On 5 and 7 Descents for Elliptic Curves

Thomas Anthony Fisher
Clare College

A dissertation submitted for
the degree of Doctor of Philosophy
at the University of Cambridge

August 2000

Preface

This dissertation is not substantially the same as any I have submitted for a degree or diploma or other qualification at any other university. It is the result of my own work and includes nothing which is the outcome of work done in collaboration.

I acknowledge with gratitude the guidance of my research supervisor Nick Shepherd-Barron. I also thank John Coates, John Cremona and Cathy O'Neil for valuable conversations along the way, and Karl Rubin for bringing to my attention the work of Cheryl Beaver [Be]. I am indebted to John Cremona for the use of his computer program `mwrank`. I also wish to thank my fellow students Paul Hacking and Jan Wierzba for many mathematical conversations. Finally I acknowledge the financial support of the Engineering and Physical Sciences Research Council.

Clare College
August 2000

Summary

We perform descent calculations for the families of elliptic curves over $\mathbf{Q}$ 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 $\mathbf{Q}$ may become arbitrarily large.

In a special case, namely when the 5-torsion of our elliptic curve splits as $\boldsymbol{\mu}_5 \oplus \mathbf{Z}/5\mathbf{Z}$, we improve our estimate for the Mordell-Weil rank by using the Cassels-Tate pairing to perform a full 5-descent. We generalise our results to curves over $\mathbf{Q}(\boldsymbol{\mu}_n)$ and finally make some calculations for the curve $X_1(11)$ over its field of 5-division points.

Contents

0.1 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 $Ш(E/K)$. 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 $Ш(E/K)$ 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 $Ш(E/K)$ 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 $Ш(E/K)$. 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 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

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

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.

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

As explained in [Ca2], 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.

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

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 $D(\mathbf{Q}) \cong \mathbf{Z}/5\mathbf{Z}$. The formulae in Appendix C give equations for the quotient map

$$(x : y : 1) = (30x_0x_1x_4 : 30^2x_2x_4^2 : -x_0^3).$$

It is then easy to check $T(\mathbf{Q}) = \emptyset$.

The curve T corresponds to an element of order 5 in $Ш(C/\mathbf{Q})$ 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 [Cr] of elliptic curves of conductor $N \leq 5300$. We find the following examples of curves C with $Ш(C/\mathbf{Q})[5] \cong (\mathbf{Z}/5\mathbf{Z})^2$

> 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 $Ш(C/\mathbf{Q})[7] \cong (\mathbf{Z}/7\mathbf{Z})^2$

> 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 curves with positive Mordell-Weil rank.

The pairs of curves C and D are parametrised by the modular curve $Y_1(n) = X_1(n) \setminus \{\text{cusps}\}$. For $n = 5$ or 7 we have $X_1(n) \cong \mathbf{P}^1$. We fix a co-ordinate λ on $\mathbf{P}^1$, essentially by listing the cusps, and write C_λ and D_λ for the pairs of curves above λ. In §1.1 we give Weierstrass equations for these curves and describe their reduction types. In §1.2 we recall the notion of *torsor*, or *principal homogeneous space*, and outline the methods we use to construct torsors under C_λ. In §1.3 and §1.4 we include some background material on modular curves and duality theorems respectively.

In Chapter 2 we state our main descent theorems over $\mathbf{Q}$ and show how they may be used both to compute ranks of elliptic curves and to exhibit elements of the Tate-Shafarevich group. Theorem 1, stated in §2.1, gives an explicit recipe for descent via n-isogeny on the curves C_λ and D_λ over $\mathbf{Q}$ parametrised by $X_1(n)$. The idea is that λ determines sets of primes $\mathcal{A}$ and $\mathcal{B}$, and the Selmer groups sought appear as the left and right kernel of a

certain "reciprocity pairing" supported on these primes. We find that $\mathcal{A} \cup \mathcal{B}$ is precisely the set of primes with root number -1. Thus our estimates for the Mordell-Weil rank have the same parity as the analytic rank. This is a special case of a result of Monsky [Mo].

The elliptic curves E_τ over $\mathbf{Q}$ whose 5-torsion splits as $\boldsymbol{\mu}_5 \oplus \mathbf{Z}/5\mathbf{Z}$ are parametrised by the modular curve $X(5)$. For these curves we may perform two different descents via 5-isogeny. Applying Theorem 1 we show that the 5-torsion of the Tate-Shafarevich group of an elliptic curve over $\mathbf{Q}$ may become arbitrarily large. Corresponding results for $n = 2$ and $n = 3$ have been established by Cassels [Ca1], Bölling [Bö] and Kramer [Kr]. Our method does not extend to $n = 7$ since there are no elliptic curves over $\mathbf{Q}$ whose 7-torsion splits as $\boldsymbol{\mu}_7 \oplus \mathbf{Z}/7\mathbf{Z}$. The best result we can give is that the 7-Selmer group may become arbitrarily large.

Theorem 2, stated in §2.4, gives an explicit recipe for (full) 5-descent on the curves E_τ over $\mathbf{Q}$ parametrised by $X(5)$. The idea is that we combine Theorem 1 with the work of Beaver [Be] on the Cassels-Tate pairing. We call Theorems 1 and 2 the first and second descent theorems respectively. A common theme is that the curves considered are parametrised by a modular curve, and we partition the primes of bad reduction by asking to which cusp our point on the modular curve reduces.

In Chapter 3 we prove the first descent theorem (Theorem 1). We begin by using the diagonal action of $\boldsymbol{\mu}_n$ to help write down explicit equations for torsors in $\mathbf{P}^{n-1}$. An understanding of the geometry of these curves leads to simple criteria for local solubility. We perform some further Hensel lemma calculations to treat the prime n itself, and then complete our proof of Theorem 1 by writing down the "reciprocity pairing" referred to above as a sum of local Tate pairings.

In Chapter 4 we discuss the geometric results required for the proof of our descent theorems. We work over an algebraically closed field and give equations in $\mathbf{P}^{n-1}$ for the elliptic curves parametrised by $X(n)$. In §4.3 we relate these equations to the torsors written down in §3.1. This gives us a handle on the geometry of the latter. The case $\mathrm{char}(K) = n$ is left to the end of the chapter.

In Chapter 5 we generalise our first descent theorem to $K = \mathbf{Q}(\boldsymbol{\mu}_n)$. One reason for doing this is that an alternative, and perhaps more natural, proof of Theorem 1 is given by working over K and then descending back to $\mathbf{Q}$. We give the details in §5.4. Although working over a field containing the nth roots of unity makes certain aspects of our proof simpler, we find that rather delicate arguments are required to establish conditions for local solubility at

the prime above n. It turns out that our calculations are just what is required to give some interesting examples from the point of view of Iwasawa theory. We refer to [CS] for details.

In Chapter 6 we explain how the second descent theorem (Theorem 2) follows from our descent calculations and those of Beaver [Be]. Beaver works with the Tate parametrisation and therefore finds it necessary to make an assumption on the reduction type at 5. We remove this assumption and give a much more explicit description of the "switching exponents". For these reasons we include rather full details.

In Chapter 7 we apply some of our methods to the elliptic curves over $\mathbf{Q}$ with conductor 11. From the point of view of Iwasawa theory there is some interest in the behaviour of the Mordell-Weil rank as we pass up various towers of number fields. For instance, the curves of conductor 11 are known to have rank 0 over $\mathbf{Q}(\boldsymbol{\mu}_{5^\infty})$. Another natural tower to consider is that defined by the 5-power division points of the curves themselves. As a first step in this direction we show that the rank is 0 over the field of 5-division points for $X_1(11)$.

In Appendix A we relate the geometrical results in Chapter 4 to the work of Buchsbaum and Eisenbud [BE] on varieties defined by Pfaffians. In Appendix B we discuss the problem of extending our descent calculations to pairs of n-isogenous curves without the assumption that one of these curves has a rational point of order n. In Appendix C we give some explicit formulae which, although not required for our descent theorems, may be of some interest for the study of specific examples. In Appendix D we illustrate our descent theorems by giving tables of examples.

Let us make two remarks that may help the reader. Firstly, as the title of this thesis indicates, we often treat the cases $n = 5$ and $n = 7$ concurrently. It then become 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 §2.2 we make use of `mwrank` to compute ranks of elliptic curves over $\mathbf{Q}$ via 2-descent, and in §7.1 we use `pari` to compute the unit group and class group of a certain number field of degree 20.

0.2 Notation

We summarise here some of our basic notation.

We work over a perfect field K and write $\overline{K}$ for the algebraic closure. We write $G_K = \mathrm{Gal}(\overline{K}/K)$ for the absolute Galois group and $H^1(K, -)$ for the Galois cohomology group $H^1(G_K, -)$. Assuming $\mathrm{char}(K) \nmid n$ we write $\boldsymbol{\mu}_n \subset \overline{K}$ for the nth roots of unity and fix $\zeta = \zeta_n$ a generator. For M a finite G_K-module we write $M^\vee$ for the Cartier dual $\mathrm{Hom}(M, \mathbf{G}_m)$.

Frequently we take K a number field and write $\mathcal{O}_K$, U_K and I_K for the ring of integers, unit group and group of fractional ideals respectively. For v a place of K we write K_v for the completion in the v-adic topology. Whenever necessary we fix embeddings $\overline{K} \hookrightarrow \overline{K}_v$ and so identify $G_v = \mathrm{Gal}(\overline{K}_v/K_v)$ as a subgroup of G_K. We reserve the term *prime* for $\mathfrak{p}$ a finite place, writing $\mathrm{ord}_\mathfrak{p} : K_\mathfrak{p}^\times \to \mathbf{Z}$ for the normalised valuation and $\mathcal{O}_\mathfrak{p}$ for the ring of $\mathfrak{p}$-adic integers.

An elliptic curve E/K is a smooth projective curve of genus 1, equipped with a specified rational point $0 \in E(K)$ taken as identity element for the group law. For n an integer we write $[n] : E \to E$ for the multiplication by n map. For $P \in E$ we write τ_P for the map "translation by P". For $\phi : E \to E'$ an isogeny of degree n we write $E[\phi]$ for its kernel, $\widehat{\phi} : E' \to E$ for the dual isogeny and $e_\phi : E[\phi] \times E'[\widehat{\phi}] \to \boldsymbol{\mu}_n$ for the Weil pairing as defined in [Si1, Exercise 3.15].

The cardinality of a set S is denoted either $|S|$ or $\#S$. For A an abelian group we write $A[n]$ for the n-torsion, and if n is prime write $A(n)$ for the n-power torsion. Given elements $a, b, \ldots$ belonging to A we write $\langle a, b, \ldots \rangle$ for the subgroup they generate. For R a ring we write R^+ for the underlying additive group, and $R^\times$ for the group of invertible elements under multiplication. The dual of a vector space V is denoted V^*. For Ξ a pairing on vector spaces V and W we write $\ker_L(\Xi) \subset V$ and $\ker_R(\Xi) \subset W$ for the left and right kernels of Ξ. For $v = (v_i)_{i=1}^n$ a vector of length n we write $\mathrm{Diag}(v)$ for the $n \times n$ diagonal matrix with entries v_i down the diagonal. The trivial group shall always be denoted 0.

Chapter 1

Preliminaries

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

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

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

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

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

Vélu's formulae [V1] tell us that C_λ has Weierstrass equation

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

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

$$\begin{array}{ll} n=5 & \Delta(C_\lambda) = \lambda(\lambda^2 - 11\lambda - 1)^5 \\ & \Delta(D_\lambda) = \lambda^5(\lambda^2 - 11\lambda - 1) \\ n=7 & \Delta(C_\lambda) = \lambda(\lambda-1)(\lambda^3 - 8\lambda^2 + 5\lambda + 1)^7 \\ & \Delta(D_\lambda) = \lambda^7(\lambda-1)^7(\lambda^3 - 8\lambda^2 + 5\lambda + 1). \end{array}$$

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.

Lemma 1.3 *Let K be a number field and let $\mathfrak{p}$ be a prime with $\mathfrak{p} \nmid n$. Then for $\lambda \in K_\mathfrak{p}$ the curves $C_\lambda/K_\mathfrak{p}$ and $D_\lambda/K_\mathfrak{p}$ have either good or multiplicative reduction.*

Proof. It suffices to show that if an elliptic curve $E/K_\mathfrak{p}$ has additive reduction then $E(K_\mathfrak{p})[n] = 0$. We consider the filtration $E(K_\mathfrak{p}) \supset E_0(K_\mathfrak{p}) \supset E_1(K_\mathfrak{p})$ as described in [Si1, Chapter VII]. By the theory of formal groups the multiplication by n map on $E_1(K_\mathfrak{p})$ is invertible. The additive reduction tells us $E_0(K_\mathfrak{p})/E_1(K_\mathfrak{p}) \cong (\mathcal{O}_K/\mathfrak{p})^+$ and the Tamagawa number $[E(K_\mathfrak{p}) : E_0(K_\mathfrak{p})]$ is at most 4. The lemma follows. □

To learn more about the reduction types we work directly with the Weierstrass equation (2). Applying Tate's algorithm, as described in [Si2] for example, we find

Lemma 1.4 *Let K be a number field and let $\mathfrak{p}$ be a prime with $\mathfrak{p} \nmid n$. Then for $\lambda \in K_\mathfrak{p}$ with $\mathrm{ord}_\mathfrak{p}(\lambda) \geq 0$ the Weierstrass equation (2) is 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 $N\mathfrak{p} \equiv 1 \pmod{n}$.
(iii) In the remaining cases C_λ and D_λ have good reduction.

The assumption $\mathrm{ord}_\mathfrak{p}(\lambda) \geq 0$ 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. In the case $K = \mathbf{Q}$ the Weierstrass equation (2) is still minimal and the reduction is additive.

We set up some notation to treat the case $K = \mathbf{Q}(\boldsymbol{\mu}_n)$. Let $\mathfrak{l} = (1-\zeta)$ be the unique prime of K above n. For $\lambda \in K_{\mathfrak{l}}$ we define

$$c(\lambda) = \min\{\, \mathrm{ord}_{\mathfrak{l}}(\lambda - u) \mid u \text{ an irrational cusp} \,\}$$

if λ reduces to an irrational cusp, and $c(\lambda) = 0$ otherwise. We write $c_{\max}$ for $\mathrm{ord}_{\mathfrak{l}}(u - v)$ where u and v are distinct irrational cusps.

Lemma 1.5 *The cusp number $c(\lambda)$ satisfies*
(i) $0 \le c(\lambda) \le c_{\max}$
(ii) $c(\lambda) = c(-1/\lambda)$, *respectively* $c(\lambda) = c((\lambda-1)/\lambda)$
(iii) $c(\lambda) + c(\eta(\lambda)) = c_{\max}$.

Proof. (i) and (ii) Straightforward.
(iii) We have $\eta(\lambda) = u(\lambda - v)/(\lambda - u)$ for suitable cusps u and v. Then

$$(\lambda - u)(\eta(\lambda) - u) = u(u - v)$$

and since u is a unit we deduce $c(\lambda) + c(\eta(\lambda)) = c_{\max}$ as required. □

To find the value of $c_{\max}$ it suffices to compute some discriminants

$$\begin{array}{lll} n = 5 & \Delta(\lambda^2 - 11\lambda - 1) = 5^3 & \Longrightarrow \quad c_{\max} = 6 \\ n = 7 & \Delta(\lambda^3 - 8\lambda^2 + 5\lambda + 1) = 7^4 & \Longrightarrow \quad c_{\max} = 4. \end{array}$$

Lemma 1.6 *Let $K = \mathbf{Q}(\boldsymbol{\mu}_n)$. Let $\lambda \in K_{\mathfrak{l}}$ with $c(\lambda)$ as defined above.*
(i) If λ or $\eta(\lambda)$ reduces to a rational cusp then C_λ and D_λ have split multiplicative reduction. In this case $c(\lambda) = 0$ or $c(\lambda) = c_{\max}$.
(ii) If $0 < c(\lambda) < c_{\max}$ then C_λ and D_λ have additive potential good supersingular reduction.
(iii) In the remaining cases C_λ and D_λ have good ordinary reduction.

Proof. As usual we may assume $\mathrm{ord}_{\mathfrak{l}}(\lambda) \ge 0$. If $c(\lambda) < c_{\max}$ then

$$\begin{array}{ll} n = 5 & \mathrm{ord}_{\mathfrak{l}}(\lambda^2 - 11\lambda - 1) < 2c_{\max} = 12 \\ n = 7 & \mathrm{ord}_{\mathfrak{l}}(\lambda^3 - 8\lambda^2 + 5\lambda + 1) < 3c_{\max} = 12. \end{array}$$

So in this case the Weierstrass equation (2) is minimal and the reduction types may be checked via computer algebra as before. Since $C_\lambda \cong D_{\eta(\lambda)}$ the general case follows by Lemma 1.5(iii).

It only remains to prove the statements concerning ordinary versus supersingular reduction. In case (iii) we may explicitly list the points $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda$ and so learn that the reduction is ordinary. In case (ii) some rather messy calculations, the details of which we omit, show that $\mathrm{ord}_\mathfrak{l}(j) > 0$, respectively $\mathrm{ord}_\mathfrak{l}(j-1728) > 0$. We recall [Ha, IV.4.23] that the supersingular j-invariants in characteristic 5 and 7 are 0 and 1728 respectively. Thus we have potential good supersingular reduction as claimed. □

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 the Galois cohomology group $H^1(K, \mathrm{Aut}(X))$.

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

$$0 \to \{\text{translations } \tau_P\} \to \mathrm{Aut}(E) \to \mathrm{Aut}(E, 0) \to 0 \tag{4}$$

where $\mathrm{Aut}(E)$ and $\mathrm{Aut}(E, 0)$ are the automorphism groups of E as a curve and as a group variety respectively. The translations make up the identity component of $\mathrm{Aut}(E)$ and may be characterised as the automorphisms without fixed points. More importantly for us they 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 $\mathrm{Aut}(E)$. 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.

Let $\phi : E \to E'$ be an isogeny defined over K. There is an exact sequence of Galois modules

$$0 \to E[\phi] \to E \to E' \to 0.$$

Taking Galois cohomology yields

$$0 \to E'(K)/\phi E(K) \to H^1(K, E[\phi]) \to \mathrm{WC}(E/K)[\phi] \to 0. \tag{5}$$

If T is a torsor under E corresponding to $\xi_T \in \mathrm{WC}(E/K)[\phi]$ then by (5) the isomorphism $\psi : T \xrightarrow{\sim} E$ may be chosen such that the cocycle $\sigma \mapsto \sigma(\psi)\psi^{-1}$ takes values in $E[\phi]$. The Selmer group attached to the isogeny ϕ is

$$S^{(\phi)}(E/K) := \ker\bigl(H^1(K, E[\phi]) \to \textstyle\prod_v \mathrm{WC}(E/K_v)\bigr).$$

It consists of those classes in $H^1(K, E[\phi])$ which describe torsors under E with points everywhere locally. The exact sequence (5) now becomes

$$0 \to E'(K)/\phi E(K) \to S^{(\phi)}(E/K) \to Ш(E/K)[\phi] \to 0. \tag{6}$$

Thus the Selmer group $S^{(\phi)}(E/K)$ contains information about both the Mordell-Weil group $E(K)$ and the Tate-Shafarevich group $Ш(E/K)$. The aim of this thesis is to present some examples where $S^{(\phi)}(E/K)$ may be computed rather explicitly. Such calculations are referred to as descent calculations, since knowledge of $E'(K)/\phi E(K)$ and $E(K)/\widehat{\phi}E'(K)$ enables one to compute the group $E(K)$ via Fermat's method of descent.

We now take $n = 5$ or 7 and consider the curves C_λ and D_λ introduced in §1.1. The exact sequence (5) becomes

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

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 $\theta \in K^\times/(K^\times)^n$. Since n is odd we may ignore the infinite places, so by definition

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

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 $\zeta \in \boldsymbol{\mu}_n$.

Lemma 1.7 *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*

$$0 \to \boldsymbol{\mu}_n(K) \to C_\lambda(K) \xrightarrow{\phi} D_\lambda(K) \xrightarrow{\delta} K^\times/(K^\times)^n \tag{9}$$

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

Proof. Pick $P' \in C_\lambda$ with $\phi(P') = P$. Then for $\sigma \in G_K$ 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

$$\begin{array}{ll} n = 5 & f(x,y) = xy + y - x^2 \\ n = 7 & f(x,y) = (\lambda+1)x^3 - x^2y + \lambda^2x^2 - (2\lambda+1)xy - \lambda^2 y. \end{array} \tag{10}$$

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

$$\left\{ \begin{array}{c} f(x,y) = \theta z^n \\ (x,y) \in D_\lambda \end{array} \right\} \subset \mathbf{A}^2 \times \mathbf{G}_m. \tag{11}$$

Remark 1.8 According to our table, the image of $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda(K)$ under δ is generated by $\alpha(\lambda) := \lambda$, respectively $\lambda^4(\lambda-1)$. It is clear from the exact sequence (9) that $\alpha(\lambda)$ is a Kummer generator for the field extension $K(C_\lambda[n])/K(\boldsymbol{\mu}_n)$. In §1.3 we explain how we may use $\alpha(\lambda)$ to construct $X(n)$ from $X_1(n)$.

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

$$D \sim 0 \iff \deg D = 0 \text{ and } \operatorname{sum} D = 0. \tag{12}$$

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

$$\zeta \mapsto \mathrm{Diag}(1 : \zeta : \ldots : \zeta^{n-1}). \tag{13}$$

Thus the torsors $C_{\lambda,\theta}$ all arise as smooth curves of genus 1, degree n in $\mathbf{P}^{n-1}$ invariant under (13). In §3.1 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 (13). 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 1.9 The action (13) 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 1.10 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 The Modular Curves $X_1(n)$ and $X(n)$

In this section we recall the definitions of the modular curves $X_1(n)$ and $X(n)$ and record some of their most basic properties.

