 976 032 597	$\{7\}$	$\{11, 31, 61, 331\}$	$\{41\}$	3	3	1	1
-8	2 148 204 542	$\{2\}$	$\{11, 491, 2801\}$	$\{71\}$	2	2	2	2
$7/2$	3 871 814 254	$\{2, 7\}$	$\{11, 41, 131, 151\}$	$\{31\}$	2	4	0	0
$-7/2$	4 037 464 046	$\{2, 7\}$	$\{11, 431, 1031\}$	$\emptyset$	0	4	0	0
$-9/2$	4 209 082 350	$\{2, 3\}$	$\{11, 31, 61, 71\}$	$\{5\}$	2	4	2	2
$7/3$	4 987 312 869	$\{3, 7\}$	$\{11, 701, 1621\}$	$\emptyset$	0	4	0	0
$8/3$	5 916 563 466	$\{2, 3\}$	$\{11, 41, 251, 281\}$	$\{31\}$	2	4	0	0
$6/5$	6 497 983 470	$\{2, 3, 5\}$	$\{11, 31, 101, 331\}$	$\emptyset$	0	6	0	0
$-7/4$	6 590 370 094	$\{2, 7\}$	$\{11, 41, 71, 241\}$	$\{61\}$	2	4	0	0
-12	6 754 920 150	$\{2, 3\}$	$\{11, 41, 3221\}$	$\{5, 31\}$	2	2	2	2
$-7/3$	6 874 167 531	$\{3, 7\}$	$\{11, 71, 6871\}$	$\{61\}$	1	3	1	1
$11/3$	8 333 929 857	$\{3, 11\}$	$\{31, 101, 1021\}$	$\emptyset$	0	4	0	0
-10	9 091 909 090	$\{2, 5\}$	$\{11, 31, 61, 401\}$	$\emptyset$	1	5	1	1

Table 3 Rational points on $T[\tau_0, \tau_1, \tau_2, \tau_3, \tau_4]$

t	$(\tau_0, \tau_1, \tau_2, \tau_3, \tau_4)$	$(X_0 : X_1 : X_2 : X_3 : X_4)$
3	$(1, 41, 1/11, 1, 3)$	$(2 : 1 : 1 : 7 : 3)$
-3	$(3, 1/181, 1, 1, -31)$	$(7 : 1 : -17 : 2 : -1)$
$4/3$	$(1, 4/3, 1/41, 31, 11)$	$(2 : 21 : 2 : -4 : -4)$
$-5/2$	$(1/151, 1/2, 1/11, 1, -1055)$	$(1 : 86 : -7 : 3 : -1)$
$7/4$	$(1/4, 2161, 7, 1, 1/341)$	$(27 : 4 : 14 : -694 : -52)$
$-5/3$	$(1, 211/11, 1, 5/251, -1/3)$	$(5666 : 149 : -9811 : -167 : -4863)$
-6	$(1, 1/31, 22, 1/61, -213)$	$(17 : 5 : -8 : 1 : -3)$
	$(22/61, 3, 71/31, 1, -1)$	$(2 : 67 : -1 : 65 : -149)$
7	$(1, 7, 331, 11, 1/1891)$	$(5 : 13 : 1 : -27 : -4)$
-8	$(1/491, 8, 2801, 1/11, -1)$	$(-4 : 41 : -2 : -12 : 1448)$
$-9/2$	$(11/31, 1, 1, 549/71, -1/2)$	$(-9 : 207 : -177 : -1 : 168)$
	$(1/2, 1, 9/2201, 61, -11)$	$(90 : 519 : -1 : -21 : -9)$
-12	$(1/121, 1, 9663, 1, -4/41)$	$(211 : 175 : -3 : -169 : -68)$
	$(3221, 1, 3, 1/121, -4/41)$	$(26 : 356 : 740 : 514 : -71)$

