J. Eur. Math. Soc. 3, 169–201 (2001)

Digital Object Identifier (DOI) 10.1007/s100970100030

Tom Fisher

Some examples of 5 and 7 descent for elliptic curves over Q

Received October 6, 2000 / final version received November 14, 2000
Published online February 15, 2001 – © Springer-Verlag & EMS 2001

Abstract. We perform descent calculations for the families of elliptic curves over **Q** with a rational point of order $n = 5$ or 7. These calculations give an estimate for the Mordell-Weil rank which we relate to the parity conjecture. We exhibit explicit elements of the Tate-Shafarevich group of order 5 and 7, and show that the 5-torsion of the Tate-Shafarevich group of an elliptic curve over **Q** may become arbitrarily large.

Introduction

Let E be an elliptic curve over a number field K. The Mordell-Weil theorem asserts that the group $E(K)$ of K-rational points on E is a finitely generated abelian group. We call $E(K)$ the Mordell-Weil group. Another important group associated to E is the Tate-Shafarevich group $\text{Ш}(E/K)$. It is defined as the set of torsors under E which have points everywhere locally. Thus a non-zero element of the Tate-Shafarevich group corresponds to a smooth curve of genus 1 that violates the Hasse Principle, *i.e.* it has (local) K_v-rational points at all places v, but no (global) K-rational points. It is known that $\text{Ш}(E/K)$ is torsion, and that the torsor corresponding to an element of order n admits a divisor class of degree n defined over K. On a curve of genus 1 a complete linear system of degree n also has dimension n. Thus for $n = 2$ we consider double covers of $\mathbf{P}^1$, for $n = 3$ plane cubics, for $n = 4$ complete intersections of two quadrics in $\mathbf{P}^3$, and so on.

There is no known algorithm guaranteed to compute the Mordell-Weil group, and the situation for the Tate-Shafarevich group is no better. However, for any integer $n \geq 2$ the proof of the Mordell-Weil theorem gives an effective upper bound on the order of $E(K)/nE(K)$. This yields an upper bound on the Mordell-Weil rank which is an overestimate precisely whenever $\text{Ш}(E/K)$ contains non-trivial n-torsion. Such calculations are referred to as descent calculations. By performing an n-descent we obtain partial information concerning the groups $E(K)$ and $\text{Ш}(E/K)$. It is therefore of interest to make descent calculations practical for as many different values of n as possible.

A great deal of work has been done on 2- and 3-descents, the advantage of n being small outweighing the fact that the primes 2 and 3 often require special

T. Fisher: University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK

treatment in the study of elliptic curves. We give some examples of 5- and 7-descents. Unfortunately we work in a special case, so our results do not apply to an arbitrary elliptic curve. Firstly, our descent calculations assume the existence of an isogeny of degree $n = 5$ or 7. Secondly, we assume one of our pair of elliptic curves has a rational point of order n. Notice that by a result of Serre [Se1], the second condition is automatically satisfied if we restrict to semi-stable elliptic curves. Here we recall a curve is semi-stable if it has good or multiplicative reduction at all primes.

Accordingly we consider pairs of elliptic curves C and D defined over K, related by the exact sequences of Galois modules

$$0 \to \boldsymbol{\mu}_n \to C \overset{\phi}{\to} D \to 0 \quad \text{and} \quad 0 \to \mathbf{Z}/n\mathbf{Z} \to D \overset{\widehat{\phi}}{\to} C \to 0. \qquad (1)$$

In other words $\phi : C \to D$ is an isogeny of degree n with kernel a labelled copy of $\boldsymbol{\mu}_n$ inside C. The Weil pairing tells us that the dual isogeny $\widehat{\phi} : D \to C$ has kernel a labelled copy of $\mathbf{Z}/n\mathbf{Z}$ inside D. We estimate the Mordell-Weil rank by bounding the groups $D(K)/\phi C(K)$ and $C(K)/\widehat{\phi} D(K)$. This process is known as descent via n-isogeny. In many cases it enables us to compute the n-torsion of the Tate-Shafarevich groups $Ш(C/K)$ and $Ш(D/K)$.

Selmer wrote down the following example of a plane cubic which violates the Hasse principle.

$$T = \left\{3x_0^3 + 4x_1^3 + 5x_2^3 = 0\right\} \subset \mathbf{P}^2.$$

As explained in [Ca3], T corresponds to an element of order 3 in $Ш(C/\mathbf{Q})$ where the Jacobian C has equation $x_0^3 + x_1^3 + 60x_2^3 = 0$. There is an action of $\boldsymbol{\mu}_3$ on T given by $x_i \mapsto \zeta_3^i x_i$. The quotient is the elliptic curve D with Weierstrass equation

$$y^2 = x^3 + 30^2.$$

A 2-descent shows $D(\mathbf{Q}) \cong \mathbf{Z}/3\mathbf{Z}$. Writing down explicit equations for the quotient map it is then easy to check $T(\mathbf{Q}) = \emptyset$.

We now give an example of an element of order 5 in the Tate-Shafarevich group.

$$T = \left\{ \begin{array}{r} x_0^2 + x_1x_4 - 6x_2x_3 = 0 \\ x_1^2 + x_0x_2 - 15x_3x_4 = 0 \\ 2x_2^2 + x_1x_3 - 5x_0x_4 = 0 \\ 3x_3^2 + x_2x_4 - x_0x_1 = 0 \\ 5x_4^2 + x_0x_3 - 2x_1x_2 = 0 \end{array} \right\} \subset \mathbf{P}^4.$$

To show T has points everywhere locally it suffices to consider the primes $p = 2, 3, 5, 569$, at all other primes the reduction being a smooth curve of genus 1. For $p = 2, 3, 5$ the reduction is a rational nodal curve of degree 5 and again local solubility is clear. Finally T meets the hyperplane $\{x_4 = 0\}$ in a point defined over $\mathbf{Q}(\sqrt[5]{12})$ and $p = 569$ splits in this field. To show T has no $\mathbf{Q}$-rational points we quotient out by the action of $\boldsymbol{\mu}_5$ on T given by $x_i \mapsto \zeta_5^i x_i$. The quotient is an elliptic curve D with Weierstrass equation

$$y^2 - 29xy - 30y = x^3 - 30x^2.$$

A 2-descent, courtesy of Cremona's program `mwrank`, shows $D(\mathbf{Q}) \cong \mathbf{Z}/5\mathbf{Z}$. It is then easy to check $T(\mathbf{Q}) = \emptyset$.

The curve T corresponds to an element of order 5 in $\text{Ш}(C/\mathbf{Q})$ where the Jacobian C is related to D by the exact sequences (1). In our example C and D have conductor $N = 17070$. We perform similar calculations for all pairs of elliptic curves C and D appearing in Cremona's tables [Cr3] of elliptic curves of conductor $N \leq 5300$. We find the following examples of curves C with $\text{Ш}(C/\mathbf{Q})[5] \cong (\mathbf{Z}/5\mathbf{Z})^2$

570L3, 570L4, 870I3, 870I4, 1050O2, 1342C3, 1938J2, 1950Y2, 2370M2, 2550EE2, 3270H2.

We are able to treat the case $n = 7$ in the same explicit manner, and find the following examples of curves C with $\text{Ш}(C/\mathbf{Q})[7] \cong (\mathbf{Z}/7\mathbf{Z})^2$

546F2, 858K2, 1230K2, 5010H2.

It is pleasing to note that, with one exception, we have recovered Cremona's list of all curves of conductor $N \leq 1000$ and Ш of analytic order n^2. The exceptional curve 275B3, with Ш of analytic order 25, is the 5-twist of one of our curves C. We are also able to exhibit examples of non-trivial Ш for elliptic curves with positive Mordell-Weil rank.

Let us make two remarks that may help the reader. Firstly, as the title of this article indicates, we often treat the cases $n = 5$ and $n = 7$ concurrently. It then becomes necessary, when giving formulae, to split into these two cases. At times we tire of reminding the reader that these are the cases $n = 5$ and $n = 7$. It is hoped that this will cause no confusion.

Secondly, we encounter many calculations that are straightforward to check with the aid of any computer algebra package, but which would be rather laborious to check by hand. The reader should either take these results on trust, or reach for his own computer. Whenever our computer calculations extend beyond these menial algebraic manipulations, we give explicit mention of the fact. For example in Sect. 1.4 we use Cremona's program `mwrank` which computes ranks of elliptic curves over **Q** via 2-descent.

1. Descent calculations

1.1. Weierstrass equations and reduction types

Let K be a number field and $n \geq 4$ an integer. We consider pairs of n-isogenous elliptic curves C and D over K. We assume $\phi : C \to D$ has kernel a labelled copy of $\boldsymbol{\mu}_n$ and $\widehat{\phi} : D \to C$ has kernel a labelled copy of $\mathbf{Z}/n\mathbf{Z}$. The pairs of such curves C and D are parametrised by the modular curve $Y_1(n)$. For n prime, $X_1(n)$ has $n-1$ cusps, of which half are defined over $\mathbf{Q}$ and half are defined over $\mathbf{Q}(\boldsymbol{\mu}_n) \cap \mathbf{R}$.

Our interest is in the cases $n = 5$ and $n = 7$ when $X_1(n) \cong \mathbf{P}^1$. We shall shortly specify a co-ordinate λ on $X_1(n)$ and write C_λ and D_λ for the pair of n-isogenous elliptic curves above λ.

Lemma 1.1. *Let E/K be an elliptic curve and $P \in E(K)$ a point of order at least 4.*

(i) E has a Weierstrass equation $y^2 + uxy + vy = x^3 + vx^2$ with $P = (0, 0)$.
(ii) The pair (E, P) uniquely determines $(u, v) \in \mathbf{A}^2(K)$.
(iii) The pair (E, P) has no automorphisms.

Proof. [Si1, Exercise 8.13] or [Si2, Exercise 3.1]. □

We now compute $mP = (x_m(u, v), y_m(u, v))$ for small integers m. Equating some of these expressions we quickly write down some affine curves whose smooth projective model is $X_1(n)$. In the cases $n = 5$ and $n = 7$ we find D_λ has Weierstrass equation

$$\begin{array}{lc} n=5 & y^2 + (1-\lambda)xy - \lambda y = x^3 - \lambda x^2 \\ n=7 & y^2 + (1+\lambda-\lambda^2)xy + (\lambda^2-\lambda^3)y = x^3 + (\lambda^2-\lambda^3)x^2. \end{array} \tag{2}$$

Computing the discriminant we find the cusps of $X_1(n)$.

$n = 5$ Rational cusps at $\lambda = 0, \infty$.
Irrational cusps at the roots of $\lambda^2 - 11\lambda - 1 = 0$.

$n = 7$ Rational cusps at $\lambda = 0, 1, \infty$.
Irrational cusps at the roots of $\lambda^3 - 8\lambda^2 + 5\lambda + 1 = 0$.

The automorphisms of $Y_1(n)$ are precisely the automorphisms of $\mathbf{P}^1$ that map cusps to cusps. There are $(n-1)/2$ automorphisms preserving the rational cusps. These correspond to relabelling our copy of $\boldsymbol{\mu}_n \hookrightarrow C$ respectively $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D$. In addition there is an involution η that swaps over the rational cusps with the irrational cusps. We find η is defined over $\mathbf{Q}(\boldsymbol{\mu}_n) \cap \mathbf{R}$ and $\boldsymbol{\mu}_n \hookrightarrow C_\lambda$ is isomorphic to $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_{\eta(\lambda)}$ over $\mathbf{Q}(\boldsymbol{\mu}_n)$. Since there is no canonical choice of isomorphism $\boldsymbol{\mu}_n \cong \mathbf{Z}/n\mathbf{Z}$ there is no canonical choice of involution η. As far as possible we shall avoid making such a choice.

Remark 1.2. The proof of Lemma 1.1 involves writing down a Weierstrass equation and then making substitutions of the form

$$x \mapsto \pi^2 x + r, \quad y \mapsto \pi^3 y + \pi^2 sx + t.$$

By this method we may easily check that for $n = 5$, $(D_\lambda, 2P) \cong (D_{-1/\lambda}, P)$, and for $n = 7$, $(D_\lambda, 2P) \cong (D_{(\lambda-1)/\lambda}, P)$.

Vélu's formulae [V] tell us that C_λ has Weierstrass equation

$$\begin{array}{c} y^2 + (1-\lambda)xy - \lambda y = x^3 - \lambda x^2 - 5tx - b_2 t - 7w \\ y^2 + (1+\lambda-\lambda^2)xy + (\lambda^2-\lambda^3)y = x^3 + (\lambda^2-\lambda^3)x^2 - 5tx - b_2 t - 7w \end{array} \tag{3}$$

where

$$n = 5 \quad \begin{cases} b_2 = \lambda^2 - 6\lambda + 1 \\ t \ = \lambda(\lambda^2 + 2\lambda - 1) \\ w = \lambda^2(2\lambda^2 + \lambda + 1) \end{cases}$$

$$n = 7 \quad \begin{cases} b_2 = \lambda^4 - 6\lambda^3 + 3\lambda^2 + 2\lambda + 1 \\ t \ = \lambda(\lambda - 1)(\lambda^2 - \lambda + 1)(\lambda^3 + 2\lambda^2 - 5\lambda + 1) \\ w = \lambda^2(\lambda - 1)^2(2\lambda^6 - 2\lambda^5 + \lambda^4 - 8\lambda^3 + 15\lambda^2 - 9\lambda + 2). \end{cases}$$

The Weierstrass equations (2) and (3) have discriminant

$$n = 5 \qquad \begin{aligned} \Delta(C_\lambda) &= \lambda(\lambda^2 - 11\lambda - 1)^5 \\ \Delta(D_\lambda) &= \lambda^5(\lambda^2 - 11\lambda - 1) \end{aligned} \tag{4}$$

$$n = 7 \qquad \begin{aligned} \Delta(C_\lambda) &= \lambda(\lambda - 1)(\lambda^3 - 8\lambda^2 + 5\lambda + 1)^7 \\ \Delta(D_\lambda) &= \lambda^7(\lambda - 1)^7(\lambda^3 - 8\lambda^2 + 5\lambda + 1). \end{aligned} \tag{5}$$

Although our descent calculations shall make remarkably little explicit use of the reduction types for C_λ and D_λ, it is good culture to describe them now. We recall that isogenous elliptic curves always have the same reduction type. Applying Tate's algorithm, as described in [Si2] for example, we find

Lemma 1.3. *Let $\mathfrak{p}$ be a prime of K with $\mathfrak{p} \nmid n$. For $\lambda \in K_{\mathfrak{p}}$ with $\operatorname{ord}_{\mathfrak{p}}(\lambda) \geq 0$ the Weierstrass equations (2) and (3) are minimal and the reduction types are as follows.*
(i) If λ reduces to a rational cusp, i.e. $\lambda \equiv 0 \pmod{\mathfrak{p}}$, respectively $\lambda(\lambda - 1) \equiv 0 \pmod{\mathfrak{p}}$, then C_λ and D_λ have split multiplicative reduction.
(ii) If λ reduces to an irrational cusp, i.e. $\lambda^2 - 11\lambda - 1 \equiv 0 \pmod{\mathfrak{p}}$, respectively $\lambda^3 - 8\lambda^2 + 5\lambda + 1 \equiv 0 \pmod{\mathfrak{p}}$, then C_λ and D_λ have multiplicative reduction and the reduction is split if and only if $\operatorname{Norm}\mathfrak{p} \equiv 1 \pmod{n}$.
(iii) In the remaining cases C_λ and D_λ have good reduction.