Definition 1.11 *Let $n \geq 4$. The pairs (E, P) where E is an elliptic curve and $P \in E[n]$ is a point of order n, are parametrised by the smooth curve $Y_1(n) \to \mathrm{Spec}\, \mathbf{Z}[1/n]$.*

Definition 1.12 *Let $n \geq 3$. The triples (E, i, Q) where E is an elliptic curve, $i : \boldsymbol{\mu}_n \hookrightarrow E$, $Q \in E[n]$ and $e_n(i(\zeta), Q) = \zeta$ for $\zeta \in \boldsymbol{\mu}_n$, are parametrised by the smooth curve $Y(n) \to \mathrm{Spec}\, \mathbf{Z}[1/n]$.*

We write $X_1(n)$ and $X(n)$ for the smooth projective curves containing as an open subset $Y_1(n)$ and $Y(n)$ respectively. For a proof of the existence of these moduli spaces, and the interpretation of $X_1(n)$ and $X(n)$ in terms of a moduli problem, we refer to [DR, Chapter IV]. We note that our restrictions on n are those required for the objects parametrised to have no automorphisms.

For simplicity we work over a field K with $\mathrm{char}(K) \nmid n$. We do *not* assume $\boldsymbol{\mu}_n \subset K$. The relationship between $X(n)$ and $X_1(n)$ is as follows. There is an action of $\boldsymbol{\mu}_n$ on $X(n)$ given by

$$\zeta : (E, i, Q) \mapsto (E, i, Q + i(\zeta)) \tag{14}$$

with quotient $X_1(n)$. In terms of function fields the map $X(n) \to X_1(n)$ is a Kummer extension of degree n. Taking $\alpha : X_1(n) \to \mathbf{P}^1$ a Kummer generator

we see $X(n)$ has affine model

$$\{(\lambda, \tau) \in X_1(n) \times \mathbf{G}_m : \alpha(\lambda) = \tau^n\}. \tag{15}$$

In §1.1 we gave a construction of the curve $X_1(n)$, and in §1.2 we computed the rational function α in the cases $n = 5$ and 7. This gives one possible construction of the modular curve $X(n)$.

In Chapter 4 we discuss another construction of $X(n)$. We work over an algebraically closed field so that $Y(n)$ may be simply described as parametrising the triples (E, P, Q) with $P, Q \in E[n]$ and $e_n(P, Q) = \zeta_n$. There is no difficulty extending our calculations to a non-algebraically closed field, but we prefer not to carry round the notation required. We define an action of $\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z})$ on $X(n)$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : (E, P, Q) \mapsto (E, aP + cQ, bP + dQ). \tag{16}$$

The quotient by this action is the j-map $j : X_1(n) \to \mathbf{P}^1$. From the analytic theory we know that the j-map is ramified at 0, 1728 and ∞ with stabilisers of order 3, 2 and n respectively. We arrive at the classical formulae

$$\begin{aligned} \#\text{ cusps on } X(n) &= (1/n)\,\#\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z}) \\ \text{genus } X(n) &= (n-6)/(12n)\,\#\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z}) + 1 \end{aligned} \tag{17}$$

where for $n \geq 3$ we recall $\#\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z}) = (n^3/2)\prod_{p|n}(1 - 1/p^2)$.

We describe $X(n)$ for some small values of n. For $n = 3, 4, 5$ the cusps are arranged as the vertices of one of the Platonic solids. The curve $X(7)$ is the Klein quartic [K1] whose automorphism group is the simple group of order 168.

n	$X(n)$	$\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z})$	cusps
3	$\mathbf{P}^1$	A_4	tetrahedron
4	$\mathbf{P}^1$	S_4	octrahedron
5	$\mathbf{P}^1$	A_5	icosahedron
6	$\{y^2 = x^3 + 1\}$	$S_3 \times A_4$	$E[1-\omega] \oplus E[2]$
7	$\{a^3b + b^3c + c^3a = 0\}$	G_{168}	points of inflection
$\vdots$	$\vdots$	$\vdots$	$\vdots$

For p a prime we record the formulae

$$\begin{aligned} \text{genus } X(p) &= (p+2)(p-3)(p-5)/24 \\ \text{genus } X_1(p) &= (p-5)(p-7)/24. \end{aligned} \tag{18}$$

1.4 Tate Local Duality and Reciprocity Laws

In this section we review some results from class field theory and arithmetic duality theory. References for this are [CF], [Se2] and [Mi].

Local Results.
Let K be a finite extension of $\mathbf{Q}_p$. We write $\mathrm{ord} : K^\times \to \mathbf{Z}$ for the normalised valuation and k for the residue field.

Let M be a finite G_K-module and let A be an abelian variety over K. We write $M^\vee$ for the Cartier dual $\mathrm{Hom}(M, \mathbf{G}_m)$ and $A^\vee$ for the dual abelian variety $\mathrm{Ext}^1(A, \mathbf{G}_m)$. We recall from [Mi] that there are naturally defined pairings

$$H^r(K, M^\vee) \times H^{2-r}(K, M) \to \mathbf{Q}/\mathbf{Z} \tag{19}$$
$$H^r(K, A^\vee) \times H^{1-r}(K, A) \to \mathbf{Q}/\mathbf{Z}. \tag{20}$$

Theorems 2.1 and 2.3 in [T1] state that (19) and (20) are non-degenerate for all r. One way to define (19) is as the pairing induced by cup product from $M^\vee \times M \to \mathbf{G}_m$ composed with the isomorphism $\mathrm{Br}(K) \stackrel{\mathrm{inv}}{\to} \mathbf{Q}/\mathbf{Z}$. We discuss three examples with $r = 1$.

Example I Let $M = \mathbf{Z}/n\mathbf{Z}$. Then (19) becomes

$$(\cdot, \cdot) : H^1(K, \boldsymbol{\mu}_n) \times H^1(K, \mathbf{Z}/n\mathbf{Z}) \to \mathbf{Z}/n\mathbf{Z}. \tag{21}$$

We identify $H^1(K, \boldsymbol{\mu}_n) = K^\times/(K^\times)^n$ and $H^1(K, \mathbf{Z}/n\mathbf{Z}) = \mathrm{Hom}(G_K, \mathbf{Z}/n\mathbf{Z})$.

Lemma 1.13 *For $a \in K^\times/(K^\times)^n$ and $\chi \in \mathrm{Hom}(G_K, \mathbf{Z}/n\mathbf{Z})$*

$$(a, \chi) = -\chi(\rho_K(a))$$

where $\rho_K : K^\times \to G_K^{\mathrm{ab}}$ is the local reciprocity map.

Proof. See [Se2, Chapter XIV]. Notice that we do *not* assume $\boldsymbol{\mu}_n \subset K$. □

Lemma 1.14 *Let L/K be an unramified abelian extension of local fields and write $\mathrm{Frob}(L/K) \in \mathrm{Gal}(L/K)$ for the Frobenius element. Then*

$$\rho_{L/K}(a) = \mathrm{Frob}(L/K)^{\mathrm{ord}(a)}$$

where $\rho_{L/K} : K^\times \to \mathrm{Gal}(L/K)$ is the local reciprocity map.

Proof. [CF, Chapter VI, §2.5]. □

We write $\mathfrak{I}_K \subset G_K$ for the inertia subgroup.

Proposition 1.15 *The "unit" and "not ramified" subgroups*

$$\begin{aligned} H^1_{\mathrm{un}}(K, \boldsymbol{\mu}_n) &:= \{\, a \in K^\times/(K^\times)^n \mid \mathrm{ord}(a) \equiv 0 \pmod{n} \,\} \\ H^1_{\mathrm{nr}}(K, \mathbf{Z}/n\mathbf{Z}) &:= \mathrm{Hom}(G_K/\mathfrak{I}_K, \mathbf{Z}/n\mathbf{Z}) \end{aligned}$$

are exact annihilators with respect to the Tate pairing (21).

Proof. Let $a \in K^\times/(K^\times)^n$ and $\chi \in \mathrm{Hom}(G_K/\mathfrak{I}_K, \mathbf{Z}/n\mathbf{Z})$. Then χ factors through $\mathrm{Gal}(L/K)$ where L/K is an unramified extension. The last two lemmas tell us

$$(a, \chi) = -\,\mathrm{ord}(a)\,\chi(\mathrm{Frob}(L/K)).$$

Thus $H^1_{\mathrm{un}}(K, \boldsymbol{\mu}_n)$ is the exact annihilator of $H^1_{\mathrm{nr}}(K, \mathbf{Z}/n\mathbf{Z})$. □

Remark 1.16 More generally for B a G_K-module it is usual to define

$$H^1_{\mathrm{nr}}(K, B) := H^1(G_K/\mathfrak{I}_K, B^{\mathfrak{I}_K}) = \ker\big(H^1(G_K, B) \xrightarrow{\mathrm{res}} H^1(\mathfrak{I}_K, B)\big).$$

If $\mathrm{char}(k) \nmid n$ then the groups $H^1_{\mathrm{un}}(K, \boldsymbol{\mu}_n)$ and $H^1_{\mathrm{nr}}(K, \boldsymbol{\mu}_n)$ are identical.

Example II Let $\phi : C \to D$ be an isogeny of elliptic curves defined over K with $\deg \phi = n$. The Weil pairing $e_\phi : C[\phi] \times D[\widehat{\phi}] \to \boldsymbol{\mu}_n$ induces a non-degenerate pairing

$$(\cdot, \cdot) : H^1(K, C[\phi]) \times H^1(K, D[\widehat{\phi}]) \to \mathbf{Z}/n\mathbf{Z}. \tag{22}$$

Proposition 1.17 *The images of the connecting maps*

$$\delta_\phi : D(K) \to H^1(K, C[\phi]) \quad \textit{and} \quad \delta_{\widehat{\phi}} : C(K) \to H^1(K, D[\widehat{\phi}])$$

are exact annihilators with respect to the Tate pairing (22).

Proof. The pairings (19) and (20) yield the following commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & D(K)/\phi C(K) & \xrightarrow{\delta_\phi} & H^1(K, C[\phi]) & \longrightarrow & H^1(K, C)[\phi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H^1(K, D)[\widehat{\phi}]^* & \longrightarrow & H^1(K, D[\widehat{\phi}])^* & \xrightarrow{\delta_{\widehat{\phi}}^*} & (C(K)/\widehat{\phi} D(K))^* & \longrightarrow & 0 \end{array}$$

Since the vertical maps are isomorphisms the exact annihilation is nothing more than the statement that the rows are exact. □

Remark 1.18 The non-degeneracy of the pairing (20) is in fact proved from the non-degeneracy of (19) by considering the above diagram in the case $\phi = \widehat{\phi} = [n]$ and employing some counting arguments.

Example III Assume $\boldsymbol{\mu}_n \subset K$. We fix a choice of isomorphism $\mathbf{Z}/n\mathbf{Z} \cong \boldsymbol{\mu}_n$. Then the pairing (21) becomes the Hilbert norm residue symbol

$$(\cdot,\cdot) : K^\times/(K^\times)^n \times K^\times/(K^\times)^n \to \boldsymbol{\mu}_n.$$

This pairing is skew-symmetric. By Lemma 1.13 an equivalent definition is

$$\rho_K(b)\sqrt[n]{a} = (a,b)\sqrt[n]{a}. \tag{23}$$

In particular the norm residue symbol does not depend upon our choice of isomorphism $\mathbf{Z}/n\mathbf{Z} \cong \boldsymbol{\mu}_n$.

Global Results.
Let L/K be a finite abelian extension of number fields. Let $\mathcal{S}$ be the set of primes ramifying in L/K. For $\mathfrak{p} \notin \mathcal{S}$ we write $(\mathfrak{p}, L/K)$ for the Frobenius element in $\mathrm{Gal}(L/K)$. Extending linearly gives the global reciprocity map

$$(\,\cdot\,, L/K) : I_K^{\mathcal{S}} \to \mathrm{Gal}(L/K).$$

Assuming $\boldsymbol{\mu}_n \subset K$ we define the power residue symbol $(a/b) \in \boldsymbol{\mu}_n$ via

$$(b, K(\sqrt[n]{a})/K)\sqrt[n]{a} = (a/b)\sqrt[n]{a} \tag{24}$$

where $a, b \in K^\times$ and $\mathrm{ord}_{\mathfrak{p}}(b) = 0$ for all $\mathfrak{p}$ ramifying in $K(\sqrt[n]{a})/K$. Thus $(a/\mathfrak{p}) = 1$ if and only if $a \in (K_{\mathfrak{p}}^\times)^n$. The aim of the nth power reciprocity law is to relate the symbols (a/b) and (b/a). The next two lemmas indicate how this may be achieved using the local Hilbert norm residue symbols $(\cdot,\cdot)_{\mathfrak{p}}$.

Lemma 1.19 *Whenever the symbol (a/b) is defined we have*

$$(a/b) \;=\; \textstyle\prod_{\mathfrak{p}\in\mathcal{B}}(a,b)_{\mathfrak{p}}$$

where $\mathcal{B}$ is any set of primes unramified in $K(\sqrt[n]{a})/K$ and containing all primes $\mathfrak{p}$ with $\mathrm{ord}_{\mathfrak{p}}(b) \neq 0$.

Proof. We compare (23) and (24) using Lemma 1.14. □

Lemma 1.20 *Let $a, b \in K^\times$ and assume $n > 2$. Then*

$$\prod_{\mathfrak{p}} (a,b)_{\mathfrak{p}} \;=\; 1.$$

Proof. This follows from the exact sequence

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

We assume $n > 2$ here so as to ignore the infinite places. □

Likewise there is a "product formula" for the local Tate pairings $(\cdot,\cdot)_{\mathfrak{p}}$ defined by (21) and (22).

Chapter 2

Descent Theorems over Q

2.1 Statement of the First Descent Theorem

Let $n = 5$ or 7. We consider the elliptic curves C_λ and D_λ over $\mathbf{Q}$ with $\boldsymbol{\mu}_n \hookrightarrow C_\lambda$ and $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda$. For $\lambda \in \mathbf{Q}$ we recall D_λ has equation

$$\begin{array}{rcll} y^2 + (1-\lambda)xy - \lambda y & = & x^3 - \lambda x^2 & \lambda \neq 0 \\ y^2 + (1+\lambda-\lambda^2)xy + (\lambda^2-\lambda^3)y & = & x^3 + (\lambda^2-\lambda^3)x^2 & \lambda \neq 0, 1. \end{array}$$

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 the case $n = 5$ we put

$$\begin{array}{rcl} \mathcal{A} & = & \{\, p \text{ prime} \mid \mathrm{ord}_p(\lambda) < 0 \text{ or } \lambda \equiv 0 \pmod{p} \,\} \\ \mathcal{B} & = & \left\{ p \text{ prime} \;\middle|\; \begin{array}{c} \lambda^2 - 11\lambda - 1 \equiv 0 \pmod{p} \text{ and } p \equiv 1 \pmod{5} \\ \text{or } \; p = 5 \text{ and } \lambda \equiv 18 \pmod{25} \end{array} \right\} \end{array}$$

and in the case $n = 7$ we put

$$\begin{array}{rcl} \mathcal{A} & = & \{\, p \text{ prime} \mid \mathrm{ord}_p(\lambda) < 0 \text{ or } \lambda \equiv 0, 1 \pmod{p} \,\} \\ \mathcal{B} & = & \left\{ p \text{ prime} \;\middle|\; \begin{array}{c} \lambda^3 - 8\lambda^2 + 5\lambda + 1 \equiv 0 \pmod{p} \text{ and } p \equiv 1 \pmod{7} \\ \text{or } \; p = 7 \text{ and } \lambda \equiv 5 \pmod{7} \end{array} \right\}. \end{array}$$

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 $\mathcal{S}$.

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*

$$S^{(\phi)}(C_\lambda/\mathbf{Q}) \cong \{\, \theta \in [\mathcal{A}] \mid \theta \in (\mathbf{Q}_p^\times)^n \text{ for all } p \in \mathcal{B} \,\}.$$

The contribution to $S^{(\phi)}(C_\lambda/\mathbf{Q})$ coming from $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda(\mathbf{Q})$ is generated by λ, respectively $\lambda^4(\lambda-1)$. 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 $S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q}) \cong \ker_R(\Xi)$.

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

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

Thus the condition for $p \equiv 1 \pmod{n}$ to belong to $\mathcal{B}$ is $\beta(\lambda) \equiv 0 \pmod{p}$. In view of the identity $\beta(\lambda) = (\lambda + 7)(\lambda - 18) + 125$, respectively $\beta(\lambda) = (\lambda+2)(\lambda-5)^2 - 49$, the condition for n to belong to $\mathcal{B}$ is $\beta(\lambda) \equiv 0 \pmod{125}$, respectively $\beta(\lambda) \equiv 0 \pmod{49}$.

Lemma 2.1 *For p a rational prime, the congruence $\beta(\lambda) \equiv 0 \pmod{p}$ is soluble if and only if $p \equiv 0, \pm 1 \pmod{n}$.*

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

Remark 2.2 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

$$[\mathcal{A}, \mathcal{B}] := (\chi_q(p))_{p \in \mathcal{A}, q \in \mathcal{B}}. \tag{25}$$

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

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

In §3.1 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 $\mathcal{B}$, so $S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q})$ is the subspace of $[\mathcal{B}]$ consisting of nth powers modulo the primes in $\mathcal{A}$. The existence of the pairing Ξ is then nothing more than a statement of the nth power reciprocity law. To make these ideas precise we must work over $\mathbf{Q}(\boldsymbol{\mu}_n)$. Since $[\mathbf{Q}(\boldsymbol{\mu}_n) : \mathbf{Q}] = n - 1$ is prime to n, there is no difficulty in descending back to $\mathbf{Q}$.

In Chapter 3 we give a proof of Theorem 1 working entirely over $\mathbf{Q}$. This proof suffers from not appearing as natural as the method sketched above, but involves considerably less work. In Chapter 5 we generalise our descent calculations to $K = \mathbf{Q}(\boldsymbol{\mu}_n)$ and give an alternative proof of Theorem 1 much closer to the above description.

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 rather delicate Hensel lemma calculations. It is these calculations which make it difficult to work over a general number field.

2.2 Examples and Applications

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

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

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

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

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

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

$$\begin{aligned} |\mathcal{A}| - \operatorname{rank}(\Xi) &= r_1 + 1 - \iota + \dim_n Ш(C_\lambda/\mathbf{Q})[\phi] \\ |\mathcal{B}| - \operatorname{rank}(\Xi) &= r_2 + \iota + \dim_n Ш(D_\lambda/\mathbf{Q})[\widehat{\phi}]. \end{aligned} \tag{26}$$

Thus the upper bound for the rank provided by first descent is

$$|\mathcal{A}| + |\mathcal{B}| - 1 - 2\,\mathrm{rank}(\Xi). \tag{27}$$

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

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

Example 2.3 *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*

$$C_{38}(\mathbf{Q}) = 0 \qquad Ш(C_{38}/\mathbf{Q})(5) = 0$$
$$D_{38}(\mathbf{Q}) \cong \mathbf{Z}/5\mathbf{Z} \qquad Ш(D_{38}/\mathbf{Q})(5) = 0.$$

Example 2.4 *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*

$$C_8(\mathbf{Q}) \cong \mathbf{Z} \qquad Ш(C_8/\mathbf{Q})(7) = 0$$
$$D_8(\mathbf{Q}) \cong \mathbf{Z}/7\mathbf{Z} \oplus \mathbf{Z} \qquad Ш(D_8/\mathbf{Q})(7) = 0.$$

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 2.5 *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` $\mathrm{rank}\, D_\lambda(\mathbf{Q}) = 0$. *By Theorem 1 we deduce*

$$Ш(C_\lambda/\mathbf{Q})[5] \cong (\mathbf{Z}/5\mathbf{Z})^2.$$

Example 2.6 *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` $\mathrm{rank}\, D_\lambda(\mathbf{Q}) = 0$. *By Theorem 1 we deduce*

$$Ш(C_\lambda/\mathbf{Q})[7] \cong (\mathbf{Z}/7\mathbf{Z})^2.$$

Example 2.7 *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*

$$Ш(C_\lambda/\mathbf{Q})[5] \cong (\mathbf{Z}/5\mathbf{Z})^2.$$

So far we have exhibited elements of Ш by comparing our n-descent with a 2-descent. We could equally compare our n-descent with values of L-functions and then cite the work of Kolyvagin [Ko]. This allows us to give examples beyond the reach of `mwrank`. We tabulate many further examples in Appendix D.

Let us assume $Ш(C_\lambda/\mathbf{Q})(n)$ and $Ш(D_\lambda/\mathbf{Q})(n)$ are finite. Since the maps ϕ and $\widehat{\phi}$ on Tate-Shafarevich groups are adjoints with respect to the Cassels-Tate pairing it follows

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

is even. In other words our estimate (27) for the rank differs from the true rank by an even integer. This leads to 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

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

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

$$\{p \text{ prime} \mid W_p = -1\} = \mathcal{A} \cup \mathcal{B}. \tag{28}$$

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

Proposition 2.8 *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

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

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

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

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

Our claim (28) now follows from the description of the reduction types in Lemma 1.4. 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

□

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 2.9 *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 $\mathbf{Q}$ may become arbitrarily large.*

Proof. Let M be the product of the first m primes. Applying Proposition 2.9 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 2.1 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 2.9 to $F(x)$ a product of distinct irreducible polynomials. It seems we must take $\lambda =$ (integer)/2 in order to satisfy the hypothesis at $p = 2$.