Table 4 Mordell-Weil generators for $E = E_t$

t	$(x_0 : x_1 : x_2 : x_3 : x_4)$	height
3	$(6 : 81 : 21 : 31 : 71)$	1.134
-3	$(189 : -1893 : 1037 : 482 : -2433)$	2.641
$-4/3$	*generator not known*	33.633
4	*generator not known*	22.371
$4/3$	$(7502 : -56208 : -46608 : 37942 : 57267)$	3.595
5	*generator not known*	34.142
-5	*generator not known*	29.241
$-5/2$	$(10505 : -48848 : 39977 : 12630 : -70250)$	3.776
$7/4$	$(4118592447 : 31088470672 : 13020915922 : -20707618498 : -27516097648)$	8.637
$-5/3$	$(11545293032268586 : -6439289981637105 : -5956542269698375 :$ $11787905264099415 : -4210746652191867)$	14.152
-6	$(51 : -891 : 786 : 64 : -2050)$	2.244
	$(331728 : -29317538 : 7117825 : 4046253 : -35387658)$	6.202
$8/5$	*generator not known*	80.610
7	$(175 : -304604 : -47007 : 41867 : 316589)$	4.280
-8	$(352 : -23168 : 372 : -8101 : 8282)$	2.992
	generator not known	≈ 66
$-9/2$	$(275581521 : 525816846 : -1540675614 : 43145111 : -1910013504)$	7.362
	$(1798854480 : -55092369 : 1126546802 : -637931742 : -155814921)$	7.471
-12	$(29830412804 : -274049792 : -7483139508 : 9909498771 : -157064775)$	8.531
	$(25841586446 : -1537085461 : 121031257722 : -455623920 : -47238156912)$	9.028
$-7/3$	*generator not known*	70.563
-10	*generator not known*	108.806

Table 5 Elliptic curves $E/\mathbf{Q}$ with $E[3] \simeq \mu_3 \times \mathbf{Z}/3\mathbf{Z}$

	r_α		r_β		$\min\{r_\alpha, r_\beta\}$		r_3	
0	247 594	20.35	57 032	4.69	267 633	22.00	378 527	31.11
1	512 138	42.09	213 730	17.57	536 514	44.09	582 220	47.85
2	350 525	28.81	351 275	28.87	336 657	27.67	229 402	18.85
3	95 849	7.88	333 628	27.42	71 844	5.90	26 154	2.15
4	10 266	0.84	191 164	15.71	4 101	0.34	462	0.04
5	387	0.03	60 585	4.98	16	0.00	0	0.00
6	6	0.00	8 918	0.73	0	0.00	0	0.00
7	0	0.00	431	0.04	0	0.00	0	0.00
8	0	0.00	2	0.00	0	0.00	0	0.00

Table 6 Elliptic curves $E/\mathbf{Q}$ with $E[5] \simeq \mu_5 \times \mathbf{Z}/5\mathbf{Z}$

	r_α		r_β		$\min\{r_\alpha, r_\beta\}$		r_5	
0	84 598	13.91	102	0.02	84 698	13.92	219 047	36.00
1	191 544	31.48	1 128	0.19	192 107	31.58	292 742	48.12
2	174 895	28.75	5 804	0.95	175 815	28.90	84 272	13.85
3	98 506	16.19	19 049	3.13	98 832	16.25	10 943	1.80
4	42 040	6.91	46 730	7.68	41 436	6.81	1 285	0.21
5	13 284	2.18	87 395	14.37	12 524	2.06	93	0.02
6	3 029	0.50	124 089	20.40	2 634	0.43	1	0.00
7	442	0.07	130 931	21.52	314	0.05	0	0.00
8	43	0.01	102 667	16.88	22	0.00	0	0.00
9	2	0.00	58 348	9.59	1	0.00	0	0.00
10	0	0.00	23 838	3.92	0	0.00	0	0.00
11	0	0.00	6 764	1.11	0	0.00	0	0.00
12	0	0.00	1 362	0.22	0	0.00	0	0.00
13	0	0.00	162	0.03	0	0.00	0	0.00
14	0	0.00	13	0.00	0	0.00	0	0.00
15	0	0.00	1	0.00	0	0.00	0	0.00

REFERENCES

[BBBCO] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, `pari/gp`, a computer algebra package, `http://www.parigp-home.de`

[Be] C.D. Beaver, 5-torsion in the Shafarevich-Tate group of a family of elliptic curves, *J. Number Theory* **82** (2000), 25–46.

[Bö] R. Bölling, Die Ordnung der Schafarewitsch-Tate-Gruppe kann beliebig gross werden, *Math. Nachr.* **67** (1975), 157–179.

[CaI] J.W.S. Cassels, Arithmetic on curves of genus 1, I. On a conjecture of Selmer, *J. Reine Angew. Math.* **202** (1959), 52–99.

[CaIV] J.W.S. Cassels, Arithmetic on curves of genus 1, IV. Proof of the Hauptvermutung, *J. Reine Angew. Math.* **211** (1962), 95–112.

[CaVI] J.W.S. Cassels, Arithmetic on curves of genus 1, VI. The Tate-Šafarevič group can be arbitrarily large, *J. Reine Angew. Math.* **214/215** (1964), 65–70.