The assumption $\operatorname{ord}_{\mathfrak{p}}(\lambda) \geq 0$ here is no loss since we are always free to replace λ by $-1/\lambda$, respectively $(\lambda - 1)/\lambda$. It remains to describe the reduction types for $\mathfrak{p}|n$. We find that cases (i) and (iii) go through as before. However if λ reduces to an irrational cusp it seems no longer possible to treat all number fields at once. If $K = \mathbf{Q}$ the Weierstrass equation (2) is still minimal and the reduction is additive. However, in this case the Weierstrass equation (3) need not be minimal, specifically if $\lambda \equiv 18 \pmod{25}$, respectively $\lambda \equiv 5 \pmod{7}$.

1.2. Selmer groups and torsors

Let E be an elliptic curve over a number field K. Let T/K be a smooth curve of genus 1. We say that T has the structure of *torsor* under E if there is a simple transitive action $E \times T \to T$ defined over K. Since T has $\overline{K}$-rational points, it is clear that T is a twist of E. It is a general principle that the twists of an object X are parametrised by $H^1(K, \operatorname{Aut}(X)) := H^1(\operatorname{Gal}(\overline{K}/K), \operatorname{Aut}(X))$.

Writing τ_P for translation by $P \in E$ there is an exact sequence

$$0 \to \{\text{translations } \tau_P\} \to \operatorname{Aut}(E) \to \operatorname{Aut}(E, 0) \to 0 \qquad (6)$$

where $\operatorname{Aut}(E)$ and $\operatorname{Aut}(E, 0)$ are the automorphism groups of E as a curve and as a group variety respectively. The translations are the automorphisms of E as a torsor under itself. Thus the torsors under E are parametrised by the Weil-Châtelet group $\mathrm{WC}(E/K) := H^1(K, E)$. Concretely, T is a torsor under E if and only if there exists $\psi : T \xrightarrow{\sim} E$ an isomorphism over $\overline{K}$ such that the cocycle $\sigma \mapsto \sigma(\psi)\psi^{-1}$ takes values in the translation subgroup of $\operatorname{Aut}(E)$. We remark that in this situation the curve T uniquely determines the curve E. In fact E is the Jacobian of T.

We write $\xi_T \in \mathrm{WC}(E/K)$ for the cohomology class determined by the torsor T/K. It is clear $T(K) \neq \emptyset$ if and only if $\xi_T = 0$. Thus the Tate-Shafarevich group

$$Ш(E/K) := \ker\big(\mathrm{WC}(E/K) \to \textstyle\prod_v \mathrm{WC}(E/K_v)\big)$$

measures the failure of the Hasse Principle for torsors T under E.

We now take $\lambda \in K$, not a cusp of $X_1(n)$, and consider the elliptic curves C_λ and D_λ introduced in Sect. 1.1. There is an exact sequence of Galois modules

$$0 \to \boldsymbol{\mu}_n \to C_\lambda \to D_\lambda \to 0.$$

Taking Galois cohomology yields

$$0 \to D_\lambda(K)/\phi C_\lambda(K) \xrightarrow{\delta} H^1(K, \boldsymbol{\mu}_n) \to \mathrm{WC}(C_\lambda/K)[\phi] \to 0 \qquad (7)$$

and by Hilbert's Theorem 90 we identify $H^1(K, \boldsymbol{\mu}_n) = K^\times/(K^\times)^n$. We write $C_{\lambda,\theta}$ for the torsor under C_λ described by $\theta \in K^\times/(K^\times)^n$. The Selmer group attached to the isogeny ϕ is defined by

$$S^{(\phi)}(C_\lambda/K) = \{\, \theta \in K^\times/(K^\times)^n \mid C_{\lambda,\theta}(K_{\mathfrak{p}}) \neq \emptyset \text{ for all primes } \mathfrak{p} \,\}. \qquad (8)$$

Notice that, since n is odd, we are able to ignore the infinite places. We give equations for the curves $C_{\lambda,\theta}$ via two different methods, which we refer to as the *push-out method* and the *projective space method.*

Equations via Push-Out. Let C_λ and D_λ be as above and write $\mathbf{1}$ for the generator of $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda(K)$. We label our copy of $\boldsymbol{\mu}_n \hookrightarrow C_\lambda$ such that $e_\phi(\zeta, \mathbf{1}) = \zeta$ for all $\zeta \in \boldsymbol{\mu}_n$. Here e_ϕ is the Weil pairing as defined in [Si1, Exercise 3.15].

Lemma 1.4. *Let $f \in K(D_\lambda)$ have divisor $(f) = n.\mathbf{1} - n.0$ and be scaled, up to nth powers, such that $f \circ \phi = g^n$ for some $g \in K(C_\lambda)$. Then the map δ in*

$$0 \to \boldsymbol{\mu}_n(K) \to C_\lambda(K) \xrightarrow{\phi} D_\lambda(K) \xrightarrow{\delta} K^\times/(K^\times)^n$$

is given by $\delta(P) = f(P) \mod (K^\times)^n$, for $P \neq 0, \mathbf{1}$.

Proof. Pick $P' \in C_\lambda$ with $\phi(P') = P$. For $\sigma \in G_K := \mathrm{Gal}(\overline{K}/K)$ we compute

$$\begin{aligned} \sigma(P') - P' &= e_\phi(\sigma(P') - P', \mathbf{1}) \\ &= g(X + \sigma(P') - P')/g(X) \qquad \text{for any } X \in C_\lambda \\ &= \sigma(g(P'))/g(P'). \end{aligned}$$

Thus $\delta(P) = g(P')^n = f{\circ}\phi(P') = f(P) \mod (K^\times)^n$. □

Taking D_λ with Weierstrass equation (2) and $\mathbf{1} = (0, 0)$ we claim that the rational function $f \in K(D_\lambda)$ is given by

$$\begin{aligned} n &= 5 \quad f(x, y) = xy + y - x^2 \\ n &= 7 \quad f(x, y) = (\lambda + 1)x^3 - x^2y + \lambda^2x^2 - (2\lambda + 1)xy - \lambda^2 y. \end{aligned} \tag{9}$$

Indeed on the affine piece of D_λ described, f only vanishes at $\mathbf{1} = (0, 0)$, as is seen by computing some resultants. It follows that f has the correct divisor. Since δ is a homomorphism it is easy to check that f is correctly scaled. To this end we compute f on the torsion $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda(K)$.

	x	y	f
2	λ	λ^2	λ^3
3	λ	0	$-\lambda^2$
4	0	λ	λ

	x	y	f
2	$\lambda^2(\lambda - 1)$	$\lambda^3(\lambda - 1)^2$	$-\lambda^6(\lambda - 1)^5$
3	$\lambda(\lambda - 1)$	$\lambda(\lambda - 1)^2$	$\lambda^2(\lambda - 1)^4$
4	$\lambda(\lambda - 1)$	$\lambda^2(\lambda - 1)^2$	$-\lambda^5(\lambda - 1)^3$
5	$\lambda^2(\lambda - 1)$	0	$\lambda^8(\lambda - 1)^2$
6	0	$\lambda^2(\lambda - 1)$	$-\lambda^4(\lambda - 1)$

Thus $C_{\lambda,\theta}$ has affine model

$$\left\{ \begin{array}{c} f(x, y) = \theta z^n \\ (x, y) \in D_\lambda \end{array} \right\} \subset \mathbf{A}^2 \times \mathbf{G}_m. \tag{10}$$

Equations in Projective Space. We recall [Si1, Chapter III] that for D a divisor on the elliptic curve E

$$D \sim 0 \iff \deg D = 0 \text{ and } \operatorname{sum} D = 0. \tag{11}$$

Thus if we embed $E \hookrightarrow \mathbf{P}^{n-1}$ by means of a complete linear system of degree n then the translation map τ_P lifts to an automorphism of $\mathbf{P}^{n-1}$ if and only if $P \in E[n]$.

Now take $T \hookrightarrow \mathbf{P}^{n-1}$ a smooth curve of genus 1 and degree n. In this situation we always take it as read that T is embedded via a complete linear system. It is equivalent to demand that T is contained in no hyperplane. We claim that the action of $\mathrm{Jac}(T)$ on T determines an inclusion of G_K-modules $\mathrm{Jac}(T)[n] \hookrightarrow \mathrm{PGL}_n$. Indeed, from a geometric point of view this situation is no different from that described in the last paragraph.

Suppose given T a torsor under C_λ with $\xi_T \in \mathrm{WC}(C_\lambda/K)[\phi]$. We know $\boldsymbol{\mu}_n \hookrightarrow C_\lambda$ acts on T with quotient U a torsor under D_λ. Then

$$\phi : \mathrm{WC}(C_\lambda/K) \to \mathrm{WC}(D_\lambda/K);\ \ \xi_T \mapsto \xi_U = 0.$$

Choosing a K-point on U gives a divisor of degree n on T and so an embedding $T \hookrightarrow \mathbf{P}^{n-1}$. As explained above, $\boldsymbol{\mu}_n \hookrightarrow C_\lambda$ lifts to an action on $\mathbf{P}^{n-1}$. Geometrically there are exactly n hyperplanes fixed under this action. They correspond to our original choice of K-point on U and its translates under $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda$. In particular these hyperplanes are defined over K, so for a suitable choice of co-ordinates on $\mathbf{P}^{n-1}$ the action $\boldsymbol{\mu}_n \hookrightarrow \mathrm{PGL}_n$ is given by

$$\zeta \mapsto \mathrm{Diag}(1 : \zeta : \ldots : \zeta^{n-1}). \tag{12}$$

Thus the torsors $C_{\lambda,\theta}$ all arise as smooth curves of genus 1, degree n in $\mathbf{P}^{n-1}$ invariant under (12). In Sect. 2.2 we shall give equations for all such curves. In the meantime, let us reverse the above argument to show that all the curves we obtain are of the form $C_{\lambda,\theta}$ for suitable λ and θ.

So let T be a smooth curve of genus 1, degree n in $\mathbf{P}^{n-1}$ invariant under the diagonal action of $\boldsymbol{\mu}_n$ given by (12). Since n is prime to 6 we know $\boldsymbol{\mu}_n \hookrightarrow \mathrm{Jac}(T)$ and so $\mathrm{Jac}(T) \cong C_\lambda$ for some $\lambda \in K$. Now T is a torsor under C_λ and $U := T/\boldsymbol{\mu}_n$ is a torsor under D_λ. But the intersection of T with one of the co-ordinate hyperplanes is an orbit under $\boldsymbol{\mu}_n$ globally defined over K. Thus U is trivial as a torsor under D_λ and $\xi_T \in \mathrm{WC}(C_\lambda/K)[\phi]$. From the exact sequence (7) it follows $T \cong C_{\lambda,\theta}$ for some $\theta \in K^\times/(K^\times)^n$.

Remark 1.5. The action (12) of $\boldsymbol{\mu}_n$ on $\mathbf{P}^{n-1}$ is the unique one that lifts to GL_n. By unique here we mean unique up to change of co-ordinates defined over K. In general the obstruction to lifting $\boldsymbol{\mu}_n \hookrightarrow \mathrm{PGL}_n$ to $\boldsymbol{\mu}_n \hookrightarrow \mathrm{GL}_n$ is given by $H^1(K, \mathbf{Z}/n\mathbf{Z})$.

Remark 1.6. The above arguments show that the torsors parametrised by $\mathrm{WC}(C/K)[\phi]$ may be embedded in $\mathbf{P}^{n-1}$. This is also known for the torsors parametrised by $Ш(C/K)[n]$, and we suspect the local assumptions here are essential. We refer to [CM] where it is explained how this result is a consequence of the Hasse Principle for Brauer-Severi varieties.

1.3. Statement of the descent theorem

Let $n = 5$ or 7 and let $\lambda \in \mathbf{Q}$ with $\lambda \neq 0$, respectively $\lambda \neq 0, 1$. We consider the elliptic curves C_λ and D_λ over $\mathbf{Q}$ defined by (3) and (2). In each case $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda$ is generated by $(x, y) = (0, 0)$ and the isogenous curve C_λ is defined as the quotient by this subgroup. We write $\phi : C_\lambda \to D_\lambda$ for the n-isogeny with $C[\phi] \cong \boldsymbol{\mu}_n$ and $D[\widehat{\phi}] \cong \mathbf{Z}/n\mathbf{Z}$. In this section we state our main results describing the Selmer groups $S^{(\phi)}(C_\lambda/\mathbf{Q})$ and $S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q})$.

To help us carry the cases $n = 5$ and $n = 7$ together we write $\alpha(\lambda)$ and $\beta(\lambda)$ for the polynomials

$$\alpha(\lambda) = \begin{cases} \lambda \\ \lambda^4(\lambda - 1) \end{cases} \qquad \beta(\lambda) = \begin{cases} \lambda^2 - 11\lambda - 1 \\ \lambda^3 - 8\lambda^2 + 5\lambda + 1. \end{cases}$$

The zeros of these polynomials are cusps of $X_1(n)$. We define disjoint sets of rational primes.

$$\mathcal{A} = \{\, p \text{ prime} \mid \operatorname{ord}_p(\lambda) < 0 \text{ or } \alpha(\lambda) \equiv 0 \pmod{p} \,\}$$

$$\mathcal{B} = \left\{ p \text{ prime} \;\middle|\; \begin{array}{l} \beta(\lambda) \equiv 0 \pmod{p} \text{ and } p \equiv 1 \pmod{n} \\ \quad \text{or} \quad p = n = 5 \text{ and } \lambda \equiv 18 \pmod{25} \\ \quad \text{or} \quad p = n = 7 \text{ and } \lambda \equiv 5 \pmod{7} \end{array} \right\}.$$

For $\mathcal{S}$ a set of rational primes, we write $[\mathcal{S}]$ for the subspace of $\mathbf{Q}^\times/(\mathbf{Q}^\times)^n$ generated by $\mathcal{S}$. For Ξ a pairing of $\mathbf{Z}/n\mathbf{Z}$-vector spaces we write $\ker_L(\Xi)$ and $\ker_R(\Xi)$ for the left and right kernels.

Theorem 1. *Let $n = 5$ or 7 and let $\lambda \in \mathbf{Q}$ with $\lambda \neq 0$, respectively $\lambda \neq 0, 1$. Let $\mathcal{A}$ and $\mathcal{B}$ be the disjoint sets of rational primes defined above. Then the Selmer group attached to the n-isogeny $\phi : C_\lambda \to D_\lambda$ is given by*

$$S^{(\phi)}(C_\lambda/\mathbf{Q}) \cong \left\{ \theta \in [\mathcal{A}] \middle| \theta \in \left(\mathbf{Q}_p^\times\right)^n \textit{ for all } p \in \mathcal{B} \right\}.$$

The contribution to $S^{(\phi)}(C_\lambda/\mathbf{Q})$ coming from $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda(\mathbf{Q})$ is generated by $\alpha(\lambda)$. Furthermore there is a pairing $\Xi : [\mathcal{A}] \times [\mathcal{B}] \to \mathbf{Z}/n\mathbf{Z}$ such that $S^{(\phi)}(C_\lambda/\mathbf{Q}) \cong \ker_L(\Xi)$ and $S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q}) \cong \ker_R(\Xi)$.

Remark 1.7. The pairing Ξ is straightforward to compute. For each prime $q \in \mathcal{B}$ we choose a non-trivial character $\chi_q : (\mathbf{Z}/q\mathbf{Z})^\times \to \mathbf{Z}/n\mathbf{Z}$, respectively $\chi_n : (\mathbf{Z}/n^2\mathbf{Z})^\times \to \mathbf{Z}/n\mathbf{Z}$. Then Ξ is represented by the matrix $(\chi_q(p))_{p \in \mathcal{A}, q \in \mathcal{B}}$.