2.3 Exhibiting Large Tate-Shafarevich Groups

Let $E/\mathbf{Q}$ be an elliptic curve with $E[5] \cong \boldsymbol{\mu}_5 \oplus \mathbf{Z}/5\mathbf{Z}$. Then E belongs to both the families C_λ and D_λ. We may estimate $\operatorname{rank} E(\mathbf{Q})$ by applying Theorem 1 for two different values of λ. Arranging for our estimates to differ we prove

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 2.10 *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. We know $C_\lambda(\mathbf{Q})[5] \neq 0$ if and only if $\lambda \in (\mathbf{Q}^\times)^5$. So as explained in §1.3 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

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

We know $C_\lambda \cong D_{\eta(\lambda)}$ over $\mathbf{Q}(\boldsymbol{\mu}_5)$. In Chapter 4 we explicitly describe the action (16) of $\mathrm{PSL}_2(\mathbf{Z}/5\mathbf{Z})$ on $X(5)$. We find that the involution ε swaps over the subgroups $\boldsymbol{\mu}_5$ and $\mathbf{Z}/5\mathbf{Z}$. The following isomorphisms are defined over $\mathbf{Q}(\boldsymbol{\mu}_n)$.

$$C_{\tau^5} \cong E_\tau \cong E_{\varepsilon(\tau)} \cong C_{\varepsilon(\tau)^5} \cong D_{\eta(\varepsilon(\tau)^5)} \tag{29}$$

We claim $\eta(\varepsilon(\tau)^5) = \tau f(\tau)/g(\tau)$. Indeed both sides have zeros at $\tau = 0$, $\zeta^2\phi$, $\zeta^3\phi$, $\zeta\overline{\phi}$, $\zeta^4\overline{\phi}$ and poles at $\tau = \infty$, $\zeta\phi$, $\zeta^4\phi$, $\zeta^2\overline{\phi}$, $\zeta^3\overline{\phi}$. It suffices to show equality at the single value $\tau = \phi$. But $f(\tau) = \tau^4 g(-1/\tau)$ and $g(\tau) = g(1-\tau)$, so $f(\phi) = \phi^4 g(\overline{\phi}) = \phi^4 g(\phi)$ and $\eta(\varepsilon(\phi)^5) = \phi^5 = \phi f(\phi)/g(\phi)$ as required. The isomorphism (29) maps

$$\mathbf{Z}/5\mathbf{Z} \hookrightarrow C_{\tau^5} \qquad \text{onto} \qquad \mathbf{Z}/5\mathbf{Z} \hookrightarrow D_{\tau f(\tau)/g(\tau)}.$$

By 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 2.11 *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 2.12 *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 $\operatorname{rank} E_\tau(\mathbf{Q})$. In the notation of Remark 2.2 these are

$$\begin{aligned} &|\mathcal{P}| + |\mathcal{Q}| + |\mathcal{R}| - 1 - 2\operatorname{rank}[\mathcal{P}, \mathcal{Q} \cup \mathcal{R}] \\ &|\mathcal{P}| + |\mathcal{Q}| + |\mathcal{R}| - 1 - 2\operatorname{rank}[\mathcal{P} \cup \mathcal{Q}, \mathcal{R}]. \end{aligned} \tag{30}$$

By repeated use of Dirichlet's theorem on primes in arithmetic progression we choose $\mathcal{Q}_0$ and $\mathcal{R}_0$ sets of primes $p \equiv 1 \pmod 5$ with $\operatorname{rank}[\mathcal{Q}_0, \mathcal{R}_0]$ 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

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

The difference in the estimates (30) 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.

Example 2.13 *For $\tau = 2$ we find $\mathcal{P} = \{2\}$, $\mathcal{Q} = \{11, 61\}$, $\mathcal{R} = \emptyset$. Taking $\lambda = \tau^5 = 32$ in Theorem 1 gives* $\operatorname{rank} E_2(\mathbf{Q}) = 0$ *and* $Ш(E_2/\mathbf{Q})(5) = 0$. *Taking $\lambda = \tau f(\tau)/g(\tau) = 122/11$ gives*

$$Ш(C_{122/11}/\mathbf{Q})(5) \cong (\mathbf{Z}/5\mathbf{Z})^2.$$

Example 2.14 *For $\tau = 8$ we find $\mathcal{P} = \{2\}$, $\mathcal{Q} = \{661, 1181\}$, $\mathcal{R} = \{5, 11\}$. Taking $\lambda = \tau f(\tau)/g(\tau) = 9448/661$ in Theorem 1 gives* $\operatorname{rank} E_8(\mathbf{Q}) = 0$ *and* $Ш(E_8/\mathbf{Q})(5) = 0$. *Taking $\lambda = \tau^5 = 2^{15}$ gives*

$$Ш(D_{2^{15}}/\mathbf{Q})(5) \cong (\mathbf{Z}/5\mathbf{Z})^2.$$

By computer search we find many more examples where one descent calculation shows the rank is zero and the other exhibits elements in the Tate-Shafarevich group. For example, writing $E'_\tau = D_{\tau^5}$ and $E''_\tau = C_{\tau f(\tau)/g(\tau)}$

$$\begin{aligned} Ш(E'_{2003}/\mathbf{Q})(5) &\cong (\mathbf{Z}/5\mathbf{Z})^6 \\ Ш(E''_{6930}/\mathbf{Q})(5) &\cong (\mathbf{Z}/5\mathbf{Z})^{10}. \end{aligned}$$

2.4 Statement of the Second Descent Theorem

We continue to consider the elliptic curves $E = E_\tau$ whose 5-torsion splits as $\boldsymbol{\mu}_5 \oplus \mathbf{Z}/5\mathbf{Z}$. By comparing our first descent calculations with a description of the Cassels-Tate pairing due to Beaver [Be] we arrive at the following second descent theorem.

Theorem 2 *Let $\tau \in \mathbf{Q}$ with $\tau \neq 0$ and let $\mathcal{P}$, $\mathcal{Q}$, $\mathcal{R}$ be the disjoint sets of rational primes defined in §2.3. For $p \in \mathcal{Q} \cup \mathcal{R}$ choose non-trivial characters $\chi_p : (\mathbf{Z}/p\mathbf{Z})^\times \to \mathbf{Z}/5\mathbf{Z}$, respectively $\chi_5 : (\mathbf{Z}/25\mathbf{Z})^\times \to \mathbf{Z}/5\mathbf{Z}$ and suppose the characters χ_p for $p \in \mathcal{Q}$ are compatible in a sense to be explained below. Then $S^{(5)}(E/\mathbf{Q}) \cong \ker(\Psi)$ where*

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

and we use the notation $[\mathcal{P},\mathcal{Q}]$ for the matrix $(\chi_q(p))_{p\in\mathcal{P},q\in\mathcal{Q}}$.

Remark 2.15 For $p \in \mathcal{Q}$ the quantity $\chi_p(p)$ is undefined. It is to be understood that Ψ is a skew-symmetric matrix, and that the diagonal entries are therefore zero.

Remark 2.16 At each prime of bad reduction for E, our point τ on $X(5)$ reduces to one of the cusps $\tau = 0, \infty, \zeta^i\phi, \zeta^i\overline{\phi}$. In fact

$$\begin{array}{rcll} \mathcal{P} & = & \{\, p \text{ prime} \mid \tau \equiv 0, \infty & \pmod p \,\} \\ \mathcal{Q} & \subset & \{\, p \text{ prime} \mid \tau \equiv \zeta^i\phi, \zeta^i\overline{\phi} & \pmod p \,\} \\ \mathcal{R} & \subset & \{\, p \text{ prime} \mid \tau \equiv \phi, \overline{\phi} & \pmod p \,\} \end{array}$$

If we fix the value of i, then each prime $p \in \mathcal{Q}$ comes equipped with a distinguished element ζ of order 5 in $(\mathbf{Z}/p\mathbf{Z})^\times$. We then take χ_p to be the composite of the maps $x \mapsto x^{(p-1)/5}$ and $\zeta \mapsto 1$, and say that the characters χ_p are compatible if chosen in this way.

Remark 2.17 The statement of Theorem 2 leaves a certain amount of freedom in choosing our characters χ_p. It is clear by row and column operations that these choices do not alter the rank of Ψ.

The estimate for $\operatorname{rank} E_\tau(\mathbf{Q})$ provided by Theorem 2 is

$$|\mathcal{P}| + |\mathcal{Q}| + |\mathcal{R}| - 1 - \operatorname{rank} \Psi. \tag{31}$$

This estimate is at most the minimum of the two estimates (30) provided by first descent. We give some examples where it is strictly smaller. For many further examples see Table 5 in Appendix D.

Example 2.18 *Let $\tau = 7$. Then $\mathcal{P} = \{7\}$, $\mathcal{Q} = \{11, 31, 61, 331\}$ and $\mathcal{R} = \{41\}$. After making a compatible choice of characters the matrix Ψ is*

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

This matrix has rank 4 so by Theorem 2, $\operatorname{rank} E_7(\mathbf{Q}) \leq 1$. *This improves on the estimate* $\operatorname{rank} E_7(\mathbf{Q}) \leq 3$ *given by Theorem 1 with $\lambda = 7^5$ or $\lambda = 25487/1891$. Running Cremona's program* `findinf` *for the Weierstrass equation (2) with $\lambda = 7^5$ we exhibit the point of infinite order*

$$(x, y) = (-149525/923^2, 29379375/923^3).$$

Thus $\operatorname{rank} E_7(\mathbf{Q}) = 1$ *and*

$$\begin{aligned} Ш(E_7/\mathbf{Q})(5) &= 0 \\ Ш(E_7'/\mathbf{Q})(5) &\cong (\mathbf{Z}/5\mathbf{Z})^2 \\ Ш(E_7''/\mathbf{Q})(5) &\cong (\mathbf{Z}/5\mathbf{Z})^2. \end{aligned}$$

Example 2.19 *Let $\tau = 12$. Then $\mathcal{P} = \{2, 3\}$, $\mathcal{Q} = \{11, 71, 251, 2411\}$ and $\mathcal{R} = \{131\}$. After making a compatible choice of characters the matrix Ψ is*

	2	3	11	71	251	2411	131
2	0	0	1	1	0	0	1
3	0	0	3	1	1	4	2
11	4	2	0	2	0	2	1
71	4	4	3	0	0	0	0
251	0	4	0	0	0	1	1
2411	0	1	3	0	4	0	1
131	4	3	4	0	4	4	0

This matrix has rank 6, so by Theorem 2, $\operatorname{rank} E_{12}(\mathbf{Q}) = 0$. *This improves on the estimates* $\operatorname{rank} E_{12}(\mathbf{Q}) \leq 4$ *and* $\operatorname{rank} E_{12}(\mathbf{Q}) \leq 2$ *given by Theorem 1 for* $\lambda = 12^5$ *and* $\lambda = 318252/17821$ *respectively. We deduce*

$$\begin{aligned} Ш(E_{12}/\mathbf{Q})(5) &= 0 \\ Ш(E'_{12}/\mathbf{Q})(5) &\cong (\mathbf{Z}/5\mathbf{Z})^4 \\ Ш(E''_{12}/\mathbf{Q})(5) &\cong (\mathbf{Z}/5\mathbf{Z})^2. \end{aligned}$$

These examples show how we may explicitly exhibit elements of Ш for the curves E'_τ and E''_τ. Our methods are less suited to finding elements of Ш for E_τ itself. However, for $\tau = 9$ the L-value listed in Table 5 is non-zero, so by Kolyvagin's theorem such elements certainly do exist.

For $\tau \in \mathbf{Z}$ with $|\tau| \leq 10000$ we estimate $\operatorname{rank} E_\tau(\mathbf{Q})$ using Theorem 1 with $\lambda = \tau$ and $\lambda = \tau f(\tau)/g(\tau)$ and then using Theorem 2. We record how these estimates are distributed.

estimate for	Theorem 1		Theorem 2
$\operatorname{rank} E_\tau(\mathbf{Q})$	$\lambda = \tau^5$	$\lambda = \tau f(\tau)/g(\tau)$	
0	635	66	7676
1	2199	297	9948
2	3696	845	2252
3	4456	1731	117
4	3984	2875	7
5	2819	3854	0
6	1442	3890	0
7	547	3164	0
8	173	1891	0
9	43	951	0
10	5	352	0
11	1	64	0
12	0	16	0
13	0	4	0

We conclude that the elliptic curves isogenous to E_τ tend to have large 5-torsion of Ш, whereas E_τ itself does not. Thus a full 5-descent on E_τ gives a much better estimate for the rank than does descent via 5-isogeny.

Chapter 3

Proof of the First Descent Theorem

3.1 Equations for Torsors in $\mathbf{P}^{n-1}$

Let $n = 5$ or 7. As explained in §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 $\mathrm{char}(K) \neq n$.

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

$$\zeta \mapsto \mathrm{Diag}(1 : \zeta : \ldots : \zeta^{n-1}). \tag{32}$$

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 (32) are the co-ordinate hyperplanes $H_i := \{x_i = 0\}$. As explained in §1.2 the action of $\mathrm{Jac}(T)[n]$ on T lifts to $\mathbf{P}^{n-1}$. Since n is prime to 6 we know $\boldsymbol{\mu}_n \hookrightarrow \mathrm{Jac}(T)$ and so this action is generated by

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

where $*$ denotes a non-zero element of $\overline{K}$. In Chapter 4 we shall see that 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

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

Lemma 3.1 *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. □

Remark 3.2 We sometimes refer to these points of intersection with the coordinate hyperplanes as *flexes*, since they are the points P with $n.P$ linearly equivalent to the hyperplane section.

We recall from §2.1 our notation

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

Definition 3.3 *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*

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

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

Proposition 3.4 *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 3.1(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 τ_i, $a_i \in K$. By Lemma 3.1(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

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

and by symmetry this completes the proof in the case $n = 5$.
(ii) Case $n = 7$. Lemma 3.1(ii) tells us that T has equations

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

for some non-zero constants τ_i, λ_i, a_i, $b_i \in K$. The action of M_2 tells us $\lambda_0 = \lambda_1 = \ldots = \lambda_{n-1}$ 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 3.1(i) we may choose $(0 : z_1 : \ldots : z_6) \in T \cap H_0$ with all $z_i \neq 0$. We find

$$\tau_2 z_2^2 + z_1 z_3 = \tau_3 z_3^2 + \lambda z_2 z_4 = \tau_4 z_4^2 + \lambda z_3 z_5 = \tau_5 z_5^2 + z_4 z_6 = 0. \tag{33}$$

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 (33) allows us to express their ratio in terms of λ and the τ_i. In particular

$$\begin{array}{rcl} z_1 z_6 + a\tau_2\tau_3\tau_4\tau_5 z_2 z_5 = 0 & \Longrightarrow & a = -1/\lambda^2 \\ \lambda z_1 z_6 + b\tau_2\tau_3^2\tau_4^2\tau_5 z_3 z_4 = 0 & \Longrightarrow & b = -1/\lambda^3 \\ \left.\begin{array}{r} (\lambda-1) z_1 z_3 + b\tau_4\tau_5^2\tau_6^2\tau_0 z_5 z_6 = 0 \\ \tau_1 z_1^2 + b\tau_3\tau_4^2\tau_5^2\tau_6 z_4 z_5 = 0 \end{array}\right\} & \Longrightarrow & \lambda^4(\lambda-1) = \prod \tau_i. \end{array}$$

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

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

Lemma 3.5 *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

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

Repeating for the other co-ordinates we find

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

The lemma follows easily from these observations. □

An important consequence of Lemma 3.5 is that geometrically, *i.e.* over $\overline{K}$, the schemes $T = T[\lambda; \tau_0, \ldots, \tau_{n-1}]$ are determined up to isomorphism

by λ. Proposition 3.10 below tells us that T is 1-dimensional and that if $\beta(\lambda) \neq 0$ then it is a smooth curve of genus 1. We originally proved the next two results by direct computation using `mathematica`. A little more thought enables us to treat the cases $n = 5$ and 7 together.

Lemma 3.6 *The scheme $T = T[\lambda; \tau_0, \ldots, \tau_{n-1}]$ 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 $i \neq j$. Then the action of $\boldsymbol{\mu}_n$ tells us that $T \cap H_i$ spans the hyperplane H_i. Since this is true for all co-ordinate hyperplanes, the map

$$H^0(\mathbf{P}^{n-1}, \mathcal{I}_T(2)) \to H^0(H_i, \mathcal{I}_{T \cap H_i}(2))$$

is injective and by counting dimensions we learn that T meets each co-ordinate hyperplane H_i in a single orbit under the action of $\boldsymbol{\mu}_n$.

By symmetry it suffices 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 this point is K-rational. We are now done by Lemma 3.5. □

Proposition 3.7 *The family of elliptic curves C_λ defined in §1.1 has equations*

$$T[\lambda; \alpha(\lambda), 1, \ldots, 1] \quad \textit{with} \quad 0 = \begin{cases} (0:1:1:-1:-1) \\ (0:1:-\lambda:-\lambda^2:\lambda^2:\lambda:-1). \end{cases}$$

Proof. We temporarily write $T_\lambda := T[\lambda; \alpha(\lambda), 1, \ldots, 1]$. For all but finitely many λ we know T_λ is a smooth curve of genus 1. We take as identity element the K-rational point constructed in the proof of Lemma 3.6. An easy calculation shows that this is the point 0 appearing in the statement of the proposition.

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 $\lambda \in K$. Equivalently there is a unique

$\lambda \in K$ such that C and T_λ are isomorphic as curves and this isomorphism respects the actions of $\boldsymbol{\mu}_n$ via translation. By Lemma 1.1(iii) we may assume K is algebraically closed. We embed $C \hookrightarrow \mathbf{P}^{n-1}$ via a complete linear system and choose co-ordinates such that the action of $\boldsymbol{\mu}_n$ on C via translation is the diagonal action (32). Then Proposition 3.4 and Lemma 3.5 tell us $C \cong T_\lambda$ for some $\lambda \in K$. To check the uniqueness statement we consider the automorphisms of $\mathbf{P}^{n-1}$ that commute with (32). 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 §1.1. But in both cases our co-ordinate λ has been chosen such that the cusps are as listed in §1.1. This completes the proof of the proposition. □

In §1.2 we considered the exact sequence

$$\ldots \to C_\lambda(K) \to D_\lambda(K) \xrightarrow{\delta} K^\times/(K^\times)^n \to \mathrm{WC}(C_\lambda/K) \to \ldots \tag{34}$$

and defined $C_{\lambda,\theta}$ to be the torsor under C_λ described by $\theta \in K^\times/(K^\times)^n$.

Lemma 3.8 *Let $\lambda \in K$ not a cusp of $X_1(n)$.*
(i) If $\tau_0, \ldots, \tau_{n-1} \in K$ with $\alpha(\lambda) = \prod \tau_i$ and $\theta = \prod \tau_i^{-i}$ then

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

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

Proof. (i) By Lemma 3.5 there is an isomorphism defined over $\overline{K}$

$$\psi : T[\lambda; \tau_0, \tau_1, \ldots, \tau_{n-1}] \xrightarrow{\sim} C_\lambda = T[\lambda; \alpha(\lambda), 1, \ldots, 1] \tag{35}$$

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

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

it is clear from (i) and the exact sequence (34) that $\alpha(\lambda) \in \operatorname{im}\delta$. Taking $\tau_0 = \ldots = \tau_{n-2} = 1$ and $\tau_{n-1} = \alpha(\lambda)$ in (35) 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 3.9 Relabelling our copy of $\boldsymbol{\mu}_n$ gives isomorphisms $C_{\lambda,\theta} \cong C_{-1/\lambda,\theta^2}$ respectively $C_{\lambda,\theta} \cong C_{(\lambda-1)/\lambda,\theta^2}$. Lemma 3.8 allows us to explicitly write down these isomorphisms. For example in the case $n = 5$ we have

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

We now drop our assumption $\mathrm{char}(K) \neq n$. The next two propositions describe the geometry of the schemes $T[\lambda;\tau_0,\ldots,\tau_{n-1}]$ and the degenerations that occur when λ becomes a cusp.

Proposition 3.10 *Let $\lambda,\tau_0,\ldots,\tau_{n-1} \in K$ with $\alpha(\lambda) = \prod \tau_i \neq 0$. We describe the geometry of the scheme $T = T[\lambda;\tau_0,\ldots,\tau_{n-1}]$.*
(a) If $\beta(\lambda) \neq 0$ then T is a smooth curve of genus 1.
(b) If $\beta(\lambda) = 0$ and $\mathrm{char}(K) \neq n$ then T is a collection of n distinct lines.
(c) If $\beta(\lambda) = 0$ and $\mathrm{char}(K) = n$ then T is a line with multiplicity n.

Proof. We postpone the proof to Chapter 4, but note here that it suffices to work over an algebraically closed field, and to treat the case $\tau_0 = \tau_1 = \ldots = \tau_{n-1}$. □

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

Proposition 3.11 *Let $\tau_0,\ldots,\tau_{n-1} \in K$ 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 collection of n lines. □

3.2 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 §3.1 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

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

Proposition 3.12 *Let $\lambda \in K$ not a cusp of $X_1(n)$. For $\theta \in K^\times/(K^\times)^n$*

$$C_{\lambda,\theta}(K) \neq \emptyset \iff \theta \in \mathrm{im}\left(\delta : D_\lambda(K) \to K^\times/(K^\times)^n\right).$$

(a) If $\mathrm{ord}^*(\lambda) > 0$ then $\mathrm{im}\,\delta = K^\times/(K^\times)^n$.
(b) If $\mathrm{ord}^*(\lambda) = 0$ and $\beta(\lambda) \not\equiv 0 \pmod{\mathfrak{p}}$ then $\mathrm{im}\,\delta = \mathcal{O}^\times/(\mathcal{O}^\times)^n$.
(c) If $\mathrm{ord}^*(\lambda) = 0$ and $\beta(\lambda) \equiv 0 \pmod{\mathfrak{p}}$ and $\mathrm{char}(k) \neq n$ then $\mathrm{im}\,\delta = 0$.

Proof. The first statement is immediate from the exact sequence (34).
(a) Let $\theta \in K^\times/(K^\times)^n$. By Remark 3.9 we may assume $\mathrm{ord}(\lambda) > 0$, respectively $\mathrm{ord}(\lambda - 1) > 0$. We write $C_{\lambda,\theta}$ in the form $T[\lambda; \tau_0, \ldots, \tau_{n-1}]$ with $\mathrm{ord}(\tau_i) \geq 0$ for all i. By Proposition 3.11 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) and (c) Suppose $\theta \in K^\times/(K^\times)^n$ with $\mathrm{ord}(\theta) \equiv 1 \pmod{n}$. We write $C_{\lambda,\theta}$ in the form $T[\lambda; \tau_0, \ldots, \tau_{n-1}]$ with $\mathrm{ord}(\tau_0) = -1$, $\mathrm{ord}(\tau_{n-1}) = 1$ and $\mathrm{ord}(\tau_i) = 0$ for all other i. We take $(x_0 : \ldots : x_{n-1})$ a K-point with $\min\{\mathrm{ord}(x_i)\} = 0$. Examining the equations for $T[\lambda; \tau_0, \ldots, \tau_{n-1}]$ we successively deduce $\mathrm{ord}(x_i) > 0$ for $i = 0, 1, \ldots, n-1$. This contradiction tells us $C_{\lambda,\theta}(K) = \emptyset$. Thus $\mathrm{im}\,\delta \subset \mathcal{O}^\times/(\mathcal{O}^\times)^n$.