[CaVIII] J.W S. Cassels, Arithmetic on curves of genus 1, VIII. On conjectures of Birch and Swinnerton-Dyer, *J. Reine Angew. Math.* **217** (1965), 180–199.

[Ca91] J.W.S. Cassels, *Lectures on elliptic curves*, LMSST **24**, Cambridge University Press, Cambridge, 1991.

[Ca98] J.W.S. Cassels, Second descents for elliptic curves, *J. Reine Angew. Math.* **494** (1998), 101–127.

[CF] J.W.S. Cassels and A. Fröhlich (Eds.), *Algebraic number theory*, Academic Press, London, 1967.

[CS] J. Coates and R. Sujatha, *Galois cohomology of elliptic curves*, TIFR Lect. on Math. **88**, Narosa, New Delhi, 2000.

[CSS] J.-L. Colliot-Thélène, A.N. Skorobogatov, H.P.F. Swinnerton-Dyer, Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points, *Invent. Math.* **134** (1998) 579–650.

[Co] I. Connell, Calculating root numbers of elliptic curves over **Q**, *Manuscripta Math.* **82** (1994), 93–104.

[Cr1] J.E. Cremona, *Algorithms for modular elliptic curves*, Second edition, Cambridge University Press, Cambridge, 1997.

[Cr2] J.E. Cremona, Modular elliptic curve data for conductors up to 10^4. `http://www.maths.nottingham.ac.uk/personal/jec/ftp/data`

[F0] T.A. Fisher, *On 5 and 7 descents for elliptic curves*, PhD thesis, Cambridge University, 2000.

[F1] T.A. Fisher, Some examples of 5 and 7 descent for elliptic curves over **Q**, *J. Eur. Math. Soc.* **3** (2001), 169–201.

[H] K. Hulek, Projective geometry of elliptic curves, *Astérisque* **137** (1986).

[Kl] R. Kloosterman, *Elliptic curves with large Selmer groups*, Master's thesis, University of Groningen, 2001.

[Kr] K. Kramer, A family of semistable elliptic curves with large Tate-Shafarevich groups, *Proc. Amer. Math. Soc.* **89** (1983), 379–386.

[L] F. Lemmermeyer, On Tate-Shafarevich groups of some elliptic curves, *Algebraic number theory and Diophantine analysis*, de Gruyter, Berlin, 2000.

[McC] W.G. McCallum, On the Shafarevich-Tate group of the Jacobian of a quotient of the Fermat curve, *Invent. Math.* **93** (1988), 637–666.

[McG] F.O. McGuinness, *The Cassels pairing in a family of elliptic curves*, Ph.D. Dissertation, Brown University, 1982.

[Mi] J.S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics **1**, Academic Press, Boston, 1986.

[Mo] P. Monsky, Generalizing the Birch-Stephens theorem, I. Modular curves, *Math. Z.* **221** (1996), 415–420.

[PS] B. Poonen and M. Stoll, The Cassels-Tate pairing on polarized abelian varieties, *Ann. of Math.* **150** (1999), 1109–1149.

[R] D.E. Rohrlich, Variation of the root number in families of elliptic curves, *Compositio Math.* **87** (1993), 119–151.

[Sc1] E.F. Schaefer, Class groups and Selmer groups, *J. Number Theory* **56** (1996), 79–114.

[Sc2] E.F. Schaefer, Can the 5-part of the Shafarevich-Tate group of an elliptic curve get arbitrarily large?
`http://math.scu.edu/~eschaefe/nt.html`

[Se1] J.-P. Serre, *Local fields*, GTM **67**, Springer-Verlag, New York-Berlin, 1979.

[Se2] J.-P. Serre, *Galois cohomology*, Springer-Verlag, Berlin, 1997.

[Si1] J.H. Silverman, *The arithmetic of elliptic curves*, GTM **106**, Springer-Verlag, New York, 1986.

[Si2] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, GTM **151**, Springer-Verlag, New York, 1994.

[T1] J. Tate, WC-groups over $\mathfrak{p}$-adic fields, *Séminaire Bourbaki*, Exposé **156**, Paris, 1958.

[T2] J. Tate, Duality theorems in Galois cohomology over number fields, *Proc. Internat. Congr. Mathematicians*, Stockholm 1962, 288–295.

[V] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris*, Sér. A-B **273** (1971), A238–A241.

[W] T. Womack, `bg.gp`, An implementation of the Buhler-Gross algorithm for computing L-series derivatives. Repaired and improved by J.E. Cremona. `tom@womack.net`