Lemma 1.8. *For p a rational prime, the congruence $\beta(\lambda) \equiv 0 \pmod{p}$ is soluble if and only if $p = n$ or $p \equiv \pm 1 \pmod{n}$.*

Proof. Consider how p factors in $\mathbf{Q}(\boldsymbol{\mu}_n) \cap \mathbf{R}$. □

Remark 1.9. In view of the identities $\lambda^2 - 11\lambda - 1 = (\lambda + 7)(\lambda - 18) + 125$ and $\lambda^3 - 8\lambda^2 + 5\lambda + 1 = (\lambda + 2)(\lambda - 5)^2 - 49$, the condition for n to belong to $\mathcal{B}$ is $\beta(\lambda) \equiv 0 \pmod{125}$, respectively $\beta(\lambda) \equiv 0 \pmod{49}$. As seen in Sect. 1.1 this is also the condition for the Weierstrass equation (3) to no longer be minimal.

We sketch the proof of Theorem 1. The definition (8) reads

$$S^{(\phi)}(C_\lambda/\mathbf{Q}) = \left\{ \theta \in \mathbf{Q}^\times/(\mathbf{Q}^\times)^n \middle| C_{\lambda,\theta}(\mathbf{Q}_p) \neq \emptyset \text{ for all primes } p \right\}.$$

In Sect. 2.2 we give equations for the $C_{\lambda,\theta}$ as curves in $\mathbf{P}^{n-1}$. We then describe the geometry of the reductions mod p and so derive some simple criteria for the existence of local points. We find that $S^{(\phi)}(C_\lambda/\mathbf{Q})$ is the subspace of $[\mathcal{A}]$ consisting of nth powers modulo the primes in $\mathcal{B}$. To treat the dual isogeny $\widehat{\phi}$, the rough idea is that the involution η swaps over the sets of primes $\mathcal{A}$ and $\mathcal{B}$. Then $S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q})$ is the subspace of $[\mathcal{B}]$ consisting of nth powers modulo the primes in $\mathcal{A}$, and the existence of the pairing Ξ is nothing more than a statement of the nth power reciprocity law. To make these ideas precise it is natural to work over $K = \mathbf{Q}(\boldsymbol{\mu}_n)$. Since $[K : \mathbf{Q}] = n - 1$ is prime to n, there is no difficulty in descending back to $\mathbf{Q}$.

In this article we give a proof of Theorem 1 working entirely over $\mathbf{Q}$. In [F] we generalise Theorem 1 to $K = \mathbf{Q}(\boldsymbol{\mu}_n)$ and so give an alternative proof of the result over $\mathbf{Q}$ which is much closer to the above sketch.

We should mention that in the case $p = n$ the projective space method fails to give complete criteria for the existence of local points. Our solution is to revert to the push-out method and perform some further Hensel lemma calculations. It is these calculations which make it difficult to work over a general number field.

1.4. Initial examples

Let $n = 5$ or 7 and let $\lambda \in \mathbf{Q}$ with $\lambda \neq 0$, respectively $\lambda \neq 0, 1$. Theorem 1 gives us information about both the Mordell-Weil groups $C_\lambda(\mathbf{Q})$ and $D_\lambda(\mathbf{Q})$ and the Tate-Shafarevich groups $Ш(C_\lambda/\mathbf{Q})$ and $Ш(D_\lambda/\mathbf{Q})$. We now make this explicit. Following Mazur's classification of torsion groups for elliptic curves over $\mathbf{Q}$ we find

$$D_\lambda(\mathbf{Q})_{\text{tors}} \cong \begin{cases} \mathbf{Z}/5\mathbf{Z} \;\text{ or }\; \mathbf{Z}/10\mathbf{Z} & \text{if } n = 5 \\ \mathbf{Z}/7\mathbf{Z} & \text{if } n = 7. \end{cases}$$

Let $r = \operatorname{rank} C_\lambda(\mathbf{Q}) = \operatorname{rank} D_\lambda(\mathbf{Q})$ and $\iota = \dim_n C_\lambda(\mathbf{Q})[n]$. Then $\iota = 0$ unless $\alpha(\lambda) \in (\mathbf{Q}^\times)^n$ and this can only happen in the case $n = 5$. Now Theorem 1 together with the exact sequences

$$0 \to D_\lambda(\mathbf{Q})/\phi C_\lambda(\mathbf{Q}) \to S^{(\phi)}(C_\lambda/\mathbf{Q}) \to Ш(C_\lambda/\mathbf{Q})[\phi] \to 0$$
$$0 \to C_\lambda(\mathbf{Q})/\widehat{\phi} D_\lambda(\mathbf{Q}) \to S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q}) \to Ш(D_\lambda/\mathbf{Q})[\widehat{\phi}] \to 0$$

tells us $r = r_1 + r_2$ with $r_1, r_2 \geq 0$ and

$$|\mathcal{A}| - \operatorname{rank}(\Xi) = r_1 + 1 - \iota + \dim_n Ш(C_\lambda/\mathbf{Q})[\phi]$$
$$|\mathcal{B}| - \operatorname{rank}(\Xi) = r_2 + \iota + \dim_n Ш(D_\lambda/\mathbf{Q})[\widehat{\phi}].$$

Thus our upper bound for the Mordell-Weil rank is

$$|\mathcal{A}| + |\mathcal{B}| - 1 - 2\operatorname{rank}(\Xi). \tag{13}$$

In the following examples we make use of the trivial exact sequences

$$0 \to Ш(C_\lambda/\mathbf{Q})[\phi] \to Ш(C_\lambda/\mathbf{Q})[n] \xrightarrow{\phi} Ш(D_\lambda/\mathbf{Q})[\widehat{\phi}]$$
$$0 \to Ш(D_\lambda/\mathbf{Q})[\widehat{\phi}] \to Ш(D_\lambda/\mathbf{Q})[n] \xrightarrow{\widehat{\phi}} Ш(C_\lambda/\mathbf{Q})[\phi].$$

Example 1.10. Let $n = 5$ and $\lambda = 38$. Then $\mathcal{A} = \{2, 19\}$ and $\mathcal{B} = \{41\}$. Since $2^8 \not\equiv 1 \pmod{41}$ it is clear that Ξ has rank 1. By Theorem 1 we deduce $C_{38}(\mathbf{Q}) = 0$, $D_{38}(\mathbf{Q}) \cong \mathbf{Z}/5\mathbf{Z}$ and $Ш(C_{38}/\mathbf{Q})(5) = Ш(D_{38}/\mathbf{Q})(5) = 0$.

Example 1.11. Let $n = 7$ and $\lambda = 8$. Then $\mathcal{A} = \{2, 7\}$ and $\mathcal{B} = \emptyset$. A computer search yields the point of infinite order $(x, y) = (30, 198)$ on D_8. By Theorem 1 we deduce $C_8(\mathbf{Q}) \cong \mathbf{Z}$, $D_8(\mathbf{Q}) \cong \mathbf{Z}/7\mathbf{Z} \oplus \mathbf{Z}$ and $Ш(C_8/\mathbf{Q})(7) = Ш(D_8/\mathbf{Q})(7) = 0$.

We may use Theorem 1 together with Cremona's program `mwrank`, which performs a 2-descent, to exhibit some elements of the Tate-Shafarevich group. As explained in the introduction these elements are explicit in the sense that we are able to give equations in $\mathbf{P}^{n-1}$ for the corresponding curves of genus 1 that violate the Hasse principle.

Example 1.12. Let $n = 5$ and $\lambda = -60, -42, -30, 30, 60$ or 90. In all these examples we have $|\mathcal{A}| = 3$ and $\mathcal{B} = \emptyset$. According to `mwrank`, $\operatorname{rank} D_\lambda(\mathbf{Q}) = 0$. By Theorem 1 we deduce $\text{Ш}(C_\lambda/\mathbf{Q})[5] \cong (\mathbf{Z}/5\mathbf{Z})^2$.

Example 1.13. Let $n = 7$ and $\lambda = -6, -5, 6, 7, 10$ or 11. In all these examples $|\mathcal{A}| = 3$ and $\mathcal{B} = \emptyset$. According to `mwrank`, $\operatorname{rank} D_\lambda(\mathbf{Q}) = 0$. By Theorem 1 we deduce $\text{Ш}(C_\lambda/\mathbf{Q})[7] \cong (\mathbf{Z}/7\mathbf{Z})^2$.

As promised in the introduction, we give some examples of non-trivial Ш for elliptic curves with positive Mordell-Weil rank.

Example 1.14. Let $n = 5$ and $\lambda = \pm 30/7, \pm 35/6$ or $14/15$. In all these examples $\mathcal{A} = \{2, 3, 5, 7\}$ and $\mathcal{B} = \emptyset$. According to `mwrank`, $\operatorname{rank} D_\lambda(\mathbf{Q}) = 1$. By Theorem 1 we deduce $\text{Ш}(C_\lambda/\mathbf{Q})[5] \cong (\mathbf{Z}/5\mathbf{Z})^2$.

2. Geometric results

2.1. The geometry of elliptic normal curves

Let K be an algebraically closed field and $n \geq 3$ an integer. We assume $\operatorname{char}(K) \nmid n$ and fix $\zeta = \zeta_n$ a primitive nth root of unity. We make further restrictions on n in due course.

Definition 2.1. *(i) An* elliptic normal curve *of degree n is an elliptic curve $E \hookrightarrow \mathbf{P}^{n-1}$ of degree n contained in no hyperplane.*
(ii) A Néron polygon *of degree n is a collection of n lines $\ell_0, \ldots, \ell_{n-1}$ in $\mathbf{P}^{n-1}$, contained in no hyperplane and arranged such that ℓ_i meets ℓ_j if and only if $i - j \equiv \pm 1 \pmod{n}$.*

Lemma 2.2. *Let $E \hookrightarrow \mathbf{P}^{n-1}$ be either (i) an elliptic normal curve or (ii) a Néron polygon. Then E lies on $n(n-3)/2$ quadrics and for $n \geq 4$ these quadrics suffice to define E.*

Proof. (i) See [H, Chapter IV].
(ii) We move the n points of intersection to $(1 : 0 : 0 : \ldots)$, $(0 : 1 : 0 : \ldots), \ldots$ and the result is clear. □

The modular curve $Y(n) = X(n) \setminus \{\text{cusps}\}$ parametrises the triples (E, P, Q) where E is an elliptic curve and $P, Q \in E[n]$ satisfy $e_n(P, Q) = \zeta_n$. For future reference we note there is an action of $\boldsymbol{\mu}_n$ on $X(n)$ given by

$$\zeta_n : (E, P, Q) \mapsto (E, P, Q + P) \tag{14}$$

with quotient $X_1(n)$.

Proposition 2.3. *Let (E, P, Q) be as above. If we embed $E \hookrightarrow \mathbf{P}^{n-1}$ by means of a complete linear system, then we may choose co-ordinates on $\mathbf{P}^{n-1}$ such that the translation maps τ_P and τ_Q are given by*

$$M_P := \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta & 0 & \cdots & 0 \\ 0 & 0 & \zeta^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \zeta^{n-1} \end{pmatrix} \quad M_Q := \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

Proof. As explained in Sect. 1.2, τ_P and τ_Q lift to elements of $\mathrm{Aut}(\mathbf{P}^{n-1}) = \mathrm{PGL}_n$. Since no hyperplane may contain more than n points of E we deduce that M_P has distinct eigenvalues and that M_Q cyclically permutes the hyperplanes fixed by M_P. Thus we may choose co-ordinates on $\mathbf{P}^{n-1}$ such that M_P and M_Q are as given, at least if we replace ζ by ζ^r for some r prime to n. We observe that M_P and M_Q commute as elements of PGL_n, but do not commute when lifted to GL_n. In fact their commutator in GL_n gives one possible definition of the Weil pairing. It follows that $r = 1$ as required. □

Proposition 2.4. *Let $n \geq 3$ odd and let (E, P, Q) be as above. If we embed $E \hookrightarrow \mathbf{P}^{n-1}$ by means of a complete linear system $|D|$ with $[-1]^*D \sim D$ then there is a unique choice of co-ordinates on $\mathbf{P}^{n-1}$ such that τ_P, τ_Q and $[-1]$ are given by M_P, M_Q and*

$$[-1] := \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \end{pmatrix}.$$

Proof. We first choose co-ordinates as described in Proposition 2.3. Since the subgroup generated by M_P and M_Q is its own centraliser inside PGL_n our co-ordinates are uniquely determined up to the action of this subgroup. We require

$$[-1]M_P[-1] = M_P^{-1} \quad [-1]M_Q[-1] = M_Q^{-1} \quad \text{and} \quad [-1]^2 = I.$$

These commutator relations determine $[-1]$ up to multiplication by elements of $\langle M_P, M_Q \rangle$. Since n is odd, the n^2 possible matrices representing the map $[-1]$ form a single orbit under the action of $\langle M_P, M_Q \rangle$ via conjugation. Taking $[-1]$ as given now fixes our choice of co-ordinates. □

We restrict to $n \geq 5$ odd, so that E is defined by quadrics. For (E, P, Q) a triple as above, we embed $E \hookrightarrow \mathbf{P}^{n-1}$ via the linear system $|n.0|$ and choose co-ordinates as in Proposition 2.4. Then (E, P, Q) is uniquely determined by the co-ordinates of the point $0 \in \mathbf{P}^{n-1}$. Indeed, given the co-ordinates of this point, the action of M_P and M_Q allows us to write down n^2 points on E. But E is defined by quadrics. So by Bézout's theorem these n^2 points suffice to determine E. Thus the above procedure gives an embedding $X(n) \hookrightarrow \mathbf{P}^{n-1}$. We shall describe the image of this map in the cases $n = 5$ and 7.

We write $x_0, x_1, \dots, x_{n-1}$ for our co-ordinates on $\mathbf{P}^{n-1}$ and agree that all subscripts are to be read mod n. Our assumption n is odd tells us

$$n.0 \sim 0 + P + 2P + \ldots + (n-1)P. \tag{15}$$

Therefore 0 belongs to exactly one of the hyperplanes fixed by M_P. But 0 is fixed by $[-1]$ so we have either

$$\begin{array}{lll} & 0 = (0 : a_1 : a_2 : \ldots : a_2 : a_1) & (+) \\ \text{or} & 0 = (0 : a_1 : a_2 : \ldots : -a_2 : -a_1) & (-) \end{array}$$

for some $a_1, a_2, \dots, a_{(n-1)/2}$ non-zero. We consider the vector spaces

$$V := H^0\big(\mathbf{P}^{n-1}, \mathcal{I}_E(2)\big) \subset W := H^0(\mathbf{P}^{n-1}, \mathcal{O}(2)).$$

The action of M_P allows us to write these as direct sums $V = \oplus_i V_i$ and $W = \oplus_i W_i$ with $V_i \subset W_i = \langle x_i^2, x_{i-1}x_{i+1}, \dots \rangle$. Since n is odd we deduce via the action of M_Q that $\dim V_i = (n-3)/2$ and $\dim W_i = (n+1)/2$. The point 0 and its translates under M_Q impose some linear conditions on the coefficients of the quadrics in V_0. This leads us to rule out the case $(+)$ and to make the following definition.