Let $\theta \in \mathcal{O}^\times/(\mathcal{O}^\times)^n$ and write $C_{\lambda,\theta}$ in the form $T[\lambda; \tau_0, \ldots, \tau_{n-1}]$ with $\mathrm{ord}(\tau_i) = 0$ for all i. The reduction of this curve is described by Proposition 3.10. In case (b) the reduction is a smooth curve of genus 1. By [Ca2,

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 (c) 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 so by Lemma 3.6 we deduce 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. □

The above proof turns up a useful observation.

Corollary 3.13 *Let F be any field. Then $\beta(u) = 0 \implies \alpha(u) \in (F^\times)^n$.*

Proof. By Proposition 3.10 we know that $T[u; \alpha(u), 1, \ldots, 1]$ is a collection of lines. Considering intersections with the hyperplanes H_i we deduce by Lemma 3.6 that $\alpha(u) \in (F^\times)^n$. □

Proposition 3.12 is incomplete in the sense that we do not treat the case $\operatorname{char}(k) = n$ when λ reduces to an irrational cusp. Indeed our equations for $T[\lambda; \tau_0, \ldots, \tau_{n-1}]$ reduce to give a line with multiplicity n, making it difficult to apply Hensel's lemma.

3.3 Further Hensel Lemma Calculations

We keep our notation for K a local field. In §3.2 we gave some criteria for $C_{\lambda,\theta}(K) \neq \emptyset$. These are sufficient to compute Selmer groups in many cases and it is tempting to restrict attention to such examples. However we consider it worthwhile to investigate the case $\operatorname{char}(k) = n$ more carefully. We recall that in §1.2 we gave equations for $C_{\lambda,\theta}$ via push-out from D_λ. Indeed

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

is given by $\delta(P) = f(P) \mod (K^\times)^n$ where $f \in K(D_\lambda)$ is an explicit rational function. It is our task to identify the image of δ when $\operatorname{char}(k) = n$ and λ reduces to an irrational cusp. The latter is equivalent to $\lambda \equiv 3 \pmod{\mathfrak{p}}$, respectively $\lambda \equiv 5 \pmod{\mathfrak{p}}$.

We use the formal group defined by D_λ as a vehicle for our Hensel lemma calculations. We recall from [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

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

and that the invariant differential has expansion

$$\omega(z) = (1 + a_1 z + (a_1^2 + a_2) z^2 + (a_1^3 + 2a_1 a_2 + 2a_3) z^3 + \dots) dz.$$

To study the curves D_λ we take

$$(a_1, a_2, a_3, a_4, a_6) = \begin{cases} (1-\lambda, -\lambda, -\lambda, 0, 0) & \text{if } n = 5 \\ (1 + \lambda - \lambda^2, \lambda^2 - \lambda^3, \lambda^2 - \lambda^3, 0, 0) & \text{if } n = 7. \end{cases}$$

The series $x(z)$, $y(z)$ and $\omega(z)$ now have coefficients in $\mathbf{Z}[\lambda]$. The composite

$$\begin{array}{ccccc} \mathfrak{p}\mathcal{O} & \longrightarrow & D_\lambda(K) & \xrightarrow{\delta} & K^\times/(K^\times)^n \\ z & \mapsto & (x(z), y(z)) & & \\ & & (x, y) & \mapsto & f(x, y) \end{array}$$

is given by $z \mapsto F(z)$ where $F(z) := \pm z^n f(x(z), y(z))$ is again a power series with coefficients in $\mathbf{Z}[\lambda]$. Explicitly in the cases $n = 5$ and 7 we find

$$\begin{aligned} F(z) &= 1 + (2\lambda - 1) z + \lambda(\lambda + 2) z^2 + \dots + \lambda(\lambda + 1) z^5 + \dots \\ F(z) &= 1 + (3\lambda^2 - 2\lambda - 2) z + (\lambda - 1)(3\lambda^3 + 3\lambda^2 - 3\lambda - 1) z^2 + \dots \\ &\qquad \dots + \lambda^4 (\lambda - 1)(\lambda^5 - \lambda^4 + 1) z^7 + \dots . \end{aligned}$$

The leading terms here are sufficient to determine the image of δ in the case $K = \mathbf{Q}_p$.

Lemma 3.14 *Let $p = n$. Let $\lambda \in \mathbf{Z}_p$ with $\beta(\lambda) \equiv 0 \pmod{p}$. Then the image of the map $\delta : D_\lambda(\mathbf{Q}_p) \to \mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^n$ is generated by $\alpha(\lambda)$.*

Proof. As seen in §1.1 our Weierstrass equation (2) for D_λ is minimal. We write $E = D_\lambda$ and recall from [Si1, Chapter VII] that there is a filtration

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

We are given $\lambda \equiv 3 \pmod 5$, respectively $\lambda \equiv 5 \pmod 7$. By inspection of the above series expansions we find $F'(0) \equiv 0 \pmod p$. If $c \in p\mathbf{Z}_p$ then

$F(c) \equiv 1 \pmod{p^2}$. But $p^2\mathbf{Z}_p \subset (\mathbf{Q}_p^\times)^n$ so δ restricted to $E_1(\mathbf{Q}_p)$ is the zero map.

Since $E_0(\mathbf{Q}_p)/E_1(\mathbf{Q}_p) \cong \widetilde{E}_{\rm ns}(\mathbf{Z}/n\mathbf{Z}) \cong \mathbf{Z}/n\mathbf{Z}$ the table of §1.2 tells us that 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. The lemma follows. □

Proposition 3.15 *Let $p = n$ and let $N = 125$, respectively 49. Let $\lambda \in \mathbf{Q}_p$ not a cusp of $X_1(n)$. For $\theta \in \mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^n$*

$$C_{\lambda,\theta}(\mathbf{Q}_p) \neq \emptyset \iff \theta \in \operatorname{im}\big(\delta : D_\lambda(\mathbf{Q}_p) \to \mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^n\big).$$

(a) If $\operatorname{ord}^*(\lambda) > 0$ *then* $\operatorname{im}\delta = \mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^n$.
(b) If $\operatorname{ord}^*(\lambda) = 0$ *and* $\beta(\lambda) \not\equiv 0 \pmod{N}$ *then* $\operatorname{im}\delta = \mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^n$.
(c) If $\operatorname{ord}^*(\lambda) = 0$ *and* $\beta(\lambda) \equiv 0 \pmod{N}$ *then* $\operatorname{im}\delta = 0$.

Proof. If $\beta(\lambda) \not\equiv 0 \pmod{p}$ then we are already done by Proposition 3.12. Otherwise Lemma 3.14 tells us that $\operatorname{im}\delta$ is generated by $\alpha(\lambda)$. So the condition for $\operatorname{im}\delta$ to be trivial is $\alpha(\lambda) \in (\mathbf{Q}_p^\times)^n$. We compute

$$\left\{\begin{array}{c}\lambda \equiv 3 \pmod 5\\ \lambda \in (\mathbf{Q}_5^\times)^5\end{array}\right\} \iff \lambda \equiv 18 \pmod{25} \iff \beta(\lambda) \equiv 0 \pmod{125}$$

$$\left\{\begin{array}{c}\lambda \equiv 5 \pmod 7\\ \lambda^4(\lambda-1) \in (\mathbf{Q}_7^\times)^7\end{array}\right\} \iff \lambda \equiv 5 \pmod 7 \iff \beta(\lambda) \equiv 0 \pmod{49}.$$

□

The reader only interested in descent calculations over $\mathbf{Q}$ should now turn to §3.4. Our next task is to develop some identities that will be crucial to our Hensel lemma calculations.

We return to considering K a local field with $\operatorname{char}(k) = n$ and write $e = \operatorname{ord}(n)$. We take $\lambda \in K$ with $\operatorname{ord}^*(\lambda) = 0$ and write $E = D_\lambda$. The points tabulated in §1.2 reduce to give $\mathbf{Z}/n\mathbf{Z} \hookrightarrow \widetilde{E}_{\rm ns}(k)$ generated by $\mathbf{1} = (0,0)$. The rational function $f \in K(E)$ reduces to $\widetilde{f} \in k(\widetilde{E})$. Since $\operatorname{char}(k) = n$ we find

$$(\,\widetilde{f}\,) = n.\mathbf{1} - n.0 \quad \text{and} \quad (\,d\widetilde{f}\,) = n.\mathbf{1} - n.0.$$

If $\widetilde{E}$ is smooth then $d\widetilde{f}/\widetilde{f}$ is a multiple of the invariant differential. If $\widetilde{E}$ is singular, hence rational, then $d\widetilde{f}/\widetilde{f} = 0$. These observations give some explanation for the congruences appearing in the next lemma.

Let $g(x,y)$ be the Weierstrass cubic (2) defining D_λ. The invariant differential is $\omega = (\partial g/\partial y)^{-1}dx = -(\partial g/\partial x)^{-1}dy$.

Lemma 3.16 *Let $I \lhd \mathbf{Z}[\lambda,x,y]$ be the ideal generated by n and $g(x,y)$. Then*

$$df/\omega = \begin{vmatrix} \partial f/\partial x & \partial f/\partial y \\ \partial g/\partial x & \partial g/\partial y \end{vmatrix} \equiv \beta'(\lambda)f \pmod{I}.$$

Proof. The first equality is a tautology. For the congruence we compute

$$\begin{aligned} n=5 \qquad df/\omega &= (-3\lambda-1)f(x,y) - 3g(x,y) + 5y^2 \\ n=7 \qquad df/\omega &= (-4\lambda^2+5\lambda-2)f(x,y) \\ &\quad + (3x+3\lambda-2)g(x,y) + 7y(\lambda x^2 - xy - \lambda y). \end{aligned}$$

□

Lemma 3.17 *Let $\lambda \in K$ with $\mathrm{ord}^*(\lambda) = 0$. Let $F(z)$ be the power series constructed above and put $t = \mathrm{ord}(\beta'(\lambda))$.*
(i) If $t < e$ then $\mathrm{ord}(F'(0)) = t$.
(ii) If $t \le e$ then $F'(z) \equiv 0 \pmod{\mathfrak{p}^t}$.

Proof. (i) This follows from the observation $F'(0) \equiv \beta'(\lambda) \pmod{n}$.
(ii) We have power series

$$df/dz = (df/\omega)(\omega/dz).$$

Since $\lambda \in \mathcal{O}$ we know $f(x(z),y(z)) \in \mathcal{O}[[z]]$ and $\omega(z)/dz \in \mathcal{O}[[z]]$. Then by Lemma 3.16, $df/\omega \equiv 0 \pmod{\mathfrak{p}^t}$. Hence $F'(z) \equiv df/dz \equiv 0 \pmod{\mathfrak{p}^t}$. □

We end this section by giving the version of Hensel's lemma we have been working towards.

Proposition 3.18 *Let $\lambda \in K$ with $\mathrm{ord}^*(\lambda) = 0$. Let $t = \mathrm{ord}(\beta'(\lambda))$ and suppose $0 < t < e$. If $\nu \ge t/(n-1)$ then*

$$\{\, F(c) \mid c \in \mathfrak{p}^\nu \mathcal{O} \,\} = \{\, \theta \in K^\times \mid \mathrm{ord}(\theta - 1) \ge t + \nu \,\}.$$

Proof. "$\subset$" Let $c \in \mathfrak{p}^\nu\mathcal{O}$. Since $F'(z) \equiv 0 \pmod{\mathfrak{p}^t}$ and $\mathrm{ord}(c^n) \ge n\nu \ge t+\nu$, we deduce $F(c) \equiv 1 \pmod{\mathfrak{p}^{t+\nu}}$ as required.

"$\supset$" Let $\theta \equiv 1 \pmod{\mathfrak{p}^{t+\nu}}$. We claim that for all $m \geq t+\nu$ there exists $c_m \in \mathfrak{p}^{\nu}\mathcal{O}$ with

$$\begin{aligned} &F(c_m) \equiv \theta \pmod{\mathfrak{p}^m} \\ &\mathrm{ord}(F'(c_m)) = t. \end{aligned} \tag{36}$$

For the case $m = t+\nu$ we take $c_m = 0$ and appeal to Lemma 3.17(i). We now suppose (36) is true for m and let $c_{m+1} = c_m + a\pi^{m-t}$ where $\mathrm{ord}(\pi) = 1$ and $a \in \mathcal{O}$ is yet to be determined. We consider the Taylor series expansion of F about c_m. Lemma 3.17(ii) and the inequality $n(m-t) > m$ give

$$F(c_{m+1}) \equiv F(c_m) + a\pi^{m-t}F'(c_m) \pmod{\mathfrak{p}^{m+1}}.$$

Since $\mathrm{ord}(F'(c_m)) = t$ we may solve for a such that $F(c_{m+1}) \equiv \theta \pmod{\mathfrak{p}^{m+1}}$. Further $F'(c_{m+1}) \equiv F'(c_m) \pmod{\mathfrak{p}^m}$ so certainly $\mathrm{ord}(F'(c_{m+1})) = t$. This proves (36) for $m+1$ and our claim follows by induction. Taking $c = \lim c_m$ gives $F(c) = \theta$ as required. □

3.4 Computation of Selmer Groups

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 §2.1. In this section we prove that the Selmer group $S^{(\phi)}(C_\lambda/\mathbf{Q})$ is as described in Theorem 1. We then complete the proof of Theorem 1 by explaining how the groups $S^{(\phi)}(C_\lambda/\mathbf{Q})$ and $S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q})$ are related.

Proposition 3.19 *Let $\lambda \in \mathbf{Q}$ not a cusp of $X_1(n)$. The connecting maps*

$$\begin{aligned} \delta_\phi &: D_\lambda(\mathbf{Q}_p) \to H^1(\mathbf{Q}_p, \boldsymbol{\mu}_n) \\ \delta_{\widehat{\phi}} &: C_\lambda(\mathbf{Q}_p) \to H^1(\mathbf{Q}_p, \mathbf{Z}/n\mathbf{Z}) \end{aligned}$$

have images

$$\mathrm{im}\,\delta_\phi = \begin{cases} H^1(\mathbf{Q}_p, \boldsymbol{\mu}_n) & \text{if } p \in \mathcal{A} \\ H^1_{\mathrm{un}}(\mathbf{Q}_p, \boldsymbol{\mu}_n) & \text{if } p \notin \mathcal{A} \cup \mathcal{B} \\ 0 & \text{if } p \in \mathcal{B} \end{cases}$$

and

$$\mathrm{im}\,\delta_{\widehat{\phi}} = \begin{cases} 0 & \text{if } p \in \mathcal{A} \\ H^1_{\mathrm{nr}}(\mathbf{Q}_p, \mathbf{Z}/n\mathbf{Z}) & \text{if } p \notin \mathcal{A} \cup \mathcal{B} \\ H^1(\mathbf{Q}_p, \mathbf{Z}/n\mathbf{Z}) & \text{if } p \in \mathcal{B} \end{cases}$$

where H^1_{un} and H^1_{nr} are the subgroups of H^1 defined in Proposition 1.15.

Proof. (i) The description of $\operatorname{im}\delta_\phi$ is given by combining Propositions 3.12 and 3.15. Note that $H^1_{\rm un}(\mathbf{Q}_p,\boldsymbol{\mu}_n) = \mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^n$ and this group is trivial unless $p = n$ or $p \equiv 1 \pmod n$.
(ii) Tate local duality, specifically Proposition 1.17, tells us $\operatorname{im}\delta_\phi$ and $\operatorname{im}\delta_{\widehat{\phi}}$ are exact annihilators with respect to the Tate pairing

$$H^1(\mathbf{Q}_p,\boldsymbol{\mu}_n) \times H^1(\mathbf{Q}_p,\mathbf{Z}/n\mathbf{Z}) \to \mathbf{Z}/n\mathbf{Z}. \tag{37}$$

The description of $\operatorname{im}\delta_{\widehat{\phi}}$ now follows from the description of $\operatorname{im}\delta_\phi$. □

The first statement of Theorem 1 is an immediate consequence.

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

We have already seen two proofs of the statement concerning torsion, in §1.2 using the push-out method, and in §3.1 using the projective space method. So to prove Theorem 1 it only remains to explain the relationship between $S^{(\phi)}(C_\lambda/\mathbf{Q})$ and $S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q})$.

For $\mathcal{S}$ a finite set of rational primes we define

$$\begin{aligned} [\mathcal{S}] &:= \ker\left(H^1(\mathbf{Q},\boldsymbol{\mu}_n) \to \textstyle\prod_{p\notin\mathcal{S}} H^1(\mathbf{Q}_p,\boldsymbol{\mu}_n)/H^1_{\rm un}(\mathbf{Q}_p,\boldsymbol{\mu}_n)\right) \\ \langle\mathcal{S}\rangle &:= \ker\left(H^1(\mathbf{Q},\mathbf{Z}/n\mathbf{Z}) \to \textstyle\prod_{p\notin\mathcal{S}} H^1(\mathbf{Q}_p,\mathbf{Z}/n\mathbf{Z})/H^1_{\rm nr}(\mathbf{Q}_p,\mathbf{Z}/n\mathbf{Z})\right). \end{aligned}$$

Since we are identifying $H^1(\mathbf{Q},\boldsymbol{\mu}_n) = \mathbf{Q}^\times/(\mathbf{Q}^\times)^n$, the notation $[\mathcal{S}]$ agrees with that used to state Theorem 1.

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

$$\Xi(a,b) \;=\; \textstyle\sum_{p\in\mathcal{B}}(a,b)_p = -\sum_{p\in\mathcal{A}}(a,b)_p \tag{38}$$

where $(\cdot,\cdot)_p$ is the Tate pairing (37). If $p \notin \mathcal{A}\cup\mathcal{B}$ then $a \in H^1_{\rm un}(\mathbf{Q}_p,\boldsymbol{\mu}_n)$ and $b \in H^1_{\rm nr}(\mathbf{Q}_p,\mathbf{Z}/n\mathbf{Z})$. So by Proposition 1.15 together with the "product formula" the two sums given in (38) are indeed equal. To complete the proof of Theorem 1 it suffices to show $\langle\mathcal{B}\rangle \cong [\mathcal{B}]$ and to identify the left and right kernels of Ξ as Selmer groups.

For each prime $p \equiv 0, 1 \pmod n$ we write $F^{(p)}$ for the degree n cyclic extension of $\mathbf{Q}$ unramified outside p. Concretely $F^{(p)}$ is the degree n subfield of $\mathbf{Q}(\boldsymbol{\mu}_p)$, respectively $\mathbf{Q}(\boldsymbol{\mu}_{n^2})$. For each $p \in \mathcal{B}$ we make an arbitrary choice of isomorphism $\xi^{(p)} : \operatorname{Gal}(F^{(p)}/\mathbf{Q}) \cong \mathbf{Z}/n\mathbf{Z}$. By class field theory there is an isomorphism $[\mathcal{B}] \cong \langle\mathcal{B}\rangle$ via $p \mapsto \xi^{(p)}$.

We relate our Selmer groups to the pairing Ξ. For any element $(*)$ we write $(*)_p$ for the corresponding local element.

$$\begin{aligned} S^{(\phi)}(C_\lambda/\mathbf{Q}) &\cong \{\, a \in H^1(\mathbf{Q}, \boldsymbol{\mu}_n) \mid a_p \in \operatorname{im}\delta_\phi \text{ for all primes } p \,\} \\ &\cong \{\, a \in [\mathcal{A}] \mid a_p = 0 \text{ for all } p \in \mathcal{B} \,\} \\ &\subset \ker_L(\Xi) \\ S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q}) &\cong \{\, b \in H^1(\mathbf{Q}, \mathbf{Z}/n\mathbf{Z}) \mid b_p \in \operatorname{im}\delta_{\widehat{\phi}} \text{ for all primes } p \,\} \\ &\cong \{\, b \in \langle\mathcal{B}\rangle \mid b_p = 0 \text{ for all } p \in \mathcal{A} \,\} \\ &\subset \ker_R(\Xi) \end{aligned}$$

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

Lemma 3.20 *The natural maps*

$$\begin{aligned} [\mathcal{A}] &\to \oplus_{p\in\mathcal{A}} H^1(\mathbf{Q}_p, \boldsymbol{\mu}_n)/H^1_{\mathrm{un}}(\mathbf{Q}_p, \boldsymbol{\mu}_n) \\ \langle\mathcal{B}\rangle &\to \oplus_{p\in\mathcal{B}} H^1(\mathbf{Q}_p, \mathbf{Z}/n\mathbf{Z})/H^1_{\mathrm{nr}}(\mathbf{Q}_p, \mathbf{Z}/n\mathbf{Z}) \end{aligned}$$

are isomorphisms.

Proof. (i) The map is injective since

$$\{\, \theta \in \mathbf{Q}^\times/(\mathbf{Q}^\times)^n \mid \operatorname{ord}_p(\theta) \equiv 0 \pmod{n} \text{ for all } p \,\}$$

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

Now take $a \in [\mathcal{A}]$ and suppose $a \in \ker_L(\Xi)$, *i.e.* $\sum_{p\in\mathcal{B}}(a,b)_p = 0$ for all $b \in \langle\mathcal{B}\rangle$. Then $a_p \in H^1_{\mathrm{un}}(\mathbf{Q}_p, \boldsymbol{\mu}_n)$ for all $p \notin \mathcal{A}$. So by Proposition 1.15 and the description of $\langle\mathcal{B}\rangle$ in Lemma 3.20 it follows $a_p = 0$ for all $p \in \mathcal{B}$. Thus $S^{(\phi)}(C_\lambda/\mathbf{Q}) \cong \ker_L(\Xi)$ and by the same reasoning $S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q}) \cong \ker_R(\Xi)$. This completes the proof of Theorem 1 subject to Proposition 3.10. We have postponed the proof of this geometrical result to the next chapter.

Chapter 4

On the Geometry of Elliptic Normal Curves

This chapter is intended as a survey of certain geometrical results relevant to our descent calculations. In particular we prove Proposition 3.10 which is an essential ingredient in the proofs of our descent theorems. The equations (41) and (42), which we derive from an elementary point of view, go back to Klein [K2] as relations among theta functions. They also feature prominently in [AR] and [V2]. In Appendix A we discuss the relationship of these equations with the work of Buchsbaum and Eisenbud [BE].

4.1 Elliptic Normal Curves

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

Definition 4.1 *(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* $i - j \equiv \pm 1 \pmod{n}$.