Definition 2.5. *For $n \geq 5$ odd, let $A(n) \subset \mathbf{P}^{n-1}$ be the subscheme defined by $a_0 = 0$, $a_{n-i} = -a_i$ and*

$$\operatorname{rank}(a_{i-j}a_{i+j})_{i,j=0}^{n-1} \leq 2. \tag{16}$$

More precisely $A(n)$ is defined by the leading 4×4 *Pfaffians.*

The above construction shows $X(n) \subset A(n)$. In fact, for p a prime, it is a theorem of Vélu that $X(p) = A(p)$. In other words, the quartics (16) suffice to define $X(p)$. Since our interest is in the cases $n = 5$ and 7, there is no need to appeal to this general theorem.

Equations for $X(5)$. Let $0 = (0 : a : b : -b : -a)$. $A(5)$ is defined by

$$\operatorname{rank}\begin{pmatrix} 0 & -a^2 & -b^2 \\ a^2 & 0 & ab \\ b^2 & -ab & 0 \end{pmatrix} \leq 2.$$

Thus $X(5) = A(5)$ is a copy of $\mathbf{P}^1$ and $V = \oplus_i V_i$ is spanned by

$$abx_0^2 + b^2x_1x_4 - a^2x_2x_3 = 0 \tag{17}$$

and cyclic permutes. There are cusps of $X(5)$ at $(a : b) = (1 : 0), (0 : 1)$. We call these the rational cusps.

Equations for $X(7)$. Let $0 = (0 : a : b : -c : c : -b : -a)$. $A(7)$ is defined by

$$\operatorname{rank}\begin{pmatrix} 0 & -a^2 & -b^2 & -c^2 \\ a^2 & 0 & ac & -bc \\ b^2 & -ac & 0 & ab \\ c^2 & bc & -ab & 0 \end{pmatrix} \leq 2 \quad \Longleftrightarrow \quad a^3b + b^3c + c^3a = 0.$$

Thus $X(7) = A(7)$ is the Klein quartic [Kl] and $V = \oplus_i V_i$ is spanned by

$$\begin{array}{rl} abx_1x_6 + bcx_2x_5 + cax_3x_4 &= 0 \\ abx_0^2 \qquad\qquad + c^2x_2x_5 - b^2x_3x_4 &= 0 \\ bcx_0^2 - c^2x_1x_6 \qquad\qquad + a^2x_3x_4 &= 0 \\ cax_0^2 + b^2x_1x_6 - a^2x_2x_5 \qquad\qquad &= 0 \end{array} \tag{18}$$

and cyclic permutes. There are cusps of $X(7)$ at $(a : b : c) = (1 : 0 : 0)$, $(0 : 1 : 0)$, $(0 : 0 : 1)$. We call these the rational cusps.

Let $n = 5$ or 7. The equations (17) and (18) each define a family of curves $\mathcal{X}(n) \to X(n)$, whose fibres above $Y(n)$ are elliptic normal curves. Furthermore, there is an action of $\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z})$ on $X(n)$ given by relabelling torsion, and this extends to an action of $\mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z})$ on $\mathcal{X}(n)$. Directly from the equations we see that the fibres of $\mathcal{X}(n) \to X(n)$ above the rational cusps are Néron polygons. But the cusps form a single orbit under the action of $\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z})$, so the same is true at all the cusps.

One way to find the irrational cusps is by explicitly writing down the action of $\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z})$ on $X(n)$. We give an alternative method. We begin by computing the action (14) of $\boldsymbol{\mu}_n$ on $X(n)$,

$$n = 5 \quad (a : b) \mapsto (\zeta a : b), \qquad\qquad n = 7 \quad (a : b : c) \mapsto (\zeta^3 a : \zeta b : c). \tag{19}$$

Up to this action, the irrational cusps $(0 : a_1 : a_2 : \dots)$ satisfy

$$\operatorname{rank}(a_{i-j})_{i,j=0}^{n-1} \leq 2. \tag{20}$$

Indeed (20) may be viewed both as the condition for $(0 : a_1 : a_2 : \dots)$ and its translates under M_Q to be collinear, and as the condition for M_Q to fix a point on the fibre of $\mathcal{X}(n) \to X(n)$. Either of these conditions is sufficient to establish degeneration from an elliptic normal curve to a Néron polygon. Essentially by solving a second order recurrence relation, we find that the solutions to (20) with $a_0 = 0$ and $a_{n-i} = -a_i$ are

$$(0 : a_1 : a_2 : \dots) = (0 : \zeta - \zeta^{-1} : \zeta^2 - \zeta^{-2} : \dots) \tag{21}$$

for ζ a primitive nth root of unity. Finally (19) and (21) allow us to list the irrational cusps.

Case $n = 5$. The cusps are at $a/b = 0, \infty, \zeta^i\phi, \zeta^i\overline{\phi}$ where ϕ is the golden ratio and $\overline{\phi}$ is its conjugate. These points may be viewed, under stereographic projection, as the vertices of an icosahedron.

Case $n = 7$. The irrational cusps are at

$$(a : b : c) = (\zeta^{3i}(\zeta - \zeta^6) : \zeta^i(\zeta^2 - \zeta^5) : \zeta^4 - \zeta^3)$$

and its translates under $(a : b : c) \mapsto (c : a : b)$. Together with the rational cusps, these are the points of inflection of the Klein quartic [Kl].

2.2. *Equations for torsors in* $\mathbf{P}^{n-1}$

Let $n = 5$ or 7. As explained in Sect. 1.2 we aim to give explicit equations for the torsors $C_{\lambda,\theta}$ as curves in $\mathbf{P}^{n-1}$. We work over a perfect field K and until further notice assume $\operatorname{char}(K) \neq n$.

Let $T \hookrightarrow \mathbf{P}^{n-1}$ be a smooth curve of genus 1 and degree n which is invariant under the action $\boldsymbol{\mu}_n \hookrightarrow \operatorname{Aut}(\mathbf{P}^{n-1})$ given by

$$\zeta \mapsto \operatorname{Diag}(1 : \zeta : \ldots : \zeta^{n-1}). \tag{22}$$

We write $(x_0 : \ldots : x_{n-1})$ for our co-ordinates on $\mathbf{P}^{n-1}$ and agree that all subscripts are to be read mod n. The hyperplanes fixed by (22) are the co-ordinate hyperplanes $H_i := \{x_i = 0\}$. As explained in Sect. 1.2 the action of $\operatorname{Jac}(T)[n]$ on T lifts to $\mathbf{P}^{n-1}$. Since n is prime to 6 we know $\boldsymbol{\mu}_n \hookrightarrow \operatorname{Jac}(T)$ and so this action is generated by

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta & 0 & \cdots & 0 \\ 0 & 0 & \zeta^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \zeta^{n-1} \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 0 & \cdots & 0 & * \\ * & 0 & \cdots & 0 & 0 \\ 0 & * & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & * & 0 \end{pmatrix}$$

where $*$ denotes a non-zero element of $\overline{K}$. By Lemma 2.2 the curve T is defined by 5 quadrics, respectively 14 quadrics. The action of M_1 divides these quadrics up into n-eigenspaces, and the action of M_2 tells us that these eigenspaces all have the same dimension. Concretely

$$H^0\big(\mathbf{P}^{n-1}, \mathcal{I}_T(2)\big) = \oplus_i V_i \quad \text{with} \quad V_i \subset \langle x_i^2, x_{i-1}x_{i+1}, \ldots \rangle.$$

Lemma 2.6. *Let* $T \hookrightarrow \mathbf{P}^{n-1}$ *satisfy the above hypotheses.*
(i) The curve T *meets the hyperplanes* H_i *in a total of* n^2 *points.*
(ii) Every non-zero quadric containing T *has at least three non-zero terms.*

Proof. (i) Let $P \in T \cap H_0$. Then the translates of P under M_1 and M_2 give the required n^2 distinct points.
(ii) Suppose V_0 contains a quadric with exactly two non-zero terms. Then the n^2 points in (i) fail to be distinct. □

Definition 2.7. *Let $\lambda, \tau_0, \dots, \tau_{n-1} \in K$ satisfy $\alpha(\lambda) = \prod \tau_i \neq 0$. We define $T[\lambda; \tau_0, \dots, \tau_{n-1}]$ to be the subscheme of $\mathbf{P}^{n-1}$ with equations*

$$n = 5 \qquad \tau_0 x_0^2 + x_1 x_4 - \tau_2\tau_3 x_2 x_3 = 0 \quad \text{\& cyclic permutes}$$

$$n = 7 \left\{ \begin{aligned} \tau_0 x_0^2 + x_1 x_6 - (1/\lambda^2)\tau_2\tau_3\tau_4\tau_5 x_2 x_5 = 0 \\ \tau_0 x_0^2 + \lambda x_1 x_6 - (1/\lambda^3)\tau_2\tau_3^2\tau_4^2\tau_5 x_3 x_4 = 0 \end{aligned} \right. \quad \text{\& cyclic permutes.}$$

Proposition 2.8. *Every curve $T \hookrightarrow \mathbf{P}^{n-1}$ satisfying the above hypotheses is equal to $T[\lambda; \tau_0, \dots, \tau_{n-1}]$ for some $\lambda, \tau_0, \dots, \tau_{n-1} \in K$.*

Proof. (i) Case $n = 5$. Lemma 2.6(ii) tells us that T has equations

$$\tau_0 x_0^2 + x_1 x_4 + a_0 x_2 x_3 = 0 \qquad \text{\& cyclic permutes}$$

for some non-zero constants $\tau_i, a_i \in K$. By Lemma 2.6(i) we may choose $(0 : z_1 : z_2 : z_3 : z_4) \in T \cap H_0$ with all $z_i \neq 0$. Then

$$\left. \begin{aligned} z_1 z_4 + a_0 z_2 z_3 &= 0 \\ \tau_2 z_2^2 + z_1 z_3 &= 0 \\ \tau_3 z_3^2 + z_2 z_4 &= 0 \end{aligned} \right\} \implies a_0 = -\tau_2\tau_3.$$

By symmetry this completes the proof in the case $n = 5$.
(ii) Case $n = 7$. Lemma 2.6(ii) tells us that T has equations

$$\begin{aligned} \tau_0 x_0^2 + x_1 x_6 + a_0 x_2 x_5 = 0 \\ \tau_0 x_0^2 + \lambda_0 x_1 x_6 + b_0 x_3 x_4 = 0 \end{aligned} \qquad \text{\& cyclic permutes}$$

for some non-zero constants $\tau_i, \lambda_i, a_i, b_i \in K$. The action of M_2 tells us $\lambda_0 = \lambda_1 = \dots = \lambda_{n-1}$ and we write λ for the common value. Similarly, the action of M_2 suggests we write $a_0 = a\tau_2\tau_3\tau_4\tau_5$ and $b_0 = b\tau_2\tau_3^2\tau_4^2\tau_5$ since these relations will still hold when we cyclically permute the subscripts. It remains to see how the quantities a, b, λ and $\prod \tau_i$ are related. By Lemma 2.6(i) we may choose $(0 : z_1 : \dots : z_6) \in T \cap H_0$ with all $z_i \neq 0$. We find

$$\tau_2 z_2^2 + z_1 z_3 = \tau_3 z_3^2 + \lambda z_2 z_4 = \tau_4 z_4^2 + \lambda z_3 z_5 = \tau_5 z_5^2 + z_4 z_6 = 0. \tag{23}$$

If $\prod z_i^{\mu_i}$ and $\prod z_i^{\nu_i}$ are two monomials with $\sum \mu_i = \sum \nu_i$ and $\sum i\mu_i = \sum i\nu_i$ then (23) allows us to express their ratio in terms of λ and the τ_i. In particular

$$\begin{aligned} z_1 z_6 + a\tau_2\tau_3\tau_4\tau_5 z_2 z_5 = 0 &\implies \quad a = -1/\lambda^2 \\ \lambda z_1 z_6 + b\tau_2\tau_3^2\tau_4^2\tau_5 z_3 z_4 = 0 &\implies \quad b = -1/\lambda^3 \end{aligned}$$

$$\left. \begin{aligned} (\lambda - 1) z_1 z_3 + b\tau_4\tau_5^2\tau_6^2\tau_0 z_5 z_6 = 0 \\ \tau_1 z_1^2 + b\tau_3\tau_4^2\tau_5^2\tau_6 z_4 z_5 = 0 \end{aligned} \right\} \implies \lambda^4(\lambda - 1) = \prod \tau_i.$$

This completes the proof in the case $n = 7$. □

We proceed to study the schemes $T = T[\lambda; \tau_0, \dots, \tau_{n-1}]$.

Lemma 2.9. *Up to rescaling co-ordinates, the schemes $T[\lambda; \tau_0, \ldots, \tau_{n-1}]$ over K are uniquely determined by $\lambda \in K$ and $\theta = \prod \tau_i^{-i} \in K^\times/(K^\times)^n$.*

Proof. Rescaling the co-ordinate x_1 by $u \in K^\times$ gives

$$T[\lambda; \tau_0, \tau_1, \tau_2, \ldots, \tau_{n-1}] \cong T\big[\lambda; u\tau_0, u^{-2}\tau_1, u\tau_2, \ldots, \tau_{n-1}\big].$$

Repeating for the other co-ordinates we find

$$T[\lambda; \tau_0, \tau_1, \tau_2, \ldots, \tau_{n-1}] \cong T\big[\lambda; u^{-n}\tau_0, u^n\tau_1, \tau_2, \ldots, \tau_{n-1}\big].$$

The lemma follows easily from these observations. □

An important consequence of Lemma 2.9 is that geometrically, *i.e.* over $\overline{K}$, the schemes $T = T[\lambda; \tau_0, \ldots, \tau_{n-1}]$ are determined by λ.

Proposition 2.10. *Let $\lambda, \tau_0, \ldots, \tau_{n-1} \in K$ with $\alpha(\lambda) = \prod \tau_i \neq 0$.*
(i) If $\beta(\lambda) \neq 0$ then T is a smooth curve of genus 1.
(ii) If $\beta(\lambda) = 0$ then T is a Néron polygon.

Proof. By Lemma 2.9 we may suppose $K = \overline{K}$ and that $\tau_0 = \tau_1 = \ldots = \tau_{n-1}$. We apply the results of Sect. 2.1.

Case $n = 5$. The curve defined by (17) is $T[\lambda; \tau, \ldots, \tau]$ where $\tau = a/b$ and $\lambda = \tau^5$. Thus T is either a smooth curve of genus 1, or degenerates to a Néron polygon. The condition for degeneration is $\lambda = \phi^5$ or $\overline{\phi^5}$, equivalently $\lambda^2 - 11\lambda - 1 = 0$.

Case $n = 7$. The curve defined by (18) is $T[\lambda; \tau, \ldots, \tau]$ where $\lambda = -ac^2/b^3$ and $\tau = ac/b^2$. So the following birational map comes for free.

$$\begin{aligned} \{a^3b + b^3c + c^3a = 0\} &\to \{\lambda^4(\lambda - 1) = \tau^7\} \\ (a : b : c) &\mapsto (-ac^2/b^3, ac/b^2) \\ (\tau^3 : -\lambda\tau : \lambda^2) &\leftarrow\!\shortmid (\lambda, \tau) \end{aligned}$$

Again we deduce T is either a smooth curve of genus 1, or degenerates to a Néron polygon. The condition for degeneration is $\lambda = -(\zeta - \zeta^6)(\zeta^4 - \zeta^3)^2/(\zeta^2 - \zeta^5)^3$ or one of its conjugates, equivalently $\lambda^3 - 8\lambda^2 + 5\lambda + 1 = 0$. □

Lemma 2.11. *The scheme $T[\lambda; \tau_0, \ldots, \tau_{n-1}]$ meets the co-ordinate hyperplanes H_i in a total of n^2 points. The points of intersection with H_i are defined over $K(\zeta, \sqrt[n]{\alpha(\lambda)^i\theta})$ where $\theta = \prod \tau_i^{-i}$.*

Proof. Directly from the equations we may check $T \cap H_i \cap H_j = \emptyset$ for all $i \neq j$. Our first claim now follows from the above geometric description of T. For our second claim it suffices, by symmetry, to show that the points $T \cap H_0$ are defined over $K(\zeta, \sqrt[n]{\theta})$. But if $T = T[\lambda; \alpha(\lambda), 1, \ldots, 1]$ then $T \cap H_0$ has a unique fixed point under

$$[-1] : (x_0 : x_1 : \ldots : x_{n-1}) \mapsto (x_0 : x_{n-1} : \ldots : x_1).$$

The uniqueness statement tells us that this point is K-rational. We are now done by Lemma 2.9. □

We relate the curves $T[\lambda; \tau_0, \dots, \tau_{n-1}]$ to the torsors $C_{\lambda,\theta}$ defined in Sect. 1.2.

Proposition 2.12. *Let $\lambda \in K$ not a cusp of $X_1(n)$.*
(i) If $\tau_0, \dots, \tau_{n-1} \in K$ with $\alpha(\lambda) = \prod \tau_i$ and $\theta = \prod \tau_i^{-i}$ then

$$T[\lambda; \tau_0, \dots, \tau_{n-1}] \cong C_{\lambda,\theta}.$$

(ii) The image of $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda(K)$ under δ is generated by $\alpha(\lambda)$.

Proof. (i) We temporarily write $T_\lambda := T[\lambda; \alpha(\lambda), 1, \dots, 1]$. By Lemma 2.11, $T_\lambda(K) \neq \emptyset$ and an explicit calculation reveals the rational point

$$0 = \begin{cases} (0:1:1:-1:-1) \\ (0:1:-\lambda:-\lambda^2:\lambda^2:\lambda:-1). \end{cases}$$

The case $\theta = 1$ of the proposition is equivalent to the statement that the families of elliptic curves C_λ and T_λ are equal. So let C/K be an elliptic curve with $\boldsymbol{\mu}_n \hookrightarrow C$. We claim that $\boldsymbol{\mu}_n \hookrightarrow C$ is isomorphic to $\boldsymbol{\mu}_n \hookrightarrow T_\lambda$ for some unique $\lambda \in K$. We embed $C \hookrightarrow \mathbf{P}^{n-1}$ via the complete linear system $|n.0|$. Then by (15) and the argument at the end of Sect. 1.2, we may choose co-ordinates such that the action of $\boldsymbol{\mu}_n$ on C via translation is the diagonal action (22). We may further assume $0 \in C \cap \{x_0 = 0\}$. Now Proposition 2.8 tells us $C \cong T[\lambda; \tau_0, \dots, \tau_{n-1}]$ for some $\lambda, \tau_0, \dots, \tau_{n-1} \in K$. By Lemma 2.11 we have $\theta = \prod \tau_i^{-i} \in (K^\times)^n$ and by Lemma 2.9 it follows $C \cong T_\lambda$. To check the uniqueness statement we consider the automorphisms of $\mathbf{P}^{n-1}$ that commute with (22). These are given by rescaling and cyclically permuting our co-ordinates. In particular they do not alter λ and this proves our claim.

To show that the families C_λ and T_λ are equal, it only remains to check that we have chosen the same co-ordinate λ on $X_1(n) \cong \mathbf{P}^1$ here as in Sect. 1.1. But in both cases our co-ordinate λ has been chosen such that the cusps are as listed in Sect. 1.1. We have now shown $C_\lambda = T[\lambda; \alpha(\lambda), 1, \dots, 1]$.

Let $\tau_0, \dots, \tau_{n-1}$ be as above. By Lemma 2.9 there is an isomorphism defined over $\overline{K}$

$$\psi : T[\lambda; \tau_0, \tau_1, \dots, \tau_{n-1}] \xrightarrow{\sim} C_\lambda = T[\lambda; \alpha(\lambda), 1, \dots, 1] \qquad (24)$$

given by rescaling co-ordinates. But the only automorphisms of C_λ given by rescaling co-ordinates belong to our diagonal action of $\boldsymbol{\mu}_n$. Thus the cocycle $\sigma \mapsto \sigma(\psi)\psi^{-1}$ takes values in $\boldsymbol{\mu}_n$. We compute $\sigma(\psi)\psi^{-1} = \sigma(\sqrt[n]{\theta})/\sqrt[n]{\theta}$.
(ii) Since

$$T[\lambda; \tau_0, \tau_1, \dots, \tau_{n-1}] \cong T[\lambda; \tau_{n-1}, \tau_0, \dots, \tau_{n-2}]$$

it is clear from (i) and the exact sequence (7) that $\alpha(\lambda) \in \operatorname{im}\delta$. Taking $\tau_0 = \dots = \tau_{n-2} = 1$ and $\tau_{n-1} = \alpha(\lambda)$ in (24) we construct $\psi : C_\lambda \to C_\lambda$, translation by an element of $C_\lambda[n]$, such that $\sigma(\psi)\psi^{-1} = \sigma(\sqrt[n]{\alpha(\lambda)})/\sqrt[n]{\alpha(\lambda)}$. Thus $\alpha(\lambda) \in \operatorname{im}\delta$ is in fact the image of the torsion $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda(K)$. □

Remark 2.13. Relabelling our copy of $\boldsymbol{\mu}_n$ gives isomorphisms $C_{\lambda,\theta} \cong C_{-1/\lambda,\theta^2}$ respectively $C_{\lambda,\theta} \cong C_{(\lambda-1)/\lambda,\theta^2}$. Proposition 2.12 allows us to explicitly write down these isomorphisms. For example in the case $n = 5$ we have

$$\begin{aligned} &T[\lambda; \tau_0, \tau_1, \tau_2, \tau_3, \tau_4] \cong T[-1/\lambda; -\tau_0/(\tau_2\tau_3), \dots, -\tau_3/(\tau_0\tau_1)] \\ &(x_0 : x_1 : x_2 : x_3 : x_4) \mapsto (x_0 : x_2 : x_4 : x_1 : x_3). \end{aligned}$$

Finally we drop our assumption $\mathrm{char}(K) \neq n$. The equations appearing in the statement of the next proposition are obtained from those for $T[\lambda; \tau_0, \dots, \tau_{n-1}]$ by manipulating under the assumption $\alpha(\lambda) = \prod \tau_i \neq 0$ and then setting $\lambda = 0$, respectively $\lambda = 1$. We write $P_0 = (1 : 0 : 0 : \dots)$, $P_1 = (0 : 1 : 0 : \dots)$, ...

Proposition 2.14. *Let $\tau_0, \dots, \tau_{n-1} \in K$ with $I = \{i \mid \tau_i = 0\} \neq \emptyset$. Then the subscheme of $\mathbf{P}^{n-1}$ with equations*

$$\begin{array}{lll} n = 5 & \tau_0 x_0^2 + x_1 x_4 - \tau_2\tau_3 x_2 x_3 = 0 & \text{\& cyclic permutes} \\ n = 7 & \left\{ \begin{array}{l} \tau_0 x_0^2 + x_1 x_6 - \tau_2\tau_3\tau_4\tau_5 x_2 x_5 = 0 \\ \tau_0^2\tau_1\tau_6 x_0^2 - x_2 x_5 + \tau_3\tau_4 x_3 x_4 = 0 \end{array} \right. & \text{\& cyclic permutes} \end{array}$$

is the union of $|I|$ rational curves. More precisely for each consecutive pair $i, i+d \in I$ we have a rational curve of degree d joining P_i and P_{i+d}.

Proof. Rescaling co-ordinates, over $\overline{K}$ if necessary, we may suppose that the non-zero τ_i are all 1. We split into cases according as the τ_i are 0 or 1. In each case a straightforward calculation proves the proposition. Notice that in the most degenerate case, namely when all the τ_i are 0, we obtain a Néron polygon. □

2.3. Local solubility for torsors

In this section we work over a field which is complete with respect to a discrete valuation and has finite residue field. We use the results of Sect. 2.2 to give some criteria for the existence of rational points on the torsors $C_{\lambda,\theta}$. We adopt the following notation.

K	a field complete with respect to the valuation $\mathrm{ord} : K^\times \twoheadrightarrow \mathbf{Z}$
$\mathcal{O}$	the ring of integers of $K = \{x \in K \mid \mathrm{ord}(x) \geq 0\}$
$\mathfrak{p}$	the maximal ideal of $\mathcal{O} = \{x \in K \mid \mathrm{ord}(x) > 0\}$
k	the residue field of $\mathcal{O} = \mathcal{O}/\mathfrak{p}$ (assumed finite).

We define $\mathrm{ord}^*(\lambda)$ to be the non-negative integer r with

$$\begin{array}{lll} n = 5 & \{\mathrm{ord}(\lambda), \mathrm{ord}(-1/\lambda)\} & = \{-r, r\} \\ n = 7 & \{\mathrm{ord}(\lambda), \mathrm{ord}((\lambda-1)/\lambda), \mathrm{ord}(1/(1-\lambda))\} & = \{-r, 0, r\}. \end{array}$$

Proposition 2.15. *Let $\lambda \in K$ not a cusp of $X_1(n)$. We describe the image of the connecting homomorphism $\delta : D_\lambda(K) \to K^\times/(K^\times)^n$.*

(a) If $\mathrm{ord}^*(\lambda) > 0$ *then* $\mathrm{im}\,\delta = K^\times/(K^\times)^n$.

(b) If $\mathrm{ord}^*(\lambda) = 0$ *then* $\mathrm{im}\,\delta \subset \mathcal{O}^\times/(\mathcal{O}^\times)^n$.

(c) If $\mathrm{ord}^*(\lambda) = 0$ *and* $\mathrm{char}(k) \neq n$ *then*

(i) If $\beta(\lambda) \not\equiv 0 \pmod{\mathfrak{p}}$ *then* $\mathrm{im}\,\delta = \mathcal{O}^\times/(\mathcal{O}^\times)^n$.

(ii) If $\beta(\lambda) \equiv 0 \pmod{\mathfrak{p}}$ *then* $\mathrm{im}\,\delta = 0$.

Proof. Let us note that by the work of Sect. 1.2, $C_{\lambda,\theta}(K) \neq \emptyset \iff \theta \in \operatorname{im}\delta$.
(a) Let $\theta \in K^\times/(K^\times)^n$. By Remark 2.13 we may assume $\operatorname{ord}(\lambda) > 0$, respectively $\operatorname{ord}(\lambda - 1) > 0$. We write $C_{\lambda,\theta}$ in the form $T[\lambda; \tau_0, \dots, \tau_{n-1}]$ with $\operatorname{ord}(\tau_i) \geq 0$ for all i. By Proposition 2.14 the reduction of this curve is a collection of rational curves each defined over k. At least one of these curves has odd degree and so is isomorphic to $\mathbf{P}^1$ over k. We pick a smooth point on the reduction and lift using Hensel's lemma to give $C_{\lambda,\theta}(K) \neq \emptyset$ as required.
(b) Suppose $\theta \in K^\times/(K^\times)^n$ with $\operatorname{ord}(\theta) \equiv 1 \pmod{n}$. We write $C_{\lambda,\theta}$ in the form $T[\lambda; \tau_0, \dots, \tau_{n-1}]$ with $\operatorname{ord}(\tau_0) = -1$, $\operatorname{ord}(\tau_{n-1}) = 1$ and $\operatorname{ord}(\tau_i) = 0$ for all other i. We take $(x_0 : \dots : x_{n-1})$ a K-point with $\min\{\operatorname{ord}(x_i)\} = 0$. Examining the equations for $T[\lambda; \tau_0, \dots, \tau_{n-1}]$ we successively deduce $\operatorname{ord}(x_i) > 0$ for $i = 0, 1, \dots, n-1$. This contradiction tells us $C_{\lambda,\theta}(K) = \emptyset$. Thus $\operatorname{im}\delta \subset \mathcal{O}^\times/(\mathcal{O}^\times)^n$.
(c) Let $\theta \in \mathcal{O}^\times/(\mathcal{O}^\times)^n$ and write $C_{\lambda,\theta}$ in the form $T[\lambda; \tau_0, \dots, \tau_{n-1}]$ with $\operatorname{ord}(\tau_i) = 0$ for all i. The reduction of this curve is described by Proposition 2.10. In case (i) the reduction is a smooth curve of genus 1. By [Ca3, Chapter 25] we have a rational point which we lift using Hensel's lemma. Thus $\operatorname{im}\delta = \mathcal{O}^\times/(\mathcal{O}^\times)^n$ as required. In case (ii) the reduction is a collection of n distinct lines. If $C_{\lambda,\theta}(K) \neq \emptyset$ then one of these lines must be defined over k. This line meets each of the hyperplanes H_i. By Lemma 2.11 we deduce that both $\alpha(\lambda)$ and θ are nth powers mod $\mathfrak{p}$. Since $\operatorname{char}(k) \neq n$ it follows $\theta \in (K^\times)^n$. Thus $\operatorname{im}\delta = 0$ as required. □

Proposition 2.15 is incomplete in that we do not fully treat the case $\operatorname{char}(k) = n$. In particular, if $\beta(\lambda) \equiv 0 \pmod{\mathfrak{p}}$, then the equations for $T[\lambda; \tau_0, \dots, \tau_{n-1}]$ reduce to give a line with multiplicity n. This makes it difficult to apply Hensel's lemma. We therefore abandon the projective space method and revert to using the push-out method also described in Sect. 1.2. Specifically we recall that the map

$$\delta : D_\lambda(K) \to K^\times/(K^\times)^n$$

may be described in terms of a rational function $f \in K(D_\lambda)$, explicitly given by (9). We use the formal group defined by D_λ as a vehicle for our Hensel lemma calculations. We recall [Si1, Chapter IV] that the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is satisfied by the power series

$$\begin{aligned} x(z) &= \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3z - (a_4 + a_1a_3)z^2 - \dots \\ y(z) &= -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1a_3)z + \dots . \end{aligned}$$

Applying this to the curves D_λ defined by (2) we find that $x(z)$ and $y(z)$ are power series with coefficients in $\mathbf{Z}[\lambda]$. We compute the first few terms of the power series $F(z) := \pm z^n f(x(z), y(z))$.

$$\begin{aligned} F(z) &= 1 + (2\lambda - 1)z + \lambda(\lambda + 2)z^2 + \dots \\ F(z) &= 1 + (3\lambda^2 - 2\lambda - 2)z + (\lambda - 1)(3\lambda^3 + 3\lambda^2 - 3\lambda - 1)z^2 + \dots \end{aligned}$$

Our interest is in the case $\mathrm{char}(k) = n$. We find $\beta(\lambda) \equiv (\lambda - 3)^2 \pmod{\mathfrak{p}}$, respectively $\beta(\lambda) \equiv (\lambda - 5)^3 \pmod{\mathfrak{p}}$, and $F'(0) \equiv \beta'(\lambda) \pmod{\mathfrak{p}}$. Thus

$$F(\mathfrak{p}\mathcal{O}) = 1 + \mathfrak{p}\mathcal{O} \qquad \text{if } \beta(\lambda) \not\equiv 0 \pmod{\mathfrak{p}} \tag{25}$$

$$F(\mathfrak{p}\mathcal{O}) \subset 1 + \mathfrak{p}^2\mathcal{O} \qquad \text{if } \beta(\lambda) \equiv 0 \pmod{\mathfrak{p}}. \tag{26}$$

In the case $K = \mathbf{Q}_p$ this gives us all we need.