Remark 4.2 Let E be an elliptic normal curve. For $d \geq 1$ the hypersurfaces of degree d in $\mathbf{P}^{n-1}$ cut out a complete linear system on E. The case $d = 1$, *i.e.* linear normality, is an immediate consequence of Riemann-Roch. For

the general case, *i.e.* projective normality, see [Ha, IV Exercises 4.1, 4.2] for a proof using Weierstrass equations, or [Hu, IV Lemma 1.2] for a proof that involves reducing to a similar statement about finite sets of points in general position.

Lemma 4.3 *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) There is a short exact sequence

$$0 \to H^0(\mathbf{P}^{n-1}, \mathcal{I}_E(2)) \to H^0(\mathbf{P}^{n-1}, \mathcal{O}_{\mathbf{P}^{n-1}}(2)) \to H^0(E, \mathcal{O}_E(2)) \to 0$$

where exactness on the right is part of the statement of projective normality. Thus $h^0(\mathbf{P}^{n-1}, \mathcal{I}_E(2)) = n(n+1)/2 - 2n = n(n-3)/2$ as required. That the quadrics suffice to define E may be proved by induction on n. We refer to [Hu, IV Theorem 1.3] where a stronger result is proved.
(ii) We move the n points of intersection to the points $(1:0:0:\dots)$, $(0:1:0:\dots), \dots$ and the result is clear. □

In order to construct the modular curve $X(n)$ defined in §1.3 we consider triples (E, P, Q) where E is an elliptic curve and $P, Q \in E[n]$ satisfy $e_n(P, Q) = \zeta_n$.

Proposition 4.4 *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 §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 M_P has distinct eigenvalues and 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. Lemma 4.5 below tells us that their commutator in GL_n gives one possible definition of the Weil pairing. It follows $r = 1$ as required. □

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

Lemma 4.5 *Let $E \hookrightarrow \mathbf{P}^{n-1}$ be an elliptic normal curve and let $P, Q \in E[n]$. Suppose τ_P and τ_Q lift to matrices $\tilde{M}_P$ and $\tilde{M}_Q$ in GL_n. Then*

$$e_n(P,Q) = \tilde{M}_P \tilde{M}_Q \tilde{M}_P^{-1} \tilde{M}_Q^{-1}.$$

Proof. It suffices to work with the triple (E, P, Q) of Proposition 4.4. We are also free to suppose $0 \in E \cap \{x_0 = 0\}$. Let g be the rational function x_1/x_0 on E. Then $(g) = \sum(rP + Q) - \sum(rP)$ where the sums run over $r \in \mathbf{Z}/n\mathbf{Z}$. For $\phi : E \to E'$ the isogeny with kernel generated by P we find

$$e_\phi(P, \phi Q) = g(X + P)/g(X) = \zeta = \tilde{M}_P \tilde{M}_Q \tilde{M}_P^{-1} \tilde{M}_Q^{-1}. \tag{39}$$

The dual isogeny is $\widehat{\phi} : E' \to E$. We take $P' \in E'$ with $\widehat{\phi} P' = P$ and compute

$$e_\phi(P, \phi Q) = e_\phi(\widehat{\phi} P', \phi Q) = e_n(P', \phi Q) = e_n(\widehat{\phi} P', Q) = e_n(P, Q). \tag{40}$$

Combining (39) and (40) proves the lemma. □

Proposition 4.6 *Let n be 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 4.4. 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. □

4.2 An Algebraic Construction of $X(n)$

For simplicity we restrict to $n \geq 5$ odd. Let (E, P, Q) be 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 4.6. We then ask the question "where is 0?". This determines an embedding $Y(n) \hookrightarrow \mathbf{P}^{n-1}$. Indeed, if we know the co-ordinates of $0 \in \mathbf{P}^{n-1}$ then M_P and M_Q allow us to write down n^2 points on E. Since E is defined by quadrics, it follows by Bézout's theorem that these n^2 points suffice to determine E.

Our assumption that n is odd tells us

$$n.0 \sim 0 + P + 2P + \ldots + (n-1)P.$$

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

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

for some $a_1, a_2, \ldots, a_{(n-1)/2}$ non-zero. We shall shortly see that $(+)$ never happens. For a proof over $\mathbf{C}$ using Weierstrass σ-functions we refer to [Hu, Chapter 1]. Working with $(-)$ we make the natural inclusions

$$Y(n) \hookrightarrow \mathbf{P}^{(n-3)/2} \hookrightarrow \mathbf{P}^{n-1}.$$

The action of $\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z})$ on $Y(n)$ extends to a projective representation $\overline{\rho} : \mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z}) \to \mathrm{PGL}_{(n-1)/2}$. In order to give an explicit description of $\overline{\rho}$ we first construct $\rho : \mathrm{SL}_2(\mathbf{Z}/n\mathbf{Z}) \to \mathrm{PGL}_n$ such that

$$\rho \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} M_P^u M_Q^v \quad \rho \begin{pmatrix} a & b \\ c & d \end{pmatrix} = M_P^{au+bv} M_Q^{cu+dv}$$

and the image of ρ commutes with $[-1]$. Then ρ and $\overline{\rho}$ are given by

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \rho(S) = (\zeta^{ij})_{i,j=0}^{n-1}, \qquad \overline{\rho}(S) = (\zeta^{ij} - \zeta^{-ij})_{i,j=1}^{(n-1)/2}$$
$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \rho(T) = \mathrm{Diag}(\zeta^{-i^2/2})_{i=0}^{n-1}, \quad \overline{\rho}(T) = \mathrm{Diag}(\zeta^{-i^2/2})_{i=1}^{(n-1)/2}.$$

Here all exponents are to be interpreted as elements of $\mathbf{Z}/n\mathbf{Z}$. A further useful observation is that ρ and $\overline{\rho}$ map diagonal matrices to permutation matrices.

We consider the vector spaces

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

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 $0 = (0 : a_1 : a_2 : \dots : -a_2 : -a_1)$ and its translates under M_Q impose some linear conditions on the coefficients of the quadrics in V_0. We are led to make the following definition.

Definition 4.7 *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*

$$\mathrm{rank}(a_{i-j}a_{i+j})_{i,j=0}^{n-1} \leq 2. \tag{41}$$

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

The above construction shows $Y(n) \subset A(n)$ and it is natural to ask whether these quartics suffice to define $X(n)$. We shall discuss below the theorem of Vélu that for p a prime $A(p) = X(p)$.

Remark 4.8 Suppose $\mathrm{char}(K) \neq 2$ and that $(+)$ holds for some triple (E, P, Q). Then the matrix (41) is symmetric and by considering the top left 3×3 minor we learn that some of the a_i are zero. This contradicts our earlier observations. For $\mathrm{char}(K) = 2$ there is of course no distinction between $(+)$ and $(-)$.

We know that the triple (E, P, Q) determines the point 0. Conversely the quadrics defining E are precisely the ones containing 0 and its translates under M_P and M_Q. We are led to make the following definition.

Definition 4.9 *For $n \geq 5$ odd, let $\mathcal{A}(n) \subset A(n) \times \mathbf{P}^{n-1}$ be the subscheme defined by*

$$\operatorname{rank}(a_{i-j}x_{i+j})_{i,j=0}^{n-1} \leq 2. \tag{42}$$

More precisely, $\mathcal{A}(n)$ is defined by the leading 4×4 Pfaffians.

If we take $0 = (0\colon a_1\colon a_2\colon \dots)$ corresponding to the triple (E, P, Q) then the 4×4 Pfaffians here are quadrics vanishing on E. A little combinatorial checking shows that we obtain all such quadrics.

Let $\mathcal{Y}(n) \subset Y(n) \times \mathbf{P}^{n-1}$ be defined by the equations (42). Then $\mathcal{Y}(n) \to Y(n)$ is a family of elliptic curves, and indeed is the universal family over $Y(n)$. We write $\mathcal{X}(n) \subset X(n) \times \mathbf{P}^{n-1}$ for the scheme-theoretic closure of $\mathcal{Y}(n)$. Then $\mathcal{X}(n) \to X(n)$ is a flat family of curves each of degree n and arithmetic genus 1.

It is easy to see that $\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z})$ acts on each of the families $\mathcal{Y}(n) \to Y(n)$, $\mathcal{X}(n) \to X(n)$ and $\mathcal{A}(n) \to A(n)$. For $A(n)$ we check $\rho(S)$ and $\rho(T)$ do not alter the rank of the matrix $(a_{i-j}a_{i+j})_{ij}$. The same calculation shows $\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z})$ acts on $\mathcal{A}(n)$.

4.3 Examples

We examine Klein's equations (41) and (42) for some small values of n. In particular we prove Proposition 3.10 under our assumption $\operatorname{char}(K) \neq n$. We postpone the case $\operatorname{char}(K) = n$ to §4.6.

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_0 is spanned by

$$abx_0^2 + b^2x_1x_4 - a^2x_2x_3 = 0. \tag{43}$$

There are rational cusps at $(a : b) = (1 : 0)$, $(0 : 1)$. The remaining cusps are found using the action of $\mathrm{PSL}_2(\mathbf{Z}/5\mathbf{Z})$ generated by

$$\begin{array}{rccl} S: & (a : b) & \mapsto & (\phi a + b : a - \phi b) \\ T: & (a : b) & \mapsto & (a : \zeta b) \end{array}$$

where $\phi = (\zeta - \zeta^4)/(\zeta^2 - \zeta^3)$ is the golden ratio. The cusps

$$a/b = 0, \infty, \zeta^i\phi, \zeta^i\overline{\phi}$$

may be viewed under stereographic projection as the vertices of an icosahedron. By inspection of the equations (43), the fibre of $\mathcal{A}(5) \to A(5)$ at each rational cusp is a Néron polygon. The action of $\mathrm{PSL}_2(\mathbf{Z}/5\mathbf{Z})$ tells us that the same is true at all the cusps.

In the notation of §3.1 the curve (43) is $T[\lambda; \tau, \ldots, \tau]$ where $\tau = a/b$ and $\lambda = \tau^5$. To prove Proposition 3.10 we must find the condition on λ for $T[\lambda; \tau_0, \ldots, \tau_4]$ to degenerate to a Néron polygon. We see that the condition is $\lambda = \phi^5$ or $\overline{\phi^5}$. These are the zeros of $\beta(\lambda) = \lambda^2 - 11\lambda - 1$ as required.

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 [K1] and V_0 is spanned by

$$\begin{array}{rcrcrcrcl} & & abx_1x_6 & + & bcx_2x_5 & + & cax_3x_4 & = & 0 \\ abx_0^2 & & & + & c^2x_2x_5 & - & b^2x_3x_4 & = & 0 \\ bcx_0^2 & - & c^2x_1x_6 & & & + & a^2x_3x_4 & = & 0 \\ cax_0^2 & + & b^2x_1x_6 & - & a^2x_2x_5 & & & = & 0. \end{array} \tag{44}$$

We have rational cusps at $(a : b : c) = (1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)$. The remaining cusps are found using the action of $\mathrm{PSL}_2(\mathbf{Z}/7\mathbf{Z})$. They are at

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

and its translates under $(a : b : c) \mapsto (b : c : a)$ and $(a : b : c) \mapsto (\zeta^3 a : \zeta b : c)$. Again we find the fibre of $\mathcal{A}(7) \to A(7)$ at each cusp is a Néron polygon.

In the notation of §3.1 the curve (44) 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.

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

To prove Proposition 3.10 we must find the condition on λ for $T[\lambda;\tau_0,\ldots,\tau_6]$ to degenerate to a Néron polygon. We see that the condition is $\lambda = -(\zeta - \zeta^6)(\zeta^4-\zeta^3)^2/(\zeta^2-\zeta^5)^3$ or one of its conjugates. These are the zeros of $\beta(\lambda) = \lambda^3 - 8\lambda^2 + 5\lambda + 1$ as required.

Equations for $X(9)$

Let $0 = (0 : a : -b : d : c : -c : -d : b : -a)$. $A(9)$ is defined by

$$\operatorname{rank}\begin{pmatrix} 0 & -a^2 & -b^2 & -d^2 & -c^2 \\ a^2 & 0 & -ad & bc & cd \\ b^2 & ad & 0 & ac & -bd \\ d^2 & -bc & -ac & 0 & -ab \\ c^2 & -cd & bd & ab & 0 \end{pmatrix} \leq 2 \iff \left\{ \begin{array}{rcl} (a^2b + b^2c + c^2a)d & = & 0 \\ ab^3 - ac^3 - bd^3 & = & 0 \\ bc^3 - ba^3 - cd^3 & = & 0 \\ ca^3 - cb^3 - ad^3 & = & 0. \end{array} \right.$$

Adding together the last three equations and factoring we find

$$X(9) = \left\{ \begin{array}{rcl} a^2b + b^2c + c^2a & = & 0 \\ ab^2 + bc^2 + ca^2 & = & d^3 \end{array} \right\} \subset \mathbf{P}^3$$

whereas $A(9)$ contains four additional isolated points

$$(0:0:0:1),\ (1:1:1:0),\ (1:\zeta^3:\zeta^6:0),\ (1:\zeta^6:\zeta^3:0).$$

We use the action of $\mathrm{PSL}_2(\mathbf{Z}/9\mathbf{Z})$ to find the cusps of $X(9)$. They are at

$$\begin{array}{rcl} (a:b:c:d) & = & (1:0:0:0),\ (1:1:\zeta^3:0),\ (1:1:\zeta^6:0), \\ & & (\zeta-\zeta^8 : \zeta^7-\zeta^2 : \zeta^4-\zeta^5 : \zeta^3-\zeta^6) \end{array}$$

and their translates under

$$\begin{array}{rcl} (a:b:c:d) & \mapsto & (b:c:a:d), \\ (a:b:c:d) & \mapsto & (\zeta^6 a : \zeta^3 b : c : \zeta d). \end{array}$$

The fibres of $\mathcal{A}(9) \to A(9)$ at the cusps are Néron polygons of degree 9. The fibres of $\mathcal{A}(9) \to A(9)$ at the isolated points consist of three disjoint copies of $\mathbf{P}^2$.

The curve $X(11)$ was described by Klein as the singular locus of the Hessian of the cubic threefold

$$\{v^2w + w^2x + x^2y + y^2z + z^2v = 0\} \subset \mathbf{P}^4.$$

We refer to Adler [AR] for further details.

4.4 The Relationship Between $A(n)$ and $X(n)$

We continue to take $n \geq 5$ odd and consider the family $\mathcal{A}(n) \to A(n)$.

Definition 4.10 *Let $c_r \in A(n)$ be the point with $a_i = 0$ for $i \not\equiv \pm r \pmod{n}$. We call the points c_r* rational cusps*, even if they do not lie on $X(n)$.*

Lemma 4.11 *The fibre of $\mathcal{A}(n) \to A(n)$ above the rational cusp c_r is a collection of k Néron polygons of degree n/k where $k = \gcd(r, n)$ and we assume $n/k \geq 5$. If $n/k = 3$ we obtain k copies of $\mathbf{P}^2$ instead.*

Proof. Let $i, j \in \mathbf{Z}/n\mathbf{Z}$ with $i - j \not\equiv 0, \pm 2r \pmod{n}$. Then

$$\#\{(i \pm r)/2, (j \pm r)/2\} = 4$$

and by considering the corresponding leading 4×4 submatrix of (42) we find $x_i x_j = 0$. The lemma follows. □

Lemma 4.11 leads us to suspect that for composite n the scheme $A(n)$ contains copies of $X(m)$ for $m|n$. More precisely we have

Lemma 4.12 *$A(n)$ contains $k \prod_{p|k}(1 + 1/p)$ copies of the curve $X(n/k)$ where $k|n$ and $n/k \geq 5$. If $n/k = 3$ we obtain isolated points instead.*

Proof. There is an inclusion $A(n/k) \hookrightarrow A(n)$ given by

$$0 = (0 : a_1 : a_2 : \dots) \mapsto 0' = (0 : a'_1 : a'_2 : \dots)$$

where $a'_i = a_{i/k}$ if $i \equiv 0 \pmod{k}$ and $a'_i = 0$ otherwise. Then the fibre of $\mathcal{A}(n) \to A(n)$ above $0'$ consists of k copies of the fibre of $\mathcal{A}(n/k) \to A(n/k)$ above 0. To see this we need only reorder rows and columns such that the matrix $(a'_{i-j} x_{i+j})_{ij}$ is in block diagonal form, with each block corresponding to a congruence class mod k.

This construction gives a copy of $X(n/k) \hookrightarrow A(n)$ with $M_P^{n/k}$ acting trivially on the fibres. By means of the action of $\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z})$ we obtain further copies for each subgroup $\mathbf{Z}/k\mathbf{Z} \hookrightarrow \langle M_P, M_Q \rangle$. So the lemma follows by counting the cyclic subgroups of order k in $(\mathbf{Z}/n\mathbf{Z})^2$. Naturally the case $n/k = 3$ is badly behaved since a plane cubic cannot be defined by quadrics. □

We suspect that the connected components of $A(n)$ are precisely the curves and points described in Lemma 4.12. In the case $n = p$ is prime this is a theorem due to Vélu [V2].

Theorem 4.13 *For p a prime the families $\mathcal{A}(p) \to A(p)$ and $\mathcal{X}(p) \to X(p)$ are the same. In particular the quartics (41) suffice to define $X(p)$.*

We recall an important step in the proof of the theorem.

Proposition 4.14 *Let C be the fibre of $\mathcal{A}(n) \to A(n)$ above $0_C = (0 : a_1 : a_2 : \dots)$ and suppose $a_i \neq 0$ for all $i \neq 0$. Then $\langle M_P \rangle$ acts freely on C with quotient $\phi : C \to D$; $(x_0 : \dots : x_{n-1}) \mapsto (X : Y : Z)$ where*

$$X = x_0 x_1 x_{n-1}, \quad Y = x_{n-1}^2 x_2, \quad Z = x_0^3$$

and D has Weierstrass equation

$$Y^2 Z - \frac{a_2^5 + a_1^4 a_4}{a_1^3 a_2 a_3} XYZ + \frac{a_2^2}{a_1^2} YZ^2 = -\frac{a_2^2}{a_1^2} X^3 + \frac{a_3}{a_1} X^2 Z. \tag{45}$$

Proof. [V2, Chapitre 9]. Vélu gives explicit formulae showing that C is isomorphic to a curve defined by push-out from D. □

In the setting of Proposition 4.14 we deduce C is either a collection of k elliptic normal curves each of degree n/k or a collection of k Néron polygons each of degree n/k. These correspond to the cases where D is a smooth cubic, respectively a nodal cubic. In the latter case the existence of a singular point on D shows that there exists $\mathbf{Z}/n\mathbf{Z} \hookrightarrow \langle M_P, M_Q \rangle$ a cyclic subgroup of order n fixing some point on C. Up to the action of $\mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z})$ we may suppose this subgroup is $\langle M_P \rangle$. Lemma 4.15 below tells us that we are at a rational cusp and we conclude by Lemma 4.11.

Lemma 4.15 *Let $(0 : a_1 : a_2 : \dots) \in A(n)$ and let C be the corresponding fibre of $\mathcal{A}(n) \to A(n)$. If C has a fixed point under $M_P^{n/k}$ then $a_i a_j = 0$ whenever $i \not\equiv \pm j \pmod{k}$.*

Proof. There exists $(x_0 : x_1 : \dots : x_{n-1}) \in C$ with $x_i = 0$ for $i \not\equiv i_0 \pmod{k}$. We choose r such that $x_r \neq 0$ and suppose $i \not\equiv \pm j \pmod{k}$. Then

$$\#\{(r \pm i)/2, (r \pm j)/2\} = 4$$

and by considering the corresponding leading 4×4 submatrix of (42) we find $a_i a_j = 0$ as required. □

We now sketch the proof of Theorem 4.13. For p a prime, Vélu [V2, Lemme 8.18] works directly from the equations (41) to show that every

point on $A(p)$ is either a rational cusp or satisfies the hypotheses of Proposition 4.14. It follows $A(p)$ consists of $Y(p)$ together with a single orbit under the action of $\mathrm{PSL}_2(\mathbf{Z}/p\mathbf{Z})$. Thus $A(p) = X(p)$ and the fibres of $\mathcal{A}(p) \to A(p)$ at the cusps are Néron polygons. Finally $\mathcal{A}(p) = \mathcal{X}(p)$ as claimed.

4.5 Alternative Criteria for Finding the Cusps

We restrict to $n \geq 5$ prime. The family $\mathcal{X}(n) \to X(n)$ consists of elliptic normal curves above the points of $Y(n)$ and Néron polygons above the cusps. One way to find the irrational cusps is to start with the rational cusps and then use the explicit description of $\overline{\rho} : \mathrm{PSL}_2(\mathbf{Z}/n\mathbf{Z}) \to \mathrm{PGL}_{(n-1)/2}$ given in §4.2. In this section we give some alternative criteria. The action (14) of $\boldsymbol{\mu}_n$ on $X(n)$ is generated by $\overline{\rho}(T)$. Up to this action we find the condition for $(0 : a_1 : a_2 : \dots)$ to be an irrational cusp is

$$\mathrm{rank}(a_{i-j})_{i,j=0}^{n-1} = 2. \tag{46}$$

Let C be the fibre of $\mathcal{X}(n) \to X(n)$ above $0_C = (0 : a_1 : a_2 : \dots)$.

Fixed point criterion. *The curve C degenerates if and only if some matrix in $\langle M_P, M_Q \rangle$ fixes a point on C.*

Proof. If C does not degenerate $\langle M_P, M_Q \rangle$ consists of translations and so has no fixed points. If C degenerates then M_P and M_Q act by rotating the Néron polygon. Thus some element of $\langle M_P, M_Q \rangle$ fixes the lines and so also fixes the points of intersection. □

If M_P fixes a point then Lemma 4.15 tells us we are at a rational cusp. Otherwise up to the action of $\boldsymbol{\mu}_n$ on $X(n)$ we may suppose M_Q fixes a point. But the fixed points under M_Q are $(1 : 1 : \dots : 1)$ and its translates under M_P. The condition (46) follows immediately from (42).