Proposition 2.16. *Let $p = n$. Let $\lambda \in \mathbf{Q}_p$ not a cusp of $X_1(n)$. We describe the image of $\delta : D_\lambda(\mathbf{Q}_p) \to \mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^n$ in the case* $\mathrm{ord}^*(\lambda) = 0$.
(i) If $\beta(\lambda) \not\equiv 0 \pmod{p}$ then $\mathrm{im}\,\delta = \mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^n$.
(ii) If $\beta(\lambda) \equiv 0 \pmod{p}$ then $\mathrm{im}\,\delta$ *is generated by $\alpha(\lambda)$. Thus the condition for δ to be the zero map is $\lambda \equiv 18 \pmod{25}$, respectively* $\lambda \equiv 5 \pmod{7}$.

Proof. As observed in Sect. 1.1, the Weierstrass equation (2) is minimal. We write $E = D_\lambda$ and recall [Si1, Chapter VII] there is a filtration

$$E(\mathbf{Q}_p) \supset E_0(\mathbf{Q}_p) \supset E_1(\mathbf{Q}_p).$$

By Lemma 1.4 the image of δ restricted to $E_1(\mathbf{Q}_p)$ is generated by $F(p\mathbf{Z}_p)$.
(i) By Proposition 2.15(b) we have $\mathrm{im}\,\delta \subset \mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^n$. Since $1 + p\mathbf{Z}_p$ generates $\mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^n$ it follows from (25) that we have equality.
(ii) Since $1 + p^2\mathbf{Z}_p \subset (\mathbf{Z}_p^\times)^n$, it follows from (26) that δ restricted to $E_1(\mathbf{Q}_p)$ is trivial. Next $E_0(\mathbf{Q}_p)/E_1(\mathbf{Q}_p) \cong \widetilde{E}_{\mathrm{ns}}(\mathbf{Z}/n\mathbf{Z}) \cong \mathbf{Z}/n\mathbf{Z}$, so by Proposition 2.12(ii) the image of δ restricted to $E_0(\mathbf{Q}_p)$ is generated by $\alpha(\lambda)$. Finally in the case of additive reduction, the Tamagawa number $[E(\mathbf{Q}_p) : E_0(\mathbf{Q}_p)]$ is at most 4, and so prime to n. It follows that there is no further contribution to the image of δ. For the last statement we compute

$$\left\{ \begin{array}{c} \lambda \equiv 3 \pmod{5} \\ \lambda \in \left(\mathbf{Q}_5^\times\right)^5 \end{array} \right\} \Longleftrightarrow \lambda \equiv 18 \pmod{25}$$

$$\left\{ \begin{array}{c} \lambda \equiv 5 \pmod{7} \\ \lambda^4(\lambda - 1) \in \left(\mathbf{Q}_7^\times\right)^7 \end{array} \right\} \Longleftrightarrow \lambda \equiv 5 \pmod{7}.$$

□

2.4. *Proof of the descent theorem*

Let $n = 5$ or 7. Let $\lambda \in \mathbf{Q}$ not a cusp of $X_1(n)$ and let $\mathcal{A}$, $\mathcal{B}$ be the sets of rational primes defined in Sect. 1.3. In this section we prove that the Selmer groups $S^{(\phi)}(C_\lambda/\mathbf{Q})$ and $S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q})$ are as described in Theorem 1.

Let p be a rational prime. The Tate pairing

$$(\cdot, \cdot)_p : H^1(\mathbf{Q}_p, C[\phi]) \times H^1\big(\mathbf{Q}_p, D[\widehat{\phi}]\big) \to \mathbf{Q}/\mathbf{Z} \tag{27}$$

is induced by cup product from the Weil pairing, followed by the "invariant" map $\mathrm{Br}(\mathbf{Q}_p) \to \mathbf{Q}/\mathbf{Z}$. Since $C[\phi] \cong \boldsymbol{\mu}_n$ and $D[\widehat{\phi}] \cong \mathbf{Z}/n\mathbf{Z}$ we identify $H^1(\mathbf{Q}_p, C[\phi]) = \mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^n$ and $H^1(\mathbf{Q}_p, D[\widehat{\phi}]) = \mathrm{Hom}(G_p, \mathbf{Z}/n\mathbf{Z})$. Here our notation is $G_p := \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ and we write $I_p \subset G_p$ for the inertia subgroup.

Proposition 2.17. *Let $\lambda \in \mathbf{Q}$ not a cusp of $X_1(n)$. The connecting maps*

$$\begin{aligned}\delta_\phi &: D_\lambda(\mathbf{Q}_p) \to H^1(\mathbf{Q}_p, C_\lambda[\phi])\\ \delta_{\widehat{\phi}} &: C_\lambda(\mathbf{Q}_p) \to H^1(\mathbf{Q}_p, D_\lambda[\widehat{\phi}])\end{aligned}$$

have images

$$\operatorname{im}\delta_\phi = \begin{cases} \mathbf{Q}_p^\times/\big(\mathbf{Q}_p^\times\big)^n & \text{if } p \in \mathcal{A}\\ \mathbf{Z}_p^\times/\big(\mathbf{Z}_p^\times\big)^n & \text{if } p \notin \mathcal{A}\cup\mathcal{B}\\ 0 & \text{if } p \in \mathcal{B}\end{cases}$$

and

$$\operatorname{im}\delta_{\widehat{\phi}} = \begin{cases} 0 & \text{if } p \in \mathcal{A}\\ \operatorname{Hom}(G_p/I_p, \mathbf{Z}/n\mathbf{Z}) & \text{if } p \notin \mathcal{A}\cup\mathcal{B}\\ \operatorname{Hom}(G_p, \mathbf{Z}/n\mathbf{Z}) & \text{if } p \in \mathcal{B}.\end{cases}$$

Proof. (i) The description of $\operatorname{im}\delta_\phi$ is given by combining Propositions 2.15 and 2.16. Note that $\mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^n$ is trivial unless $p = n$ or $p \equiv 1 \pmod{n}$.
(ii) Tate local duality [T1, Theorem 2.3] tells us that for E an elliptic curve over $\mathbf{Q}_p$ there is a non-degenerate pairing $E(\mathbf{Q}_p) \times H^1(\mathbf{Q}_p, E) \to \mathbf{Q}/\mathbf{Z}$ compatible with the Tate pairing (27). We obtain a commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & D(\mathbf{Q}_p)/\phi C(\mathbf{Q}_p) \arrow[r, "\delta_\phi"] \arrow[d] & H^1(\mathbf{Q}_p, C[\phi]) \arrow[r] \arrow[d] & H^1(\mathbf{Q}_p, C)[\phi] \arrow[r] \arrow[d] & 0\\ 0 \arrow[r] & H^1(\mathbf{Q}_p, D)[\widehat{\phi}]^* \arrow[r] & H^1(\mathbf{Q}_p, D[\widehat{\phi}])^* \arrow[r, "\delta_{\widehat{\phi}}^*"] & (C(\mathbf{Q}_p)/\widehat{\phi}D(\mathbf{Q}_p))^* \arrow[r] & 0. \end{tikzcd}$$

Since the vertical maps are isomorphisms we learn that $\operatorname{im}\delta_\phi$ and $\operatorname{im}\delta_{\widehat{\phi}}$ are exact annihilators with respect to the Tate pairing. Thus the description of $\operatorname{im}\delta_{\widehat{\phi}}$ follows from the description of $\operatorname{im}\delta_\phi$. It remains to check that $\mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^n$ and $\operatorname{Hom}(G_p/I_p, \mathbf{Z}/n\mathbf{Z})$ are exact annihilators. We recall [Se2, Chapter XIV] that the Tate pairing

$$\mathbf{Q}_p^\times/\big(\mathbf{Q}_p^\times\big)^n \times \operatorname{Hom}(G_p, \mathbf{Z}/n\mathbf{Z}) \to \mathbf{Z}/n\mathbf{Z}$$

is given by $(\theta, \chi) \mapsto -\chi(\rho(\theta))$ where $\rho : \mathbf{Q}_p^\times \to G_p^{\mathrm{ab}}$ is the local reciprocity map. Thus our claim follows from the description of the local reciprocity map in the unramified case [CF, Chapter VI, §2.5]. □

The description of $S^{(\phi)}(C_\lambda/\mathbf{Q})$ given in Theorem 1 is immediate from Proposition 2.17(i).

$$\begin{aligned} S^{(\phi)}(C_\lambda/\mathbf{Q}) &= \big\{\theta \in \mathbf{Q}^\times/(\mathbf{Q}^\times)^n \big| C_{\lambda,\theta}(\mathbf{Q}_p) \neq \emptyset \text{ for all primes } p\big\}\\ &= \big\{\theta \in [\mathcal{A}] \big| \theta \in (\mathbf{Q}_p^\times)^n \text{ for all } p \in \mathcal{B}\big\}.\end{aligned}$$

We have already seen two proofs of the statement concerning torsion, in Sect. 1.2 via the push-out method, and in Sect. 2.2 via the projective space method. So to prove Theorem 1 it only remains to explain the relationship between $S^{(\phi)}(C_\lambda/\mathbf{Q})$ and $S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q})$. We shall make use of the "product" formula for the local Tate pairings, namely

$$\textstyle\sum_p (a,b)_p = 0.$$

This is a consequence of the well known exact sequence of class field theory

$$0 \longrightarrow \mathrm{Br}(\mathbf{Q}) \longrightarrow \oplus_v \mathrm{Br}(\mathbf{Q}_v) \xrightarrow{\sum \mathrm{inv}} \mathbf{Q}/\mathbf{Z} \longrightarrow 0.$$

where again we have used the fact n is odd to ignore the infinite places. For $\mathcal{S}$ a finite set of rational primes we write

$$\begin{aligned}[\mathcal{S}] &:= \{\, \theta \in \mathbf{Q}^\times/(\mathbf{Q}^\times)^n \mid \mathrm{ord}_p(\theta) \equiv 0 \pmod{n} \text{ for all } p \notin \mathcal{S} \,\} \\ \langle \mathcal{S} \rangle &:= \{\, \chi \in \mathrm{Hom}(G_{\mathbf{Q}}, \mathbf{Z}/n\mathbf{Z}) \mid \chi(I_p) = 0 \text{ for all } p \notin \mathcal{S} \,\}\end{aligned}$$

We define $\Xi : [\mathcal{A}] \times \langle \mathcal{B} \rangle \to \mathbf{Z}/n\mathbf{Z}$ via

$$\Xi(a,b) = \textstyle\sum_{p \in \mathcal{B}} (a,b)_p = -\sum_{p \in \mathcal{A}} (a,b)_p \tag{28}$$

where the two expressions given are equal by Proposition 2.17 and the product formula. Since $\mathcal{B}$ consists of primes $p \equiv 0, 1 \pmod{n}$ it follows by class field theory, specifically the Kronecker-Weber theorem, that $\langle \mathcal{B} \rangle$ has dimension $|\mathcal{B}|$. Thus $[\mathcal{B}] \cong \langle \mathcal{B} \rangle$ as $\mathbf{Z}/n\mathbf{Z}$-vector spaces. So to complete the proof of Theorem 1 it only remains to identify the left and right kernels of Ξ as Selmer groups. For any element $(*)$ we write $(*)_p$ for the corresponding local element.

$$\begin{aligned} S^{(\phi)}(C_\lambda/\mathbf{Q}) &= \left\{\, a \in \mathbf{Q}^\times/(\mathbf{Q}^\times)^n \middle| a_p \in \mathrm{im}\,\delta_\phi \text{ for all primes } p \,\right\} \\ &= \{\, a \in [\mathcal{A}] \mid a_p = 0 \text{ for all } p \in \mathcal{B} \,\} \\ &\subset \ker_L(\Xi) \\ S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q}) &= \{\, b \in \mathrm{Hom}(G_{\mathbf{Q}}, \mathbf{Z}/n\mathbf{Z}) \mid b_p \in \mathrm{im}\,\delta_{\widehat{\phi}} \text{ for all primes } p \,\} \\ &= \{\, b \in \langle \mathcal{B} \rangle \mid b_p = 0 \text{ for all } p \in \mathcal{A} \,\} \\ &\subset \ker_R(\Xi). \end{aligned}$$

To show that these inclusions are in fact equalities we need a lemma.

Lemma 2.18. *The following natural maps are isomorphisms.*
(i) $[\mathcal{A}] \to \oplus_{p \in \mathcal{A}} \mathbf{Q}_p^\times/\big(\mathbf{Q}_p^\times\big)^n \,/\, \mathbf{Z}_p^\times/\big(\mathbf{Z}_p^\times\big)^n$
(ii) $\langle \mathcal{B} \rangle \to \oplus_{p \in \mathcal{B}} \mathrm{Hom}(G_p, \mathbf{Z}/n\mathbf{Z}) \,/\, \mathrm{Hom}(G_p/I_p, \mathbf{Z}/n\mathbf{Z})$

Proof. (i) The map is injective since

$$\left\{\, \theta \in \mathbf{Q}^\times/(\mathbf{Q}^\times)^n \middle| \mathrm{ord}_p(\theta) \equiv 0 \pmod{n} \text{ for all } p \,\right\}$$

is trivial. Both spaces have dimension $|\mathcal{A}|$.
(ii) The map is injective since **Q** has no unramified (abelian) extensions. For $p \equiv 0, 1 \pmod{n}$ we know $\mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^n$ is cyclic of order n. Thus both spaces have dimension $|\mathcal{B}|$. □

Theorem 1 now follows by (28) and the exact annihilation of $\mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^n$ and $\mathrm{Hom}(G_p/I_p, \mathbf{Z}/n\mathbf{Z})$.

3. Examples and applications

3.1. Relationship with the parity conjecture

The estimate (13) for $r = \operatorname{rank} C_\lambda(\mathbf{Q}) = \operatorname{rank} D_\lambda(\mathbf{Q})$ differs from the true rank by

$$\dim_n Ш(C_\lambda/\mathbf{Q})[\phi] + \dim_n Ш(D_\lambda/\mathbf{Q})[\widehat{\phi}] \tag{29}$$

Let us assume that $Ш(C_\lambda/\mathbf{Q})(n)$ and $Ш(D_\lambda/\mathbf{Q})(n)$ are both finite. Since the maps ϕ and $\widehat{\phi}$ on Tate-Shafarevich groups are adjoints with respect to the Cassels-Tate pairing [Ca2, Theorem 1.2], it follows that (29) is even. So Theorem 1 furnishes the following parity result.

Corollary 1. *Let $E/\mathbf{Q}$ be an elliptic curve with a rational point of order $n = 5$ or 7. Assume $Ш(E/\mathbf{Q})(n)$ is finite. Then the parity of the rank of $E(\mathbf{Q})$ is as predicted by the Birch Swinnerton-Dyer conjecture.*

Proof. Theorem 1 and the finiteness assumption on Ш tells us

$$\operatorname{rank} E(\mathbf{Q}) \equiv |\mathcal{A}| + |\mathcal{B}| - 1 \pmod 2.$$

On the other hand, the Birch Swinnerton-Dyer conjecture predicts

$$(-1)^{\operatorname{rank} E(\mathbf{Q})} = \textstyle\prod_v W_v$$

where $W_v = \pm 1$ are the local root numbers. Since $W_\infty = -1$ for any elliptic curve over $\mathbf{Q}$ it suffices for us to prove

$$\{p \text{ prime} \mid W_p = -1\} = \mathcal{A} \cup \mathcal{B}. \tag{30}$$

The following explicit description of the local root numbers for an elliptic curve over $\mathbf{Q}$ is taken from [R]. See also [Co].

Proposition 3.1. *Let E be an elliptic curve over $\mathbf{Q}$ and let p be a prime.*
(i) If E has good reduction at p then $W_p = +1$.
(ii) If E has multiplicative reduction at p then

$$W_p = \begin{cases} -1 & \textit{if } E \textit{ has split reduction} \\ +1 & \textit{if } E \textit{ has non-split reduction.} \end{cases}$$

(iii) If E has additive reduction at p and $p \geq 5$ then

$$W_p = \begin{cases} (-1/p) & \textit{if } e = 2 \textit{ or } 6 \\ (-3/p) & \textit{if } e = 3 \\ (-2/p) & \textit{if } e = 4 \end{cases}$$

where (a/p) is the quadratic Legendre symbol and $e = 12/\gcd(\mathrm{ord}_p(\Delta), 12)$.

Our claim (30) now follows from the description of the reduction types in Lemma 1.3. The following table summarises the calculations required in the case of additive reduction.

$p = n$	λ	$\mathrm{ord}_p(\beta(\lambda))$	e	W_p
5	$\mathrm{ord}_5(\lambda - 18) = 1$	2	6	$+1$
5	$\mathrm{ord}_5(\lambda - 18) \geq 2$	3	4	-1
7	$\mathrm{ord}_7(\lambda - 5) \geq 1$	2	6	-1

□

Remark 3.2. Corollary 1 is in fact a special case of a result of Monsky [Mo], who works with elliptic curves E over **Q** admitting a rational isogeny of prime degree. His method is to find a quadratic twist of E with analytic rank 0, and then to apply the work of Kolyvagin and others.

3.2. Exhibiting large selmer groups

We may use Theorem 1 to exhibit elliptic curves with large n-Selmer group. To do this we choose $\lambda \in \mathbf{Q}$ such that $|\mathcal{A}|$ is large and $|\mathcal{B}|$ is small, or vice versa. I am grateful to Ed Schaefer for bringing to my attention the following result.

Proposition 3.3. *Let $F(x)$ be an irreducible polynomial of degree d with integer coefficients. Suppose that for all primes p the congruence $F(x) \equiv 0 \pmod{p}$ has fewer than p solutions. Then there exist infinitely many integers y such that $F(y)$ consists of at most $d + 1$ prime factors.*

Proof. [HR, Theorem 9.7]. □

Corollary 2. *For $n = 5$ or 7 the n-Selmer group of an elliptic curve over* **Q** *may become arbitrarily large.*

Proof. Let M be the product of the first m primes. Applying Proposition 3.3 to the polynomial $F(x) = \beta(Mx)$ gives infinitely many integers $\lambda = My$ with $|\mathcal{A}| \geq m$ and $|\mathcal{B}| \leq (n + 1)/2$. The corollary is now immediate from Theorem 1. □

We could equally prove Corollary 2 by taking $|\mathcal{A}|$ small and $|\mathcal{B}|$ large. Lemma 1.8 shows how we may force $|\mathcal{B}|$ to be large by imposing linear congruences on λ. In the case $n = 5$ we then appeal to Dirichlet's theorem on primes in arithmetic progression to give $|\mathcal{A}| = 1$. (In fact this is all we shall need in the next section to show that the 5-torsion of the Tate-Shafarevich group may become arbitrarily large.) In the case $n = 7$ we appeal to [HR, Theorem 10.11] which generalises Proposition 3.3 to $F(x)$ a product of distinct irreducible polynomials. It seems we must take $\lambda = (\text{integer})/2$ in order to satisfy the hypothesis at $p = 2$.

3.3. Exhibiting large Tate-Shafarevich groups

Results of Cassels [Ca1], Bölling [Bö] and Kramer [Kr] show that the 2- and 3-torsion of the Tate-Shafarevich group of an elliptic curve over $\mathbf{Q}$ may become arbitrarily large. In this section we give a corresponding result for the 5-torsion. The idea is that the elliptic curves $E/\mathbf{Q}$ with $E[5] \cong \boldsymbol{\mu}_5 \oplus \mathbf{Z}/5\mathbf{Z}$ belong to both the families C_λ and D_λ. We may therefore estimate rank $E(\mathbf{Q})$ by applying Theorem 1 for two different values of λ. We then arrange for these estimates to differ.

Corollary 3. *The 5-torsion of the Tate-Shafarevich group of an elliptic curve over* $\mathbf{Q}$ *may become arbitrarily large.*

We define polynomials

$$\begin{aligned} f(\tau) &= \tau^4 + 3\tau^3 + 4\tau^2 + 2\tau + 1 = ((\tau+1)^5 + 1)/(\tau+2) \\ g(\tau) &= \tau^4 - 2\tau^3 + 4\tau^2 - 3\tau + 1 = ((\tau-1)^5 + \tau^5)/(2\tau - 1). \end{aligned}$$

Lemma 3.4. *The elliptic curves* $E/\mathbf{Q}$ *with* $E[5] \cong \boldsymbol{\mu}_5 \oplus \mathbf{Z}/5\mathbf{Z}$ *are the curves* $E_\tau := C_{\tau^5} \cong D_{\tau f(\tau)/g(\tau)}$ *for* $\tau \in \mathbf{Q}$ *with* $\tau \neq 0$.

Proof. The statement concerning torsion in Theorem 1 tells us that the required universal family is $E_\tau := C_{\tau^5}$. Here τ is a co-ordinate on $X(5) \cong \mathbf{P}^1$ and the cusps are at $\tau = 0, \infty, \zeta^i\phi, \zeta^i\overline{\phi}$, where $\phi = 1 + \zeta + \zeta^4$ is the golden ratio and $\overline{\phi} = 1 + \zeta^2 + \zeta^3$ is its conjugate. There are involutions

$$\begin{aligned} \eta : X_1(5) \to X_1(5)\,; &\qquad \lambda \mapsto (\phi^5\lambda + 1)/(\lambda - \phi^5) \\ \varepsilon : X(5) \to X(5)\,; &\qquad \tau \mapsto (\phi\tau + 1)/(\tau - \phi) \end{aligned}$$

mapping cusps to cusps. In fact $C_\lambda \cong D_{\eta(\lambda)}$ over $\mathbf{Q}(\boldsymbol{\mu}_5)$, whereas ε belongs to the action of $\mathrm{PSL}_2(\mathbf{Z}/5\mathbf{Z})$ on $X(5)$. The following isomorphisms are defined over $\mathbf{Q}(\boldsymbol{\mu}_5)$

$$C_{\tau^5} \cong E_\tau \cong E_{\varepsilon(\tau)} \cong C_{\varepsilon(\tau)^5} \cong D_{\eta(\varepsilon(\tau)^5)}. \tag{31}$$

We find $\eta(\varepsilon(\tau)^5) = \tau f(\tau)/g(\tau)$ and the isomorphism (31) maps $\mathbf{Z}/5\mathbf{Z} \hookrightarrow C_{\tau^5}$ onto $\mathbf{Z}/5\mathbf{Z} \hookrightarrow D_{\tau f(\tau)/g(\tau)}$. Comparing this isomorphism with its Galois conjugates, and appealing to Lemma 1.1(iii), we deduce $C_{\tau^5} \cong D_{\tau f(\tau)/g(\tau)}$ over $\mathbf{Q}$. □

For $\tau \in \mathbf{Q}$ with $\tau \neq 0$ we define disjoint sets of rational primes

$$\begin{aligned} \mathcal{P} &= \{\, p \text{ prime} \mid \mathrm{ord}_p(\tau) \neq 0 \,\} \\ \mathcal{Q} &= \{\, p \text{ prime} \mid f(\tau)g(\tau) \equiv 0 \pmod{p} \text{ and } p \equiv 1 \pmod{5} \,\} \\ \mathcal{R} &= \{\, p \text{ prime} \mid \tau^2 - \tau - 1 \equiv 0 \pmod{p} \text{ and } p \equiv 0, 1 \pmod{5} \,\}. \end{aligned}$$

Lemma 3.5. *For p a rational prime,*
(i) $f(\tau) \equiv 0 \pmod{p}$ *is soluble* $\iff$ $p = 5$ *or* $p \equiv 1 \pmod{5}$
(ii) $g(\tau) \equiv 0 \pmod{p}$ *is soluble* $\iff$ $p = 5$ *or* $p \equiv 1 \pmod{5}$
(iii) $\tau^2 - \tau - 1 \equiv 0 \pmod{p}$ *is soluble* $\iff$ $p = 5$ *or* $p \equiv \pm 1 \pmod{5}$.

Proof. Consider how p factors in $\mathbf{Q}(\boldsymbol{\mu}_5)$. □

Lemma 3.6. *We apply Theorem 1 for* $\lambda = \tau^5$ *and* $\lambda = \tau f(\tau)/g(\tau)$.
(i) If $\lambda = \tau^5$ *then* $\mathcal{A} = \mathcal{P}$ *and* $\mathcal{B} = \mathcal{Q} \cup \mathcal{R}$.
(ii) If $\lambda = \tau f(\tau)/g(\tau)$ *then* $\mathcal{A} = \mathcal{P} \cup \mathcal{Q}$ *and* $\mathcal{B} = \mathcal{R}$.

Proof. These claims follow from the identities

$$\begin{aligned} \tau^{10} - 11\tau^5 - 1 &= (\tau^2 - \tau - 1) f(\tau) g(\tau) \\ \tau^2 f(\tau)^2 - 11\tau f(\tau) g(\tau) - g(\tau)^2 &= (\tau^2 - \tau - 1)^5. \end{aligned}$$

For τ prime to 5 we are assisted by the observation

$$\mathrm{ord}_5(\tau^2 - \tau - 1) = \mathrm{ord}_5(f(\tau)) = \mathrm{ord}_5(g(\tau)) = 0 \text{ or } 1.$$

□

Proof of Corollary 3. Let $\tau \in \mathbf{Q}$ with $\tau \neq 0$. Theorem 1 gives two estimates for rank $E_\tau(\mathbf{Q})$. Writing $[\mathcal{A}, \mathcal{B}]$ for the matrix $(\chi_q(p))_{p \in \mathcal{A}, q \in \mathcal{B}}$, these are

$$\begin{aligned} &|\mathcal{P}| + |\mathcal{Q}| + |\mathcal{R}| - 1 - 2\,\mathrm{rank}[\mathcal{P}, \mathcal{Q} \cup \mathcal{R}] \\ &|\mathcal{P}| + |\mathcal{Q}| + |\mathcal{R}| - 1 - 2\,\mathrm{rank}[\mathcal{P} \cup \mathcal{Q}, \mathcal{R}]. \end{aligned} \tag{32}$$

By repeated use of Dirichlet's theorem on primes in arithmetic progression, we choose $\mathcal{Q}_0$ and $\mathcal{R}_0$ disjoint sets of primes $p \equiv 1 \pmod 5$ with $\mathrm{rank}[\mathcal{Q}_0, \mathcal{R}_0]$ arbitrarily large. With one final application of Dirichlet we choose τ prime such that $\mathcal{Q} \supset \mathcal{Q}_0$ and $\mathcal{R} \supset \mathcal{R}_0$. Then $|\mathcal{P}| = 1$ and

$$\mathrm{rank}[\mathcal{P}, \mathcal{Q} \cup \mathcal{R}] \ll \mathrm{rank}[\mathcal{P} \cup \mathcal{Q}, \mathcal{R}].$$

The difference in the estimates (32) now proves the corollary. □

A closer inspection of the proof of Corollary 3 shows that we are forcing elements of order 5 in the Tate-Shafarevich group of the elliptic curves isogenous to E_τ rather than for E_τ itself.

3.4. Relationship with a formula of Cassels

We compare our Theorem 1 with a formula of Cassels. This section is based on similar calculations in [Lo, §7].

Let $\phi : E \to E'$ and $\widehat{\phi} : E' \to E$ be dual isogenies of elliptic curves over $\mathbf{Q}$. We recall a formula of Cassels [Ca2], relating the order of the Selmer group attached to ϕ to the order of the Selmer group attached to $\widehat{\phi}$.

$$\frac{\#S^{(\phi)}(E/\mathbf{Q})}{\#S^{(\widehat{\phi})}(E'/\mathbf{Q})} = \frac{\#E(\mathbf{Q})[\phi]}{\#E'(\mathbf{Q})[\widehat{\phi}]} \times \frac{\Omega_{E'}}{\Omega_E} \times \prod_p \frac{c_p(E')}{c_p(E)}. \tag{33}$$

Here $\Omega_E = \int_{E(\mathbf{R})} \omega$ with ω the canonical Néron differential on E, and $c_p(E) = [E(\mathbf{Q}_p) : E_0(\mathbf{Q}_p)]$ is the Tamagawa number at the prime p.

Let $n = 5$ or 7 and let $\lambda \in \mathbf{Q}$ with $\lambda \neq 0$, respectively $\lambda \neq 0, 1$. We check that (33), applied to the n-isogeny $\phi : C_\lambda \to D_\lambda$ is compatible with our descent calculations. By Theorem 1 the LHS of (33) is

$$\# S^{(\phi)}(C_\lambda/\mathbf{Q}) / \# S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q}) = n^{|\mathcal{A}|-|\mathcal{B}|}.$$

We now compute the RHS of (33). As seen in Sect. 1.1 we are always free to assume $\operatorname{ord}_p(\lambda) \geq 0$. The only primes p to contribute to the product of Tamagawa numbers are the primes where C_λ and D_λ have split multiplicative reduction. For these primes the Weierstrass equations (2) and (3) are minimal and so $c_p = \operatorname{ord}_p(\Delta)$. By inspection of the discriminants (4) and (5) we find

$$c_p(D_\lambda)/c_p(C_\lambda) = \begin{cases} n & \text{if } p \in \mathcal{A} \\ n^{-1} & \text{if } p \in \mathcal{B}. \end{cases}$$

We write ω_C and ω_D for the Néron differentials on C_λ and D_λ respectively. Assuming $n \notin \mathcal{B}$, the Weierstrass equations (2) and (3) are both globally minimal. Since (3) was obtained from (2) using Vélu's formulae, it follows [V, Remarque 2] that $\omega_D = \widehat{\phi}^* \omega_C$. Thus

$$\Omega_D = \int_{D_\lambda(\mathbf{R})} \omega_D = \int_{D_\lambda(\mathbf{R})} \widehat{\phi}^* \omega_C = \int_{\widehat{\phi} D_\lambda(\mathbf{R})} \omega_C = n \int_{C_\lambda(\mathbf{R})} \omega_C = n \Omega_C$$

where $\widehat{\phi} : D_\lambda(\mathbf{R}) \to C_\lambda(\mathbf{R})$ is an n-fold cover. If $n \in \mathcal{B}$ then the Weierstrass equation (3) is no longer minimal at $p = n$. We then find $\omega_D = n^{-1} \widehat{\phi}^* \omega_C$ and $\Omega_D = \Omega_C$. Finally the RHS of (33) is

$$\frac{1}{n} \times \frac{\Omega_D}{\Omega_C} \times \prod_p \frac{c_p(D_\lambda)}{c_p(C_\lambda)} = n^{|\mathcal{A}|-|\mathcal{B}|}$$

and the formula is verified. This verification could equally be viewed as giving an alternative proof of the last part of Theorem 1.