Flex alignment criterion. *The curve C degenerates if and only if there exist collinear points $R_0, \dots, R_{n-1}$ with $R_i \in C \cap \{x_i = 0\}$.*

Proof. If C is a Néron polygon then clearly such points $R_0, \dots, R_{n-1}$ exist. Conversely if the flexes line up on a line ℓ then C, being defined by quadrics, must contain ℓ. □

Some matrix in $\langle M_P, M_Q \rangle$ preserves the line ℓ. As before we may suppose this matrix is M_Q. Then $R_0, \dots, R_{n-1}$ are the points 0_C and its translates under M_Q. Again the condition (46) follows.

Lemma 4.16 *Let $x_0, x_1, \ldots, x_{n-1} \in K$ with all subscripts read mod n. Then the matrix $\mathrm{rank}(x_{i-j})_{i,j=0}^{n-1} \leq 2$ has rank 2 if and only if there exist non-zero $A, B \in K$ and distinct $\zeta_A, \zeta_B \in \boldsymbol{\mu}_n$ such that $x_i = A\zeta_A^i + B\zeta_B^i$.*

Proof. If the matrix has rank 2 then the x_i satisfy a second order recurrence relation $x_{i+1} + bx_i + cx_{i-1} = 0$. This may be written

$$\begin{pmatrix} x_i \\ x_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -c & -b \end{pmatrix} \begin{pmatrix} x_{i-1} \\ x_i \end{pmatrix}.$$

The 2×2 matrix has minimal polynomial $m(X) = X^2 + bX + c$. We require $m(X) | (X^n - 1)$. Since $\mathrm{char}(K) \nmid n$ it follows $m(X) = (X - \zeta_A)(X - \zeta_B)$ where ζ_A, ζ_B are distinct nth roots of unity. Thus $x_i = A\zeta_A^i + B\zeta_B^i$ as required. □

We use the lemma to interpret the condition (46). We have $a_i = A\zeta_A^i + B\zeta_B^i$. But $a_0 = 0$ and $a_{n-i} = -a_i$ forcing $A + B = 0$ and $\zeta_A \zeta_B = 1$. So the solutions to (46) are

$$(0 : a_1 : a_2 : \ldots) = (0 : \zeta - \zeta^{-1} : \zeta^2 - \zeta^{-2} : \ldots) \tag{47}$$

where ζ is a primitive nth root of unity. This description of the cusps is in agreement with our earlier calculations.

4.6 Calculations with $\mathrm{char}(K) = n$

We continue to take $n \geq 5$ prime, but now work over K an algebraically closed field with $\mathrm{char}(K) = n$. We consider the family of curves $\mathcal{A}(n) \to A(n)$ defined by (41) and (42), but do not attempt to relate these to any moduli problem. Let C be the fibre of $\mathcal{A}(n) \to A(n)$ above $0_C = (0 : a_1 : a_2 : \ldots)$. If 0_C is a rational cusp then C is a Néron polygon of degree n, exactly as before. It is easy to check $A(n)$ contains the point $\varpi := (0 : 1 : 2 : 3 : \ldots)$.

Proposition 4.17 *Let C be as above with 0_C not a rational cusp.*
(i) If $0_C \neq \varpi$ then C is an elliptic curve of degree n.
(ii) If $0_C = \varpi$ then C is a line with multiplicity n.

Proof. Since $a_1, a_2, \ldots, a_{(n-1)/2}$ are non-zero, we may follow Vélu's proof of Proposition 4.14. We deduce that $C \hookrightarrow \mathbf{P}^{n-1}$ is an irreducible curve of degree n and that the (non-reduced) group scheme $\boldsymbol{\mu}_n$ acts on C with quotient $\phi : C \to D$. Here D is the plane cubic defined by (45).

(i) If D is a smooth cubic then we recognise $\phi : C \to D$ as an inseparable isogeny of degree n. In particular C is an elliptic curve.
(ii) If D has a singular point, then *a priori* this could be either a node or a cusp. Either way C has a fixed point under M_Q. But the only fixed point under M_Q is $(1 : 1 : \ldots : 1)$ and the condition for C to contain this point is

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

Adapting Lemma 4.16 to the case $\operatorname{char}(K) = n$ gives $a_i = A + Bi$ for some $A, B \in K$. Since $a_0 = 0$ it follows $0_C = \varpi$.

It only remains to describe C in the case $0_C = \varpi$. Then C contains ϖ and its translates under M_Q and these lie on a line ℓ. Since C is defined by quadrics it must contain ℓ. We now know that $C \hookrightarrow \mathbf{P}^{n-1}$ is an irreducible curve of degree n which is set-theoretically a line. Although these conditions certainly do not suffice to determine C as a scheme, we shall be content to call C a line with multiplicity n. □

Remark 4.18 In the above proof $\phi : C \to D$ is set-theoretically an isomorphism. So in case (ii) the plane cubic D must have a cusp rather than a node. Substituting $a_i = i$ into the Weierstrass equation (45) gives

$$(Y - 3X + 2Z)^2 Z = -4(X - Z)^3 \tag{48}$$

and this is indeed the equation of a cuspidal cubic.

Remark 4.19 The linear subspaces preserved by M_Q are

$$\Pi^r := \{\, (f(0) : f(1) : \ldots : f(n-1)) \mid f(x) \in K[x] \text{ with } \deg f \leq r \,\}.$$

If $0_C = \varpi$ then C is set-theoretically equal to the line Π^1 and contains the point $\Pi^0 = (1 : 1 : \ldots : 1)$. This point is distinguished on C by its Zariski tangent space Π^3. All other points on C have tangent space Π^2.

Proposition 4.17 allows us to complete our proof of Proposition 3.10. In the case $n = 5$ we have $A(5) = \mathbf{P}^1$ and $\varpi = (1 : 2)$. Thus the condition for $T[\lambda, \tau_0, \ldots, \tau_4]$ to degenerate is $\beta(\lambda) = (\lambda - 3)^2 = 0$. In the case $n = 7$ we have $A(7) = \{a^3b + b^3c + c^3a = 0\}$ and $\varpi = (1 : 2 : 4)$. Thus the condition for $T[\lambda, \tau_0, \ldots, \tau_6]$ to degenerate is $\beta(\lambda) = (\lambda - 5)^3 = 0$.

We suspect the curves C appearing in Proposition 4.17(i) are elliptic normal curves. We are able to prove this in the cases $n = 5$ and 7.

Lemma 4.20 *Let $n = 5$ or 7 and let $(0 : a_1 : a_2 : \dots) \in A(n)$. Then the matrix $(a_{i-j})_{i,j=0}^{n-1}$ has either rank 2 or rank $n-1$.*

Proof. In the case $n = 5$ this is immediate. In the case $n = 7$ all the 6×6 Pfaffians are equal to $(a + 2b + 4c)^3$. It is easy to check that the line $a + 2b + 4c = 0$ meets $A(7)$ only at the point ϖ. □

The elliptic curve C passes through the points $0_C = (0 : a_1 : a_2 : \dots)$ and its translates under M_Q. By Lemma 4.20 these points span the hyperplane

$$H := \{x_0 + x_1 + \dots + x_{n-1} = 0\}.$$

Thus to prove C is (projectively) normal we are reduced to showing C is not contained in H. We give three proofs of this in the case $n = 5$, the last of which generalises to $n = 7$.

The first proof uses the fact that C is defined by quadrics. If C is contained in $H \cong \mathbf{P}^3$, then it lies in the intersection of two quadrics and so has degree at most 4. But we know C has degree 5 and this gives the required contradiction.

For our second proof we use computer algebra to give equations for the tangent line to C at $0 = (0 : a : b : -b : -a)$. The tangent line passes through the point

$$(10a^3b^3 : a(a^5 - 3b^5) : -b(3a^5 + b^5) : -b(3a^5 + b^5) : a(a^5 - 3b^5)).$$

Adding up the co-ordinates we find that the condition for C to lie in H is $2(a^2 - ab - b^2)^3 = 0$. Since $\mathrm{char}(K) = 5$ this is equivalent to $(a : b) = \varpi$. Similar calculations for $n = 7$ are possible but rather messy.

For our third proof we take $n = 5$ or 7 and recall C meets the hyperplane $H_0 = \{x_0 = 0\}$ at a single point, and likewise for the other co-ordinate hyperplanes, thanks to the action of M_Q. It therefore suffices to prove the cases $n = 5$ and 7 of the following conjecture.

Conjecture 4.21 *Let $n \geq 3$ prime, and let E/K be an elliptic curve with $E[n] \cong \mathbf{Z}/n\mathbf{Z}$. Then the divisors $\{nP \mid P \in E[n]\}$ span a complete linear system.*

We may prove this conjecture for $n = 5$ and 7 by means of a direct calculation. Indeed the curves in question are the D_λ with Weierstrass equation (2). We recall that $\mathbf{1} = (0, 0)$ generates $\mathbf{Z}/n\mathbf{Z} \hookrightarrow D_\lambda(K)$. In the case $n = 5$ we write

down rational functions $f_r \in \langle x^2, xy, x, y, 1\rangle$ with $(f_r) = 5.(r\mathbf{1}) - 5.0$. We obtain a 5×5 matrix

	x^2	xy	x	y	1
f_0	0	0	0	0	1
f_1	-1	1	0	1	0
f_2	2λ	-1	$\lambda^3 - 3\lambda^2$	$-\lambda^2 + \lambda$	λ^3
f_3	$-\lambda - 1$	-1	$\lambda^2 + 2\lambda$	$-\lambda^2 + \lambda$	$-\lambda^2$
f_4	$\lambda - 2$	-1	$2\lambda - 1$	-1	λ

with determinant $(\lambda^2 - \lambda - 1)^2(\lambda^2 - 6\lambda - 1)$. Since $\mathrm{char}(K) = 5$, this matrix is non-singular whenever D_λ is non-singular. In the case $n = 7$ the rational functions $f_r \in \langle x^3, x^2y, x^2, xy, y^2, x, y, 1\rangle$ for $0 \leq r \leq 6$ together with the equation for D_λ itself give an 8×8 matrix. In characteristic 7 this matrix is non-singular whenever D_λ is non-singular. Computing the f_r here is straightforward. Indeed, $f_1 = f$ is given by (10) and the remaining f_r follow from the substitutions envisaged in Remark 1.2.

To end this chapter we sketch an alternative proof of Proposition 4.17(i), specific to the cases $n = 5$ and 7, but which does not rely on Vélu's explicit formulae. First we express K as the residue field for some local field of characteristic zero, see [Se2, Chapter II, Theorem 3]. Then we deduce from our work in the case $\mathrm{char}(K) \neq n$ that C contains a curve C_1 of degree n and arithmetic genus 1. Since $0_C \neq \varpi$, Lemma 4.20 tells us that M_Q acts on C without fixed points and that the points of intersection of C with the hyperplanes H_i span H. From these observations it follows C_1 is irreducible and smooth. Then the above proof of Conjecture 4.21 in the cases $n = 5$ and 7 tells us C_1 is an elliptic normal curve. Finally C and C_1 are both defined by $n(n-3)/2$ quadrics and so $C = C_1$ as required.

Chapter 5

Descent Theorems over $\mathbf{Q}(\boldsymbol{\mu}_n)$

Let $n = 5$ or 7. In this chapter we generalise our first descent theorem to $K = \mathbf{Q}(\boldsymbol{\mu}_n)$. It is well known that K has class number 1 and ring of integers $\mathbf{Z}[\zeta]$ where ζ is a primitive nth root of unity. The unit group U_K is generated modulo torsion by the ratios $(\zeta^i - \zeta^{-i})/(\zeta^j - \zeta^{-j})$. For $\mathfrak{p}$ a prime we recall $\dim_n \mathcal{O}_\mathfrak{p}^\times/(\mathcal{O}_\mathfrak{p}^\times)^n = 1 + \mathrm{ord}_\mathfrak{p}(n)$, and indeed for $\mathfrak{p} \nmid n$ this is immediate by Hensel's lemma. At $\mathfrak{l} = (1-\zeta)$, the unique prime above n, we work with the filtration $\mathcal{O}_\mathfrak{l}^\times \supset U_1 \supset U_2 \supset \ldots$, where $U_r = \{x \in \mathcal{O}_\mathfrak{l}^\times \mid x \equiv 1 \pmod{\mathfrak{l}^r}\}$ and for $r \geq 1$ the quotient U_r/U_{r+1} is cyclic of order n.

5.1 Statement of the First Descent Theorem

Let $\lambda \in K$ not a cusp of $X_1(n)$. Let C_λ and D_λ be the n-isogenous elliptic curves introduced in §1.1. We define disjoint sets of primes

$$\begin{array}{rcl} \mathcal{A} & = & \{\ \mathfrak{p} \text{ prime} \mid \mathrm{ord}^*_\mathfrak{p}(\lambda) > 0\ \} \\ \mathcal{B} & = & \{\ \mathfrak{p} \text{ prime} \mid \mathrm{ord}^*_\mathfrak{p}(\eta(\lambda)) > 0\ \} \end{array} \tag{49}$$

where $\mathrm{ord}^*_\mathfrak{p}$ is as defined in §3.2 and η is the involution of $X_1(n)$ swapping over the rational and irrational cusps. We define $d = d(\lambda)$ as a function of the cusp number $c = c(\lambda)$ introduced in §1.1.

$n = 5$

c	0	1	2	3	4	5	6
d	0	0	1	2	3	4	4

$n = 7$

c	0	1	2	3	4
d	0	1	3	5	6

Theorem 3 *Let $n = 5$ or 7 and let $\lambda \in K$ not a cusp of $X_1(n)$. For $\mathcal{A}$, $\mathcal{B}$ defined by (49) and $d = d(\lambda)$ we write*

$$\begin{aligned} [\mathcal{A}] &= \{\, \theta \in K^\times/(K^\times)^n \mid \mathrm{ord}_{\mathfrak{p}}(\theta) \equiv 0 \pmod{n} \text{ for all } \mathfrak{p} \notin \mathcal{A} \,\} \\ I(\mathcal{B}, d) &= (\text{subgroup of } I_K/I_K^n \text{ generated by } \mathcal{B}) \oplus U_{n-d}/U_n. \end{aligned}$$

Then the Selmer group attached to the n-isogeny $\phi : C_\lambda \to D_\lambda$ is given by

$$S^{(\phi)}(C_\lambda/K) \cong \left\{ \theta \in [\mathcal{A}] \;\middle|\; \begin{array}{c} \theta \in (K_{\mathfrak{p}}^\times)^n \text{ for all } \mathfrak{p} \in \mathcal{B} \\ \text{and } \theta^{n-1} \equiv 0, 1 \pmod{\mathfrak{l}^{d+1}} \end{array} \right\}.$$

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

Remark 5.1 The pairing Ξ is again straightforward to compute. First we give a basis for $[\mathcal{A}]$ consisting of units and generators for the primes in $\mathcal{A}$. Then for each prime $\mathfrak{p} \in \mathcal{B}$ with $\mathfrak{p} \neq \mathfrak{l}$ we choose a non-trivial character $\chi_{\mathfrak{p}} : (\mathcal{O}_K/\mathfrak{p})^\times \to \mathbf{Z}/n\mathbf{Z}$ and compute $\chi_{\mathfrak{p}}$ on our basis for $[\mathcal{A}]$. To treat the conditions at $\mathfrak{l}$ we define characters $\chi_i : \mathcal{O}_{\mathfrak{l}}^\times \to \mathbf{Z}/n\mathbf{Z}$ via

$$\theta \equiv (1-\gamma)^{\chi_1(\theta)}(1-\gamma^2)^{\chi_2(\theta)} \ldots (1-\gamma^n)^{\chi_n(\theta)} \mod (K_{\mathfrak{l}}^\times)^n \qquad (50)$$

where $\gamma = 1 - \zeta$. The matrix representing Ξ has columns corresponding to $\chi_1, \ldots, \chi_d$. If $d = n - 1$ then we include the character χ_n precisely whenever the prime $\mathfrak{l}$ belongs to $\mathcal{B}$.

Remark 5.2 Replacing λ by $\eta(\lambda)$ in Theorem 3 leads to pairings Ξ represented by matrices of different sizes, even though the Selmer groups computed must be the same. When computing examples by hand we naturally choose to work with the smaller matrix.

Remark 5.3 Let $G := \mathrm{Gal}(K/\mathbf{Q})$. In many cases of interest the sets $\mathcal{A}$ and $\mathcal{B}$ are G-stable. For example this happens whenever C_λ and D_λ admit models over $\mathbf{Q}$. In these cases the pairing Ξ is G-equivariant, *i.e.*

$$\Xi(\sigma a, \sigma b) = \sigma\, \Xi(a, b) \qquad \text{for all } \sigma \in G.$$

We may thus simplify our calculations by first decomposing the G-modules $[\mathcal{A}]$ and $I(\mathcal{B}, d)$ into 1-dimensional submodules. We write ψ for the cyclotomic character $G \xrightarrow{\sim} (\mathbf{Z}/n\mathbf{Z})^\times$ and do not distinguish in our notation between characters and the 1-dimensional G-modules they describe. Thus $U_K/U_K^n \cong \psi \oplus \psi^2$, respectively $\psi \oplus \psi^2 \oplus \psi^4$, and $U_r/U_{r+1} \cong \psi^r$. The contribution from each rational prime p merely depends on how p splits in K.

5.2 Examples and Applications

Let $n = 5$ or 7 and let $\lambda \in K$ not a cusp of $X_1(n)$. Theorem 3 gives us information about both the Mordell-Weil groups $C_\lambda(K)$ and $D_\lambda(K)$ and the Tate-Shafarevich groups $Ш(C_\lambda/K)$ and $Ш(D_\lambda/K)$. We now make this explicit. Let $R = \operatorname{rank} C_\lambda(K) = \operatorname{rank} D_\lambda(K)$ and define $s, t \geq 1$ via $|C_\lambda(K)(n)| = n^s$ and $|D_\lambda(K)(n)| = n^t$. Theorem 3 together with the exact sequences

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

tells us $R = R_1 + R_2$ with $R_1, R_2 \geq 0$ and

$$\begin{aligned} |\mathcal{A}| + (n-1)/2 - \operatorname{rank}(\Xi) &= R_1 + t + 1 - s + \dim_n Ш(C_\lambda/K)[\phi] \\ |\mathcal{B}| + d - \operatorname{rank}(\Xi) &= R_2 + s + 1 - t + \dim_n Ш(D_\lambda/K)[\widehat{\phi}]. \end{aligned} \tag{51}$$

Thus the upper bound for the rank provided by first descent is

$$|\mathcal{A}| + |\mathcal{B}| + (n-1)/2 + d - 2 - 2\operatorname{rank}(\Xi). \tag{52}$$

Example 5.4 *Let $n = 5$ and $\lambda = 2$. Then $\mathcal{A} = \{2\}$, $\mathcal{B} = \{\mathfrak{p}_1, \mathfrak{p}_2\}$ and $d = 0$ where $(19) = \mathfrak{p}_1\mathfrak{p}_2$. Since $[\mathcal{A}] \cong 1 \oplus \psi \oplus \psi^2$ and $I(\mathcal{B}, d) \cong 1 \oplus \psi^2$ as G-modules, we know* $\operatorname{rank}(\Xi) \leq 1$. *But $5^2 \nmid 19^2 - 1$, so $\zeta \notin (\mathbf{F}_{19^2}^\times)^5$ and* $\operatorname{rank}(\Xi) = 1$. *Reducing modulo a few primes we learn $D_2(K)_{\mathrm{tors}} \cong \mathbf{Z}/5\mathbf{Z}$ and so $(x, y) = (1, (3 + \sqrt{5})/2)$ is a point of infinite order. By Theorem 3 we deduce*

$$\begin{aligned} C_2(K) &\cong \mathbf{Z}/5\mathbf{Z} \oplus \mathbf{Z} & Ш(C_2/K)(5) &= 0 \\ D_2(K) &\cong \mathbf{Z}/5\mathbf{Z} \oplus \mathbf{Z} & Ш(D_2/K)(5) &= 0. \end{aligned}$$

Example 5.5 *Let $n = 7$ and $\lambda = \eta(5)$. Then $\mathcal{A} = \emptyset$, $\mathcal{B} = \{\mathfrak{p}_1, \mathfrak{p}_2, 5\}$ and $d = 0$ where $(2) = \mathfrak{p}_1\mathfrak{p}_2$. Since $[\mathcal{A}] \cong \psi \oplus \psi^2 \oplus \psi^4$ and $I(\mathcal{B}, d) \cong 1 \oplus 1 \oplus \psi^3$ as G-modules, we know* $\operatorname{rank}(\Xi) \leq 2$. *But $7^2 \nmid 2^3 - 1$, so $\zeta \notin (\mathbf{F}_{2^3}^\times)^7$ and* $\operatorname{rank}(\Xi) \geq 1$. *If* $\operatorname{rank}(\Xi) = 1$ *then $\zeta + \zeta^{-1} \equiv 1 \pmod{\mathfrak{p}_1}$ and $\zeta + \zeta^{-1} \equiv 1 \pmod{\mathfrak{p}_2}$. This gives $\zeta + \zeta^{-1} \equiv 1 \pmod 2$ which is absurd. So* $\operatorname{rank}(\Xi) = 2$ *and by Theorem 3 we deduce*

$$\begin{aligned} C_5(K) &\cong \mathbf{Z}/7\mathbf{Z} & Ш(C_5/K)(7) &= 0 \\ D_5(K) &\cong \mathbf{Z}/7\mathbf{Z} & Ш(D_5/K)(7) &= 0. \end{aligned}$$

Let $\Sigma(\lambda) = \{\lambda, -1/\lambda\}$, respectively $\{\lambda, (\lambda-1)/\lambda, 1/(1-\lambda)\}$. For $\lambda \in K$ the curves C_λ and D_λ admit models over $\mathbf{Q}$ if and only if $\Sigma(\lambda)$ is G-stable. We obtain elliptic curves over $\mathbf{Q}$ with a labelled copy of the Tate twist $\mathbf{Z}/n\mathbf{Z}(k)$. For each $0 \le k < n-1$ these curves are parametrised by some twist of $Y_1(n)$. For E an elliptic curve over $\mathbf{Q}$ we write E^* for the 5- respectively -7-twist of E. Then the families under discussion are

$$n = 5 \begin{array}{c|cccc} k & 0 & 1 & 2 & 3 \\ \hline & D_\lambda & C_\lambda & D^*_\lambda & C^*_\lambda \end{array} \qquad n = 7 \begin{array}{c|cccccc} k & 0 & 1 & 2 & 3 & 4 & 5 \\ \hline & D_\lambda & C_\lambda & B^*_\rho & D^*_\lambda & C^*_\lambda & B_\rho \end{array}.$$

We give equations for the curves B_ρ in Appendix B. We choose our coordinate ρ with cusps at the roots of

$$\rho^3 - \rho^2 - 2\rho + 1 = 0 \quad \text{and} \quad \rho^3 - 2\rho^2 - \rho + 1 = 0.$$

The automorphisms of $\mathbf{P}^1$ permuting these cusps are generated by $\rho \mapsto 1/\rho$ and $\rho \mapsto 1-\rho$. We find $B_\rho \cong B_{(\rho-1)/\rho}$ whereas B_ρ and $B^*_{1-\rho}$ are related by 7-isogeny.