3.5. Tables of examples

We apply Theorem 1 for some values $\lambda \in \mathbf{Q}$ chosen such that the elliptic curves C_λ and D_λ have conductor $N \leq 5300$. The list of curves considered is extracted from Cremona's tables [Cr3] by searching for curves with rational torsion of order 5, 7 or 10. We recall that Cremona lists the curves by conductor, with a letter to distinguish isogeny classes with the same conductor, and a number to distinguish curves within each isogeny class. The quantities we tabulate are the conductor N, the Cremona labels #, the sets of primes $\mathcal{A}$ and $\mathcal{B}$, the rank of the pairing Ξ, the dimensions of the Selmer groups $S^{(\phi)}(C_\lambda/\mathbf{Q})$ and $S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q})$ and our estimate $r_\phi = |\mathcal{A}| + |\mathcal{B}| - 1 - 2\operatorname{rank}(\Xi)$ for the rank. Finally we compare with $r = \operatorname{rank} D_\lambda(\mathbf{Q})$ taken directly from Cremona's tables. Whenever the columns r_ϕ and r differ, we deduce that there are elements of order n in the Tate-Shafarevich group. We thus arrive at the lists of curves cited in the introduction.

Table 1. ($n = 5$) Descent via $\phi : C_\lambda \to D_\lambda$ over $\mathbf{Q}$

λ	N	#	$\mathcal{A}$	$\mathcal{B}$	Ξ	ϕ	$\widehat{\phi}$	r_ϕ	r
1	11	A1, 3	∅	{11}	0	0	1	0	0
11	11	A2, 1	{11}	∅	0	1	0	0	0
2	38	B2, 1	{2}	∅	0	1	0	0	0
−2	50	B3, 1	{2}	∅	0	1	0	0	0
8	50	B4, 2	{2}	∅	0	1	0	0	0
9	57	C2, 1	{3}	∅	0	1	0	0	0
4	58	B2, 1	{2}	∅	0	1	0	0	0
12	66	C3, 1	{2, 3}	{11}	1	1	0	0	0
9/2	66	C4, 2	{2, 3}	{11}	1	1	0	0	0
3	75	C2, 1	{3}	∅	0	1	0	0	0
10	110	A2, 1	{2, 5}	{11}	1	1	0	0	0
−4	118	B2, 1	{2}	∅	0	1	0	0	0
−3	123	A2, 1	{3}	{41}	0	1	1	1	1
4/3	150	A1, 3	{2, 3}	{5}	1	1	0	0	0
18	150	A2, 4	{2, 3}	{5}	1	1	0	0	0
5	155	A2, 1	{5}	{31}	0	1	1	1	1
16	158	C2, 1	{2}	∅	0	1	0	0	0
−7	175	A1, 2	{7}	{5}	0	1	1	1	1
6	186	B2, 1	{2, 3}	{31}	1	1	0	0	0
7	203	A2, 1	{7}	∅	0	1	0	0	0
32/3	246	B2, 1	{2, 3}	{41}	1	1	0	0	0
13/2	286	D2, 1	{2, 13}	{11}	1	1	0	0	0
−8	302	A2, 1	{2}	{151}	0	1	1	1	1
13	325	E2, 1	{13}	∅	0	1	0	0	0
3/2	366	B2, 1	{2, 3}	{61}	1	1	0	0	0
−5	395	C2, 1	{5}	∅	0	1	0	0	0
−3/2	426	A2, 1	{2, 3}	{71}	1	1	0	0	0
−9	537	E2, 1	{3}	∅	0	1	0	0	0
11/2	550	K1, 2	{2, 11}	{5}	1	1	0	0	0
−32	550	K2, 3	{2}	{5, 11}	1	0	1	0	0
48/5	570	L3, 1	{2, 3, 5}	∅	0	3	0	2	0
100/9	570	L4, 2	{2, 3, 5}	∅	0	3	0	2	0
14	574	J2, 1	{2, 7}	{41}	1	1	0	0	0
−6	606	F2, 1	{2, 3}	{101}	1	1	0	0	0
7/5	665	D2, 1	{5, 7}	∅	0	2	0	1	1
25/2	710	D2, 1	{2, 5}	{71}	1	1	0	0	0
27/2	786	M2, 1	{2, 3}	{131}	1	1	0	0	0
−26	806	F2, 1	{2, 13}	{31}	1	1	0	0	0
−4/3	834	G2, 1	{2, 3}	∅	0	2	0	1	1
−16	862	E2, 1	{2}	{431}	0	1	1	1	1
45/4	870	I3, 1	{2, 3, 5}	∅	0	3	0	2	0
50/3	870	I4, 2	{2, 3, 5}	∅	0	3	0	2	0
23/2	874	E2, 1	{2, 23}	∅	0	2	0	1	1

λ	N	#	$\mathcal{A}$	$\mathcal{B}$	Ξ	ϕ	$\widehat{\phi}$	r_ϕ	r
15	885	D2, 1	{3, 5}	∅	0	2	0	1	1
5/2	890	G2, 1	{2, 5}	∅	0	2	0	1	1
21/2	1050	O2, 1	{2, 3, 7}	∅	0	3	0	2	0
37	1147	B2, 1	{37}	{31}	0	1	1	1	1
−15/7	1155	N2, 1	{3, 5, 7}	{11}	1	2	0	1	1
8/3	1254	K2, 1	{2, 3}	{11}	1	1	0	0	0
27	1293	E2, 1	{3}	{431}	0	1	1	1	1
−5/2	1310	C2, 1	{2, 5}	{131}	1	1	0	0	0
32	1342	C2, 1	{2}	{11, 61}	1	0	1	0	0
122/11	1342	C3, 2	{2, 11, 61}	∅	0	3	0	2	0
−17/3	1479	F2, 1	{3, 17}	∅	0	2	0	1	1
7/2	1526	E2, 1	{2, 7}	∅	0	2	0	1	1
32/13	1586	D2, 1	{2, 13}	{61}	1	1	0	0	0
−9/2	1650	R2, 1	{2, 3}	{11}	1	1	0	0	0
−12	1650	S2, 1	{2, 3}	{11}	1	1	0	0	0
16/3	1686	C2, 1	{2, 3}	{281}	1	1	0	0	0
17	1717	C2, 1	{17}	{101}	0	1	1	1	1
25	1745	E2, 1	{5}	∅	0	1	0	0	0
20	1790	D2, 1	{2, 5}	∅	0	2	0	1	1
24	1866	I2, 1	{2, 3}	{311}	1	1	0	0	0
−85/8	1870	H2, 1	{2, 5, 17}	{11}	1	2	0	1	1
−8/3	1914	O2, 1	{2, 3}	{11}	1	1	0	0	0
−54	1914	P2, 1	{2, 3}	{11}	1	1	0	0	0
−68/3	1938	J2, 1	{2, 3, 17}	∅	0	3	0	2	0
144/13	1950	Y2, 1	{2, 3, 13}	∅	0	3	0	2	0
9/4	1986	G2, 1	{2, 3}	{331}	1	1	0	0	0
−10	2090	N2, 1	{2, 5}	{11}	1	1	0	0	0
5/4	2110	E2, 1	{2, 5}	{211}	1	1	0	0	0
56/5	2170	Q2, 1	{2, 5, 7}	{31}	1	2	0	1	1
29/3	2175	J1, 2	{3, 29}	{5}	1	1	0	0	0
5/3	2235	F2, 1	{3, 5}	∅	0	2	0	1	1
−5/4	2290	D2, 1	{2, 5}	∅	0	2	0	1	1
19/2	2318	E2, 1	{2, 19}	{61}	1	1	0	0	0
47/4	2350	N1, 2	{2, 47}	{5}	1	1	0	0	0
54/5	2370	M2, 1	{2, 3, 5}	∅	0	3	0	2	0
34/3	2550	EE2, 1	{2, 3, 17}	∅	0	3	0	2	0
−11	2651	C2, 1	{11}	{241}	0	1	1	1	1
−5/3	2715	C2, 1	{3, 5}	{181}	1	1	0	0	0
−9/4	2766	I2, 1	{2, 3}	{461}	1	1	0	0	0
−7/2	2786	D2, 1	{2, 7}	∅	0	2	0	1	1
27/4	2850	W2, 1	{2, 3}	∅	0	2	0	1	1
19	2869	B2, 1	{19}	{151}	0	1	1	1	1
17/2	3026	D2, 1	{2, 17}	∅	0	2	0	1	1
−27	3075	L2, 1	{3}	{41}	0	1	1	1	1

λ	N	#	$\mathcal{A}$	$\mathcal{B}$	Ξ	ϕ	$\widehat{\phi}$	r_ϕ	r
−18	3126	C2, 1	{2, 3}	{521}	1	1	0	0	0
25/3	3135	H2, 1	{3, 5}	{11}	1	1	0	0	0
49/4	3206	E2, 1	{2, 7}	$\emptyset$	0	2	0	1	1
15/2	3270	H2, 1	{2, 3, 5}	$\emptyset$	0	3	0	2	0
101/9	3333	G2, 1	{3, 101}	{11}	1	1	0	0	0
92/7	3542	R2, 1	{2, 7, 23}	{11}	1	2	0	1	1
81/8	3786	G2, 1	{2, 3}	{631}	1	1	0	0	0
173/8	3806	K2, 1	{2, 173}	{11}	1	1	0	0	0
7/4	3850	T2, 1	{2, 7}	{11}	1	1	0	0	0
8/5	4010	E2, 1	{2, 5}	{401}	1	1	0	0	0
7/3	4011	D2, 1	{3, 7}	{191}	1	1	0	0	0
−13	4043	A2, 1	{13}	{311}	0	1	1	1	1
21	4389	K2, 1	{3, 7}	{11}	1	1	0	0	0
89/8	4450	K2, 1	{2, 89}	$\emptyset$	0	2	0	1	1
−25	4495	D2, 1	{5}	{31}	0	1	1	1	1
−16/3	4650	LL2, 1	{2, 3}	{31}	1	1	0	0	0
9/8	4650	PP2, 1	{2, 3}	{31}	1	1	0	0	0
−56	4774	J2, 1	{2, 7}	{11, 31}	1	1	1	1	1
−7/4	4774	K2, 1	{2, 7}	{11, 31}	1	1	1	1	1
−8/5	4790	C2, 1	{2, 5}	$\emptyset$	0	2	0	1	1
−9/8	4854	C2, 1	{2, 3}	$\emptyset$	0	2	0	1	1
−14	4886	F2, 1	{2, 7}	$\emptyset$	0	2	0	1	1
25/4	4910	G2, 1	{2, 5}	{491}	1	1	0	0	0
−24	5034	E2, 1	{2, 3}	$\emptyset$	0	2	0	1	1
43/4	5074	D2, 1	{2, 43}	$\emptyset$	0	2	0	1	1

Table 2. ($n = 7$) Descent via $\phi : C_\lambda \to D_\lambda$ over **Q**

λ	N	#	$\mathcal{A}$	$\mathcal{B}$	Ξ	ϕ	$\widehat{\phi}$	r_ϕ	r
2	26	B2, 1	{2}	$\emptyset$	0	1	0	0	0
3	174	B2, 1	{2, 3}	{29}	1	1	0	0	0
4	258	F2, 1	{2, 3}	{43}	1	1	0	0	0
−2	294	B1, 2	{2, 3}	{7}	1	1	0	0	0
5	490	K1, 2	{2, 5}	{7}	1	1	0	0	0
7	546	F2, 1	{2, 3, 7}	$\emptyset$	0	3	0	2	0
8	574	I2, 1	{2, 7}	$\emptyset$	0	2	0	1	1
−3	678	D2, 1	{2, 3}	{113}	1	1	0	0	0
9	762	G2, 1	{2, 3}	{127}	1	1	0	0	0
−9/2	858	K2, 1	{2, 3, 11}	$\emptyset$	0	3	0	2	0
6	1230	K2, 1	{2, 3, 5}	$\emptyset$	0	3	0	2	0
−4	2110	H2, 1	{2, 5}	{211}	1	1	0	0	0
−10	4730	K2, 1	{2, 5, 11}	{43}	1	2	0	1	1
5/2	5010	H2, 1	{2, 3, 5}	$\emptyset$	0	3	0	2	0

Acknowledgements. The author would like to thank his supervisor Nick Shepherd-Barron for his guidance in researching this topic; John Coates, John Cremona, Cathy O'Neil and Ed Schaefer for comments and suggestions along the way; and John Cremona in particular for the use of his computer program `mwrank`. Nearly all of this article is taken directly from the author's PhD thesis.

References

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

[Ca1] J.W.S. Cassels: Arithmetic on curves of genus 1, VI. The Tate-Shafarevich group can be arbitrarily large. J. Reine Angew. Math. **214/215**, 65–70 (1964)

[Ca2] J.W.S. Cassels: Arithmetic on curves of genus 1, VIII. On conjectures of Birch and Swinnerton-Dyer. J. Reine Angew. Math. **217**, 180–199 (1965)

[Ca3] J.W.S. Cassels: Lectures on elliptic curves. LMSST **24**: Cambridge University Press 1991

[CF] J.W.S. Cassels, A. Fröhlich (eds.): Algebraic number theory. Academic Press 1967

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

[CM] J.E. Cremona, B. Mazur: Visualizing elements in the Shafarevich-Tate group. Exp. Math. **9**(1), 13–28 (2000)

[Cr1] J.E. Cremona: Algorithms for modular elliptic curves (second edition). Cambridge University Press 1997

[Cr2] J.E. Cremona: `mwrank`, a program for 2-descent on elliptic curves over **Q**. See `http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs`

[Cr3] J.E. Cremona: Modular elliptic curve data for conductors up to 5300. See `http://www.maths.nottingham.ac.uk/personal/jec/ftp/data`

[F] T.A. Fisher: On 5 and 7 descents for elliptic curves. Cambridge PhD Thesis (2000)

[HR] H. Halberstam, H.-E. Richert: Sieve methods. LMS Monographs **4**: Academic Press 1974

[H] K. Hulek: Projective geometry of elliptic curves. Soc. Math. de France, Astérisque **137** (1986)

[Kl] F. Klein: Über die Transformation siebenter Ordnung der elliptischen Funktionen. Math. Ann. **14**, 428–471 (1879). English translation in [Le] 287–331

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

[Le] S. Levy (ed.): The eightfold way, the beauty of Klein's quartic curve. MSRI Publications **35**, Cambridge University Press 1999

[Lo] M. DeLong: A formula for the selmer group of a rational three-isogeny (1999)

[Ma1] B. Mazur: Arithmetic on curves. Bull. Am. Math. Soc. **14**, 207–259 (1986)

[Ma2] B. Mazur: On the passage from local to global in number theory. Bull. Am. Math. Soc. **29**, 14–50 (1993)

[Mi] J.S. Milne: Arithmetic duality theorems. Persp. in Math. **1**. Academic Press 1986

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

[Mu1] D. Mumford: On the equations defining abelian varieties. I. Invent. math. **1**, 287–354 (1966)

[Mu2] D. Mumford: Abelian varieties. TIFR Studies in Math. **5**: Oxford University Press 1970

[O'N] C.H. O'Neil: Jacobians of curves of genus one. Harvard PhD thesis (1999)

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

[Se1] J.-P. Serre: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. math. **15**, 259–331 (1972)

[Se2] J.-P. Serre: Local fields. GTM **67**. Springer 1979

[Si1] J.H. Silverman: The arithmetic of elliptic curves. GTM **106**. Springer 1986

[Si2] J.H. Silverman: Advanced topics in the arithmetic of elliptic curves. GTM **151**. Springer 1994

[T1] J. Tate: Duality theorems in Galois cohomology over number fields. Proc. Intern. Congress Math. Stockholm (1962), 288–295

[T2] J. Tate: The arithmetic of elliptic curves. Invent. math. **23**, 179–206 (1974)

[V] J. Vélu: Isogénies entre courbes elliptiques. C. R. Acad. Sci. Paris **273**, 238–241 (1971)