We may exhibit elements of the Tate-Shafarevich group by comparing two different 5-descents. As we saw in §2.3 we need only apply our first descent theorem for $\lambda = \tau^5$ and $\lambda = \tau f(\tau)/g(\tau)$ and compare estimates. In the case $\tau = 1$ the curves in question are

$$C_1 \cong D_{11} \cong X_0(11) \quad \text{and} \quad D_1 \cong X_1(11).$$

The next two examples duplicate some of the work in [CS].

Example 5.6 *Let $n = 5$ and $\lambda = 1$. Then $\mathcal{A} = \emptyset$, $\mathcal{B} = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4\}$ and $d = 0$ where $(11) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$. Since $[\mathcal{A}] \cong \psi \oplus \psi^2$ is generated by ζ and $\phi = 1 + \zeta + \zeta^4$ with $\zeta, \phi \not\equiv \pm 1 \pmod{\mathfrak{p}_1}$ it follows* $\operatorname{rank}(\Xi) = 2$. *Theorem 3 gives*

$$C_1(K) \cong (\mathbf{Z}/5\mathbf{Z})^2 \qquad Ш(C_1/K)(5) = 0$$
$$D_1(K) \cong \mathbf{Z}/5\mathbf{Z} \qquad Ш(D_1/K)(5) = 0.$$

Example 5.7 *Let $n = 5$ and $\lambda = 11$. Then $\mathcal{A} = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4\}$, $\mathcal{B} = \emptyset$ and $d = 0$. We have $[\mathcal{A}] \cong 1 \oplus \psi \oplus \psi \oplus \psi^2 \oplus \psi^2 \oplus \psi^3$ and $D_{11}[5] \cong 1 \oplus \psi$. Since $C_1 \cong D_{11}$, the last example and Theorem 3 give*

$$Ш(C_{11}/K)(5) \cong \psi \oplus \psi^2 \oplus \psi^2 \oplus \psi^3.$$

Noting $[K : \mathbf{Q}]$ is prime to 5 it follows $Ш(C^*_{11}/\mathbf{Q})(5) \cong (\mathbf{Z}/5\mathbf{Z})^2$. According to Cremona's tables [Cr] this curve C^*_{11} =275B3 is the first curve, by conductor, with Ш of analytic order 25.

Example 5.8 *Let $n = 7$ and let $\lambda \in \mathbf{Q}(\boldsymbol{\mu}_7) \cap \mathbf{R}$ with $\eta(\lambda) = \lambda$. The curves C_λ and D_λ admit complex multiplication by some order in $\mathbf{Q}(\sqrt{-7})$. Since the sets of primes $\mathcal{A}$ and $\mathcal{B}$ are disjoint we must have $\mathcal{A} = \mathcal{B} = \emptyset$. Similarly from the identity $c(\lambda) + c(\eta(\lambda)) = 4$ we deduce $c(\lambda) = 2$ and $d(\lambda) = 3$. Thus*

$$[\mathcal{A}] \cong \psi \oplus \psi^2 \oplus \psi^4 \quad \text{and} \quad I(\mathcal{B}, d) \cong \psi^4 \oplus \psi^5 \oplus 1.$$

Now $\Xi : [\mathcal{A}] \times I(\mathcal{B}, d) \to \boldsymbol{\mu}_7$ is G-equivariant and the proof of Theorem 3 reveals $\ker_L(\Xi) \cong \ker_R(\Xi)$ as G-modules. Thus $\operatorname{rank}(\Xi) = 2$ and

$$\operatorname{rank} C_\lambda(K) = \operatorname{rank} D_\lambda(K) = 0.$$

Remark 5.9 The curves in Example 5.8 each admit a pair of models over $\mathbf{Q}$. These models are B_ρ and B_ρ^* for $\rho = 0, 1, \infty$ and $\rho = -1, \frac{1}{2}, 2$, equivalently the curves 49A in Cremona's tables [Cr]. The quotient of the Klein quartic

$$X(7) = \{a^3b + b^3c + c^3a = 0\}$$

by the automorphism $(a : b : c) \mapsto (c : a : b)$ is the elliptic curve $X_0(49)$. We refer to [E, §2.1] for explicit formulae. We have just shown that this curve has rank 0 over $K = \mathbf{Q}(\boldsymbol{\mu}_7)$. A straightforward calculation now shows that the only K-rational points on the Klein quartic are the 24 points of inflection.

Remark 5.10 We have no analogue of Example 5.8 in the case $n = 5$ since the fixed points of η are defined over $\mathbf{Q}(\boldsymbol{\mu}_5, \sqrt{-1})$ but not over $\mathbf{Q}(\boldsymbol{\mu}_5)$. This may be related to the fact $\mathbf{Q}(\sqrt{-5})$ has Hilbert class field $\mathbf{Q}(\sqrt{5}, \sqrt{-1})$.

The following problem was suggested by John Coates. Our motivation is to find examples to illustrate the theory in [CS]. We continue to write $K = \mathbf{Q}(\boldsymbol{\mu}_n)$ with $n = 5$ or 7.

Problem 5.11 *Find some examples of elliptic curves E/K satisfying*
(a) $\operatorname{rank} E(K) = 0$ *and* $Ш(E/K)(n) = 0$.
(b) E admits a model over $\mathbf{Q}$.
(c) The Tamagawa numbers $c_\mathfrak{p} = [E(K_\mathfrak{p}) : E_0(K_\mathfrak{p})]$ are prime to n.
(d) E has good ordinary reduction at $\mathfrak{l} = (1 - \zeta)$.
(e) E does not admit complex multiplication (over $\overline{K}$).

It is known that the curve $X_1(11)$ satisfies all these conditions for $n = 5$. We use Theorem 3 to give further examples with $E(K)[n] \neq 0$. Accordingly

we take $E = D_\lambda$ for some $\lambda \in K$. Condition (b) tells us that the set $\Sigma(\lambda)$ is G-stable and in particular $\lambda \in \mathbf{R}$. Condition (c) tells us that the set $\mathcal{A}$ defined by (49) must be empty. Indeed in the case of split multiplicative reduction the Tamagawa number $c_\mathfrak{p}$ is $\mathrm{ord}_\mathfrak{p}(\Delta)$, so our claim follows by Lemma 1.4 and inspection of the discriminant $\Delta(D_\lambda)$ recorded in §1.1.

In the case $n = 5$ the condition $\mathcal{A} = \emptyset$ tells us $\lambda \in K$ is a unit. We have either $\lambda = \pm 1$ corresponding to $X_1(11)$ or $\lambda = \pm\phi^j$ for some odd integer j. We apply Theorem 3 for $|j| \leq 23$ and tabulate the results in Appendix D.

In the case $n = 7$ the condition $\mathcal{A} = \emptyset$ tells us $\lambda \in K$ is an exceptional unit, *i.e.* both λ and $\lambda - 1$ are units. In any number field it is known there are only finitely many exceptional units. Nagell [Na, Théorème 8] has determined all the exceptional units in $\mathbf{Q}(\boldsymbol{\mu}_7) \cap \mathbf{R}$. The solutions satisfying (b) are the roots of

$$\lambda^3 - t\lambda^2 + (t-3)\lambda + 1 = 0 \tag{53}$$

for $t = 1,\ 2,\ -5,\ 8,\ -12,\ 15,\ -1259,\ 1262$. For a discussion of this problem of computing exceptional units, and further references to the literature, see [Sm] and [Ni]. The roots of (53) for $t = 8$ are the irrational cusps of $X_1(7)$. We apply Theorem 3 for the remaining 7 curves and tabulate the results in Appendix D.

All the curves in Tables 9 and 10 with entry $R = 0$ satisfy (a), (b) and (c). We check (d) using Lemma 1.6 and check (e) by computing the j-invariant and comparing with the table in [Si2]. Finally we arrive at some solutions to Problem 5.11 which we list by giving their Cremona labels

$$n = 5 \quad \text{11A3, 150A1, 150A2, 2350N1} \qquad\qquad n = 7 \quad \text{294B1, 490K1.}$$

In each case reducing modulo a few primes we learn $E(K)(n) \cong \mathbf{Z}/n\mathbf{Z}$. By inspection of the table of §1.2 the reduction map $E(K)(n) \to \tilde{E}(\mathcal{O}_K/\mathfrak{l})(n)$ is an isomorphism. It follows from [CS, Chapter 3] that each curve on our list has rank 0 over $\mathbf{Q}(\boldsymbol{\mu}_{n^\infty})$.

5.3 Computation of Selmer Groups

Let $n = 5$ or 7. Let $\lambda \in K$ not a cusp of $X_1(n)$ and let $\mathcal{A}$, $\mathcal{B}$ and d be as defined in §5.1. In this section we prove that the Selmer group $S^{(\phi)}(C_\lambda/K)$ is as described by Theorem 3. The definition (8) reads

$$S^{(\phi)}(C_\lambda/K) = \{\, \theta \in K^\times/(K^\times)^n \mid C_{\lambda,\theta}(K_\mathfrak{p}) \neq \emptyset \text{ for all } \mathfrak{p} \,\}. \tag{54}$$

For $\theta \in K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^n$ the exact sequence (7) tells us

$$C_{\lambda,\theta}(K_\mathfrak{p}) \neq \emptyset \iff \theta \in \mathrm{im}\left(\delta : D_\lambda(K_\mathfrak{p}) \to K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^n\right). \tag{55}$$

Proposition 5.12 below describes the image of δ. If $\mathfrak{p} \neq \mathfrak{l}$ this description is an immediate consequence of Proposition 3.12 and the observation

$$\beta(\lambda) \equiv 0 \pmod{\mathfrak{p}} \iff \mathrm{ord}_\mathfrak{p}^*(\eta(\lambda)) > 0. \tag{56}$$

Proposition 5.12 *The map $\delta = \delta_\phi$ has image*

$$\mathrm{im}\,\delta = \begin{cases} K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^n & \text{if } \mathfrak{p} \in \mathcal{A} \\ \mathcal{O}_\mathfrak{p}^\times/(\mathcal{O}_\mathfrak{p}^\times)^n & \text{if } \mathfrak{p} \notin \mathcal{A} \cup \mathcal{B} \text{ and } \mathfrak{p} \neq \mathfrak{l} \\ 0 & \text{if } \mathfrak{p} \in \mathcal{B}. \end{cases}$$

If $\mathfrak{p} \notin \mathcal{A} \cup \mathcal{B}$ and $\mathfrak{p} = \mathfrak{l}$ then $\mathrm{im}\,\delta = U_{d+1}(K_\mathfrak{l}^\times)^n/(K_\mathfrak{l}^\times)^n$.

Since we are working over $K = \mathbf{Q}(\boldsymbol{\mu}_n)$ we may identify $\mathbf{Z}/n\mathbf{Z} \cong \boldsymbol{\mu}_n$ and so have connecting maps

$$\begin{aligned} \delta_\phi &: D_\lambda(K_\mathfrak{p}) \to K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^n \\ \delta_{\widehat{\phi}} &: C_\lambda(K_\mathfrak{p}) \to K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^n. \end{aligned}$$

Tate local duality tells us $\mathrm{im}\,\delta_\phi$ and $\mathrm{im}\,\delta_{\widehat{\phi}}$ are exact annihilators with respect to the norm residue symbol

$$(\cdot,\cdot)_\mathfrak{p} : K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^n \times K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^n \to \boldsymbol{\mu}_n.$$

We define the "unit" and "not ramified" subgroups

$$\begin{aligned} H^1_{\mathrm{un}}(K_\mathfrak{p}, \boldsymbol{\mu}_n) &= \{\, \theta \in K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^n \mid \mathrm{ord}_\mathfrak{p}(\theta) \equiv 0 \pmod{n} \,\} \\ H^1_{\mathrm{nr}}(K_\mathfrak{p}, \boldsymbol{\mu}_n) &= \{\, \theta \in K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^n \mid K_\mathfrak{p}(\sqrt[n]{\theta})/K_\mathfrak{p} \text{ is unramified} \,\} \end{aligned}$$

and recall from §1.4 that these are exact annihilators with respect to the norm residue symbol. If $\mathfrak{p} \neq \mathfrak{l}$ then $H^1_{\mathrm{un}}(K_\mathfrak{p}, \boldsymbol{\mu}_n) = H^1_{\mathrm{nr}}(K_\mathfrak{p}, \boldsymbol{\mu}_n) = \mathcal{O}_\mathfrak{p}^\times/(\mathcal{O}_\mathfrak{p}^\times)^n$ is a maximal isotropic subspace of $K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^n$. Thus Proposition 5.12 is compatible with Tate local duality in the sense that if we replace λ by $\eta(\lambda)$ then $\mathrm{im}\,\delta$ is replaced by its exact annihilator. For $\mathfrak{p} = \mathfrak{l}$ we check the compatibility first, as this will shorten our proofs. We begin with a detailed description of the norm residue symbol $(\cdot,\cdot)_\mathfrak{l}$.

Lemma 5.13 *Let* $U_r' = U_r(K_\mathfrak{l}^\times)^n/(K_\mathfrak{l}^\times)^n$. *Then*

$$K_\mathfrak{l}^\times/(K_\mathfrak{l}^\times)^n \supset U_1' \supset U_2' \supset \ldots \supset U_n' \supset U_{n+1}' = 0$$

and for $1 \le r < s \le n+1$ *we identify* $U_r'/U_s' = U_r/U_s$.
(i) $H^1_{\mathrm{un}}(K_\mathfrak{l}, \boldsymbol{\mu}_n) = U_1'$ *and* $H^1_{\mathrm{nr}}(K_\mathfrak{l}, \boldsymbol{\mu}_n) = U_n'$.
(ii) The subgroups U_r' *and* U_{n+1-r}' *are exact annihilators.*
(iii) The norm residue symbol induces a non-degenerate pairing

$$U_1/U_n \times U_1/U_n \to \boldsymbol{\mu}_n$$

and the subspace generated by U_K *is a maximal isotropic subspace.*

Proof. See [CF, Exercise 2] or [W, Exercise 9.3]. For (iii) we note that the natural map $U_K/U_K^n \to U_1'/U_n'$ is injective since K has no unramified abelian extensions. The image is isotropic by Lemmas 1.19 and 1.20 and maximally isotropic by counting. □

By Lemma 1.5(iii) and the table of §5.1

$$d(\lambda) + d(\eta(\lambda)) = n - 1. \tag{57}$$

Thus Proposition 5.12 in the case $\mathfrak{p} = \mathfrak{l}$ is compatible with Tate local duality. It therefore suffices to prove the proposition for, say, $c(\lambda) \le c_{\max}/2$. If $c(\lambda) = 0$ then we are already done by Proposition 3.12. The next two lemmas treat the case $0 < c(\lambda) < c_{\max}$.

Lemma 5.14 *Let* $\lambda \in K_\mathfrak{l}$ *with* $0 < c(\lambda) < c_{\max}$. *Then* $c(\lambda) = \mathrm{ord}_\mathfrak{l}(\lambda - u)$ *where* u *is any irrational cusp and*

$$\mathrm{ord}_\mathfrak{l}(\beta'(\lambda)) = \mathrm{ord}_\mathfrak{l}(\alpha(\lambda) - \alpha(u)) = \begin{cases} \mathrm{ord}_\mathfrak{l}(\lambda - u) & \text{if } n = 5 \\ 2\,\mathrm{ord}(\lambda - u) & \text{if } n = 7. \end{cases}$$

Proof. The only subtle part is proving $\mathrm{ord}_\mathfrak{l}(\alpha(\lambda) - \alpha(u)) = 2\,\mathrm{ord}_\mathfrak{l}(\lambda - u)$ in the case $n = 7$. We first compute $\mathrm{ord}_\mathfrak{l}(\alpha'(u)) = c_{\max}$ and $\mathrm{ord}_\mathfrak{l}(\alpha''(u)) = 0$ and then consider the Taylor series expansion of $\alpha(\lambda)$ about u. □

Lemma 5.15 *Let* $\lambda \in K_\mathfrak{l}$ *with* $0 < c(\lambda) < c_{\max}$ *and let* $t = \mathrm{ord}_\mathfrak{l}(\beta'(\lambda))$. *Then the map* $\delta : D_\lambda(K_\mathfrak{l}) \to K_\mathfrak{l}^\times/(K_\mathfrak{l}^\times)^n$ *has image* $U_t' = U_t(K_\mathfrak{l}^\times)^n/(K_\mathfrak{l}^\times)^n$.

Proof. By the proof of Lemma 1.6 our Weierstrass equation (2) for D_λ is minimal. We write $E = D_\lambda$ and recall from [Si1, Chapter VII] there is a filtration

$$E(K_\mathfrak{l}) \supset E_0(K_\mathfrak{l}) \supset E_1(K_\mathfrak{l}).$$

If $t < n-1$ then Proposition 3.18 with $\nu = 1$ tells us that the image of δ restricted to $E_1(K_\mathfrak{l})$ is U'_{t+1}. Now $E_0(K_\mathfrak{l})/E_1(K_\mathfrak{l}) \cong \mathbf{Z}/n\mathbf{Z}$ is generated by $\mathbf{1} = (0,0)$. So the image of δ restricted to $E_0(K_\mathfrak{l})$ is generated by $\alpha(\lambda)$ and U'_{t+1}. But Corollary 3.13 and Lemma 5.14 imply $\alpha(\lambda)$ is a generator for U'_t/U'_{t+1}. So δ restricted to $E_0(K_\mathfrak{l})$ has image U'_t. The additive reduction tells us the Tamagawa number $[E(K_\mathfrak{l}) : E_0(K_\mathfrak{l})]$ is at most 4 and so prime to n. This proves the lemma in the case $t < n-1$ and the general case follows by Tate local duality. □

This completes the proof of Proposition 5.12.

Remark 5.16 We briefly indicate how we may prove Proposition 5.12 without using Tate local duality. For the proof of Lemma 5.15 it remains to extend the Hensel lemma calculations of §3.3 to treat the case $t \geq n-1$. If we write $F(z) = 1 + \gamma_1 z + \ldots + \gamma_n z^n + \ldots$ it turns out the correct modification to Lemma 3.17(i) is $\mathrm{ord}_\mathfrak{l}(\gamma_1 - n\gamma_n) = t$.

In the case $c(\lambda) = c_{\max}$ our push-out calculations are useless since (2) is no longer a minimal Weierstrass equation. However, replacing λ by $\eta(\lambda)$, it suffices to find the image of

$$\delta_{\widehat{\phi}} : C_\lambda(K_\mathfrak{l}) \to K_\mathfrak{l}^\times/(K_\mathfrak{l}^\times)^n$$

in the case $c(\lambda) = 0$. We take $C_\lambda \hookrightarrow \mathbf{P}^{n-1}$ with the equations of Proposition 3.7 and let $\{h(x_0, \ldots, x_{n-1}) = 0\}$ be the hyperplane cutting out the divisor $n.0$. We then compute the image of $\delta_{\widehat{\phi}}$ via push-out from C_λ using the rational function

$$h(x_0, \zeta^{-1}x_1, \ldots, \zeta x_{n-1})/h(x_0, x_1, \ldots, x_{n-1}).$$

Proposition 5.17 *Let $\lambda \in K$ not a cusp of $X_1(n)$. Then*

$$S^{(\phi)}(C_\lambda/K) \cong \left\{ \theta \in [\mathcal{A}] \;\middle|\; \begin{array}{l} \theta \in (K_\mathfrak{p}^\times)^n \text{ for all } \mathfrak{p} \in \mathcal{B} \\ \quad \text{and } \theta^{n-1} \equiv 0, 1 \pmod{\mathfrak{l}^{d+1}} \end{array} \right\}$$

$$S^{(\widehat{\phi})}(D_\lambda/K) \cong \left\{ \theta \in [\mathcal{B}] \;\middle|\; \begin{array}{l} \theta \in (K_\mathfrak{p}^\times)^n \text{ for all } \mathfrak{p} \in \mathcal{A} \\ \quad \text{and } \theta^{n-1} \equiv 0, 1 \pmod{\mathfrak{l}^{n-d}} \end{array} \right\}.$$

Proof. The description of $S^{(\phi)}(C_\lambda/K)$ is immediate from the definition (54) and Proposition 5.12. The description of $S^{(\widehat{\phi})}(D_\lambda/K)$ follows on replacing λ by $\eta(\lambda)$. □

5.4 Proof of the First Descent Theorem over Q

We use Proposition 5.17 to give an alternative proof of our first descent theorem over $\mathbf{Q}$. The idea is to relate $S^{(\phi)}(C_\lambda/K)$ and $S^{(\widehat{\phi})}(D_\lambda/K)$ via the nth power reciprocity law and then to descend to a statement about Selmer groups over $\mathbf{Q}$. We obtain a proof closer to the sketch given in §2.1.

Let $G = \mathrm{Gal}(K/\mathbf{Q})$ and let $\psi : G \xrightarrow{\sim} (\mathbf{Z}/n\mathbf{Z})^\times$ be the cyclotomic character. For A a G-module, written multiplicatively, and $\chi : G \to (\mathbf{Z}/n\mathbf{Z})^\times$ a character we adopt the notation

$$A^\chi = \{\, a \in A \mid \sigma(a) = a^{\chi(\sigma)} \text{ for all } \sigma \in G \,\}.$$

The restriction maps give isomorphisms

$$\begin{array}{rcl} H^1(\mathbf{Q}, \boldsymbol{\mu}_n) & = & (K^\times/(K^\times)^n)^1 \\ \pi : H^1(\mathbf{Q}, \mathbf{Z}/n\mathbf{Z}) & \xrightarrow{\sim} & (K^\times/(K^\times)^n)^\psi \end{array} \tag{58}$$

where π depends on a choice of isomorphism $\mathbf{Z}/n\mathbf{Z} \cong \boldsymbol{\mu}_n$.

Lemma 5.18 *Let $p \equiv 0, 1 \pmod n$ and let $\xi^{(p)} \in H^1(\mathbf{Q}, \mathbf{Z}/n\mathbf{Z})$ describe $F^{(p)}$, the degree n cyclic extension of $\mathbf{Q}$ unramified outside p.*
(i) If $p \equiv 1 \pmod n$ then $\pi\xi^{(p)}$ is a product of primes above p.
(ii) If $p = n$ then $\pi\xi^{(n)}$ is a primitive nth root of unity.
Moreover in case (i) $\pi\xi^{(p)} \in U_n(K_\mathfrak{l}^\times)^n$ whereas in case (ii) $\pi\xi^{(n)} \notin U_2(K_\mathfrak{l}^\times)^n$.

Proof. The element $\pi\xi^{(p)}$ is a Kummer generator for $KF^{(p)}/K$ and the lemma follows from the fact this extension is unramified outside p. □

Let $\lambda \in \mathbf{Q}$ not a cusp of $X_1(n)$. The maps (58) induce isomorphisms

$$\begin{array}{rcl} S^{(\phi)}(C_\lambda/\mathbf{Q}) & \cong & S^{(\phi)}(C_\lambda/K)^1 \\ S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q}) & \cong & S^{(\phi)}(C_{\eta(\lambda)}/K)^\psi. \end{array} \tag{59}$$

The crucial point here is that $[K : \mathbf{Q}]$ is prime to n, so the torsor $T/\mathbf{Q}$ has points everywhere locally if and only if T/K has points everywhere locally. For a detailed account of this argument see [Sw].

We write $\mathcal{A}_{\mathbf{Q}}$ and $\mathcal{B}_{\mathbf{Q}}$ for the sets of rational primes defined in §2.1 and $\mathcal{A}_K$, $\mathcal{B}_K$ and d_K for the quantities defined in §5.1. Then $\mathcal{A}_K$ is precisely the set of primes above $\mathcal{A}_{\mathbf{Q}}$, and $\mathcal{B}_K$ contains all the primes above $\mathcal{B}_{\mathbf{Q}} \setminus \{n\}$. The condition for $n \in \mathcal{B}_{\mathbf{Q}}$ is equivalent to $d_K = n - 1$. By Proposition 5.17 and Lemma 5.18 we deduce

$$\begin{array}{rcl} S^{(\phi)}(C_\lambda/\mathbf{Q}) & \cong & \{a \in [\mathcal{A}_{\mathbf{Q}}] \mid a \in (\mathbf{Q}_p^\times)^n \text{ for all } p \in \mathcal{B}_{\mathbf{Q}}\} \\ S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q}) & \cong & \{b \in \langle \mathcal{B}_{\mathbf{Q}} \rangle \mid \pi b \in (K_{\mathfrak{p}}^\times)^n \text{ for all } \mathfrak{p}|p \text{ with } p \in \mathcal{A}_{\mathbf{Q}}\} \end{array} \tag{60}$$

where the notation $[\ ]$ and $\langle\ \rangle$ is retained from §3.4. For the rest of this section let us write $\mathcal{A} = \mathcal{A}_{\mathbf{Q}}$ and $\mathcal{B} = \mathcal{B}_{\mathbf{Q}}$.

We define $\Xi : [\mathcal{A}] \times \langle \mathcal{B} \rangle \to \boldsymbol{\mu}_n$ via

$$\Xi(a,b) = \prod_{p \in \mathcal{B}} \prod_{\mathfrak{p}|p} (a, \pi b)_{\mathfrak{p}} = \prod_{p \in \mathcal{A}} \prod_{\mathfrak{p}|p} (\pi b, a)_{\mathfrak{p}} \tag{61}$$

where the two expressions given are equal by the product formula. Indeed if $p \notin \mathcal{A} \cup \mathcal{B}$ then $a \in H^1_{\mathrm{un}}(K_{\mathfrak{p}}, \boldsymbol{\mu}_n)$ and $\pi b \in H^1_{\mathrm{nr}}(K_{\mathfrak{p}}, \boldsymbol{\mu}_n)$ so the term $(a, \pi b)_{\mathfrak{p}}$ makes no contribution. If $n \notin \mathcal{B}$ then (61) is equivalent to the more appealing definition $\Xi(a,b) = (a/\pi b) = (\pi b/a)$ where $(\cdot/\cdot)$ is the power residue symbol.

Lemma 5.19 *Let $\Xi : [\mathcal{A}] \times \langle \mathcal{B} \rangle \to \boldsymbol{\mu}_n$ be the pairing defined above.*
(i) If $a \in [\mathcal{A}]$ and $p \in \mathcal{B}$ then $\Xi(a, \xi^{(p)}) = 1 \iff a \in (\mathbf{Q}_p^\times)^n$.
(ii) If $p \in \mathcal{A}$ and $b \in \langle \mathcal{B} \rangle$ then $\Xi(p,b) = 1 \iff \pi b \in (K_{\mathfrak{p}}^\times)^n$ for all $\mathfrak{p}|p$.

Proof. The action of $\mathrm{Gal}(K/\mathbf{Q})$ tells us the term $(a, \pi b)_{\mathfrak{p}}$ is independent of the choice of $\mathfrak{p}|p$.
(i) If $p \neq n$ and $\mathfrak{p}$ is any prime of K above p then

$$\Xi(a, \xi^{(p)}) = 1 \iff (a, \xi^{(p)})_{\mathfrak{p}} = 1 \iff (a/\mathfrak{p}) = 1 \iff a \in (\mathbf{Q}_p^\times)^n.$$

If $p = n$ then $\Xi(a, \xi^{(n)}) = (\pi \xi^{(n)}/a) = (\zeta/a)$ and by Euler's criterion

$$\Xi(a, \xi^{(n)}) = 1 \iff a^{n-1} \equiv 1 \pmod{n^2} \iff a \in (\mathbf{Q}_p^\times)^n.$$

(ii) If $\mathfrak{p}$ is any prime of K above p then

$$\Xi(p,b) = 1 \iff (\pi b, p)_{\mathfrak{p}} = 1 \iff (\pi b/\mathfrak{p}) = 1 \iff \pi b \in (K_{\mathfrak{p}}^\times)^n.$$

□

Finally (60) and Lemma 5.19 give

$$\begin{array}{rcll} S^{(\phi)}(C_\lambda/\mathbf{Q}) & \cong & \{a \in [\mathcal{A}] \mid \Xi(a, \xi^{(p)}) = 1 \text{ for all } p \in \mathcal{B}\} & = \ \ker_L(\Xi) \\ S^{(\widehat{\phi})}(D_\lambda/\mathbf{Q}) & \cong & \{b \in \langle \mathcal{B} \rangle \mid \Xi(p,b) = 1 \text{ for all } p \in \mathcal{A}\} & = \ \ker_R(\Xi). \end{array}$$

This completes our alternative proof of Theorem 1.

Remark 5.20 The pairing $\Xi = \Xi_{\text{Hilb}}$ defined here is related to $\Xi = \Xi_{\text{Tate}}$ defined in §3.4 via

$$-\Xi_{\text{Tate}}(a,b) = \text{Ind}_\zeta\, \Xi_{\text{Hilb}}(a,b) \tag{62}$$

where Ind_ζ is the inverse of the map $\mathbf{Z}/n\mathbf{Z} \cong \boldsymbol{\mu}_n$ used to construct π. This follows from the relationship between the Tate pairing and the Hilbert norm residue symbol. We recall that the restriction map $\text{Br}(\mathbf{Q}_p) \to \text{Br}(K_\mathfrak{p})$ satisfies inv res $= [K_\mathfrak{p} : \mathbf{Q}_p]$ inv. This accounts for the factor $[K : \mathbf{Q}] \equiv -1 \pmod{n}$ in the above formula.

5.5 Proof of the First Descent Theorem over $\mathbf{Q}(\boldsymbol{\mu}_n)$

We now complete the proof of Theorem 3. Proposition 5.17 gives a description of the Selmer groups attached to the isogeny ϕ and its dual. So it only remains to prove the following version of the power reciprocity law.

Proposition 5.21 *Let $n = 5$ or 7 and let $K = \mathbf{Q}(\boldsymbol{\mu}_n)$. Let $\mathcal{A}, \mathcal{B}$ be disjoint finite sets of primes of K. Let $0 \le d \le n-1$ be an integer, and suppose if $\mathfrak{l} \in \mathcal{A}$ then $d = 0$, and if $\mathfrak{l} \in \mathcal{B}$ then $d = n-1$. Define*

$$\begin{aligned} [\mathcal{A}] &= \{\, a \in K^\times/(K^\times)^n \mid \text{ord}_\mathfrak{p}(a) \equiv 0 \pmod{n} \text{ for all } \mathfrak{p} \notin \mathcal{A} \,\} \\ I(\mathcal{B}, d) &= (\text{subgroup of } I_K/I_K^n \text{ generated by } \mathcal{B}) \oplus U_{n-d}/U_n. \end{aligned}$$

Then there is a pairing $\Xi : [\mathcal{A}] \times I(\mathcal{B}, d) \to \boldsymbol{\mu}_n$ with

$$\begin{aligned} \ker_L(\Xi) &\cong \{a \in [\mathcal{A}] \mid a \in (K_\mathfrak{p}^\times)^n \text{ for all } \mathfrak{p} \in \mathcal{B} \text{ and } a^{n-1} \equiv 0, 1 \pmod{\mathfrak{l}^{d+1}}\} \\ \ker_R(\Xi) &\cong \{b \in [\mathcal{B}] \mid b \in (K_\mathfrak{p}^\times)^n \text{ for all } \mathfrak{p} \in \mathcal{A} \text{ and } b^{n-1} \equiv 0, 1 \pmod{\mathfrak{l}^{n-d}}\}. \end{aligned}$$

Proof. For $\mathcal{S}$ a set of primes of K we adopt the notation

$$\begin{aligned} [\mathcal{S}] &= \ker\left(H^1(K, \boldsymbol{\mu}_n) \to \textstyle\prod_{\mathfrak{p} \notin \mathcal{S}} H^1_{\text{un}}(K_\mathfrak{p}, \boldsymbol{\mu}_n)\right) \\ &= \{\, \theta \in K^\times/(K^\times)^n \mid \text{ord}_\mathfrak{p}(\theta) \equiv 0 \pmod{n} \text{ for all } \mathfrak{p} \notin \mathcal{S} \,\} \\ I(\mathcal{S}) &= \oplus_{\mathfrak{p} \in \mathcal{S}} H^1(K_\mathfrak{p}, \boldsymbol{\mu}_n)/H^1_{\text{un}}(K_\mathfrak{p}, \boldsymbol{\mu}_n) \\ &= \text{subgroup of } I_K/I_K^n \text{ generated by } \mathcal{S}. \end{aligned}$$

Since K has class number 1 there is an exact sequence

$$0 \to U_K/U_K^n \to [\mathcal{S}] \to I(\mathcal{S}) \to 0. \tag{63}$$

For $\mathcal{A}$, $\mathcal{B}$ and d as described in the proposition we define

$$\begin{aligned}[\mathcal{B},d] &= \{b \in [\mathcal{B}] \mid b^{n-1} \equiv 0,1 \pmod{\mathfrak{l}^{n-d}}\} \\ I(\mathcal{B},d) &= \begin{cases} \oplus_{\mathfrak{p}\in\mathcal{B}} H^1(K_\mathfrak{p},\boldsymbol{\mu}_n)/H^1_{\mathrm{nr}}(K_\mathfrak{p},\boldsymbol{\mu}_n) & \text{if } \mathfrak{l} \in \mathcal{B} \\ I(\mathcal{B}) \oplus U_{n-d}/U_n & \text{if } \mathfrak{l} \notin \mathcal{B}. \end{cases}\end{aligned}$$

By Lemma 5.13(iii) and applying the snake lemma to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_K/U_K^n & \longrightarrow & [\mathcal{B}] & \longrightarrow & I(\mathcal{B}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & U_1/U_n & \longrightarrow & I(\mathcal{B},n-1) & \longrightarrow & I(\mathcal{B}) & \longrightarrow & 0 \end{array}$$

we learn there is an exact sequence

$$0 \to [\mathcal{B}] \to I(\mathcal{B},n-1) \to (U_K/U_K^n)^\vee \to 0.$$

Since $[\mathcal{B},d] \subset [\mathcal{B}]$ is the inverse image of $I(\mathcal{B},d) \subset I(\mathcal{B},n-1)$ it follows

$$0 \to [\mathcal{B},d] \to I(\mathcal{B},d) \to (U_K/U_K^n)^\vee \tag{64}$$

is exact. We define pairings

$$\begin{aligned} \Xi &: [\mathcal{A}] \times I(\mathcal{B},d) \to \boldsymbol{\mu}_n\,; \quad (a,b) \mapsto \textstyle\prod_\mathfrak{p}(a,b)_\mathfrak{p} \\ \Xi' &: I(\mathcal{A}) \times [\mathcal{B},d] \to \boldsymbol{\mu}_n\,; \quad (a,b) \mapsto \textstyle\prod_\mathfrak{p}(b,a)_\mathfrak{p} \end{aligned}$$

where $(\cdot,\cdot)_\mathfrak{p}$ is the norm residue symbol. The assumptions on $\mathcal{A}$, $\mathcal{B}$ and d made in the statement of the proposition are sufficient for these pairings to be well-defined. The exact sequences (63) and (64) now give a diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & [\mathcal{B},d] & \longrightarrow & I(\mathcal{B},d) & \longrightarrow & (U_K/U_K^n)^\vee & & \\ & & \downarrow{\scriptstyle \Xi'} & & \downarrow{\scriptstyle \Xi} & & \| & & \\ 0 & \longrightarrow & I(\mathcal{A})^\vee & \longrightarrow & [\mathcal{A}]^\vee & \longrightarrow & (U_K/U_K^n)^\vee & \longrightarrow & 0 \end{array}$$

and the product formula for the norm residue symbol tells us that this diagram is commutative. We compute

$$\begin{aligned} \ker_L(\Xi) &= \{a \in [\mathcal{A}] \mid a \in (K_\mathfrak{p}^\times)^n \text{ for all } \mathfrak{p} \in \mathcal{B} \text{ and } a^{n-1} \equiv 0,1 \pmod{\mathfrak{l}^{d+1}}\} \\ \ker_R(\Xi) &\cong \ker_R(\Xi') \\ &= \{b \in [\mathcal{B},d] \mid b \in (K_\mathfrak{p}^\times)^n \text{ for all } \mathfrak{p} \in \mathcal{A}\} \\ &= \{b \in [\mathcal{B}] \mid b \in (K_\mathfrak{p}^\times)^n \text{ for all } \mathfrak{p} \in \mathcal{A} \text{ and } b^{n-1} \equiv 0,1 \pmod{\mathfrak{l}^{n-d}}\}. \end{aligned}$$

This completes the proof of Proposition 5.21 and so also of Theorem 3. We remark that our proof of Proposition 5.21 holds for n replaced by any odd regular prime. □

Chapter 6

Proof of the Second Descent Theorem

6.1 Outline of the Proof

In this chapter we establish our explicit recipe for 5-descent on the elliptic curves E_τ over $\mathbf{Q}$ whose 5-torsion splits as $\boldsymbol{\mu}_5 \oplus \mathbf{Z}/5\mathbf{Z}$. We begin by showing that Theorem 2, as stated in §2.4, is a consequence of the following more detailed proposition. We write $\phi : E_\tau \to E'_\tau$ and $\widehat{\psi} : E_\tau \to E''_\tau$ for the isogenies with kernel $\boldsymbol{\mu}_5$ and $\mathbf{Z}/5\mathbf{Z}$ respectively.

Proposition 6.1 *Let $E = E_\tau$ for $\tau \in \mathbf{Q}$ with $\tau \neq 0$.*
(i) There are natural inclusions

$$\begin{array}{ccccc} S^{(\widehat{\psi})}(E/\mathbf{Q}) & \subset & \phi S^{(5)}(E/\mathbf{Q}) & \subset & S^{(\widehat{\phi})}(E'/\mathbf{Q}) \\ S^{(\phi)}(E/\mathbf{Q}) & \subset & \widehat{\psi} S^{(5)}(E/\mathbf{Q}) & \subset & S^{(\psi)}(E''/\mathbf{Q}). \end{array}$$

(ii) Let $\Xi_\phi = \begin{pmatrix} [\mathcal{P},\mathcal{Q}] & [\mathcal{P},\mathcal{R}] \end{pmatrix}$ and $\Xi_\psi = \begin{pmatrix} [\mathcal{P},\mathcal{R}] \\ [\mathcal{Q},\mathcal{R}] \end{pmatrix}$. Then

$$\begin{array}{lcllcl} S^{(\widehat{\psi})}(E/\mathbf{Q}) & \cong & \ker_R(\Xi_\psi), & S^{(\widehat{\phi})}(E'/\mathbf{Q}) & \cong & \ker_R(\Xi_\phi) \\ S^{(\phi)}(E/\mathbf{Q}) & \cong & \ker_L(\Xi_\phi), & S^{(\psi)}(E''/\mathbf{Q}) & \cong & \ker_L(\Xi_\psi). \end{array}$$

(iii) The image of the map $\phi : S^{(5)}(E/\mathbf{Q}) \to S^{(\widehat{\phi})}(E'/\mathbf{Q})$ is the kernel of Ψ_R restricted to $S^{(\widehat{\phi})}(E'/\mathbf{Q})$ where

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

(iv) The image of the map $\widehat{\psi} : S^{(5)}(E/\mathbf{Q}) \to S^{(\psi)}(E''/\mathbf{Q})$ *is the kernel of* Ψ_L *restricted to* $S^{(\psi)}(E''/\mathbf{Q})$ *where*

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

We make a few remarks about the proof of Proposition 6.1.
(i) This is a consequence of the assumption that E has split torsion. It is easily proved by examining the first diagram of §6.3.
(ii) This is merely a restatement of Theorem 1 for the values $\lambda = \tau^5$ and $\lambda = \tau f(\tau)/g(\tau)$. See §2.3 for details.
(iii), (iv) We must compute the Cassels-Tate pairing on the Selmer groups $S^{(\widehat{\phi})}(E'/\mathbf{Q})$ and $S^{(\psi)}(E''/\mathbf{Q})$. This is the main content of the above proposition, and will occupy us for most of this chapter.

The work of Beaver [Be] gives a proof of Proposition 6.1(iv) in the case $\mathrm{ord}_5(\tau) > 0$. We shall essentially follow her proof, making the modifications necessary to remove the condition $\mathrm{ord}_5(\tau) > 0$.

We now explain how Theorem 2 follows from Proposition 6.1. For this we need the following linear algebra lemma.

Lemma 6.2 *Let* V *be a finite dimensional vector space over a field* F. *Let* $V = U \oplus W$ *and write* $pr : V \to W$ *for the projection map. Let* $\Psi : V \times V \to F$ *be either a symmetric form or a skew-symmetric form, and suppose that* Ψ *is isotropic on* U, i.e. $\Psi(u, u') = 0$ *for all* $u, u' \in U$. *Then*

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

where $W_1 = W \cap U^\perp$.

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

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

Proof of Theorem 2. Taking Galois cohomology of

$$0 \to E[\phi] \to E[5] \xrightarrow{\phi} E'[\widehat{\phi}] \to 0$$

and restricting to Selmer groups we obtain an exact sequence

$$0 \to S^{(\phi)}(E/\mathbf{Q}) \to S^{(5)}(E/\mathbf{Q}) \xrightarrow{\phi} S^{(\widehat{\phi})}(E'/\mathbf{Q}). \tag{65}$$

We apply Lemma 6.2 with $V = [\mathcal{P} \cup \mathcal{Q} \cup \mathcal{R}]$, $U = [\mathcal{P}]$, $W = [\mathcal{Q} \cup \mathcal{R}]$ and Ψ the pairing of Theorem 2. Proposition 6.1 allows us to identify (65) with the exact sequence

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

Indeed, Proposition 6.1(ii) gives $S^{(\phi)}(E/\mathbf{Q}) = U \cap V^{\perp}$ and $S^{(\widehat{\phi})}(E'/\mathbf{Q}) = W_1$. Then by Proposition 6.1(iii) and Lemma 6.2 we have

$$\phi S^{(5)}(E/\mathbf{Q}) = \ker(\,\Psi \mid W_1 \times W_1) = W_1 \cap W_1^{\perp} = pr(V^{\perp}).$$

It follows that $S^{(5)}(E/\mathbf{Q}) = V^{\perp}$ as required. □

Remark 6.3 Theorem 2 may also be deduced from the exact sequence

$$0 \to S^{(\widehat{\psi})}(E/\mathbf{Q}) \to S^{(5)}(E/\mathbf{Q}) \xrightarrow{\widehat{\psi}} S^{(\psi)}(E''/\mathbf{Q}) \tag{66}$$

using Proposition 6.1(iv). In this case we apply Lemma 6.2 with $U = [\mathcal{R}]$ and $W = [\mathcal{P} \cup \mathcal{Q}]$.

6.2 Definition of the Cassels-Tate Pairing

We briefly recall the definition of the Cassels-Tate pairing. The following treatment is taken from McCallum [Mc]. See also [Mi].

Let K be a number field and let $\phi : C \to D$ be an n-isogeny of elliptic curves over K. For any element $(*)$ we write $(*)_v$ for the corresponding local element. We consider the following commutative diagram, both in its own right and with K replaced by K_v for each place v.

$$\begin{array}{ccccc}
C(K) & \xrightarrow{\phi} & D(K) & \xrightarrow{\delta_\phi} & H^1(K, C[\phi]) \\
\| & & \downarrow{\scriptstyle \widehat{\phi}} & & \downarrow{\scriptstyle \iota} \\
C(K) & \xrightarrow{n} & C(K) & \xrightarrow{\delta_n} & H^1(K, C[n]) \\
\downarrow{\scriptstyle \phi} & & \| & & \downarrow{\scriptstyle \phi} \\
D(K) & \xrightarrow{\widehat{\phi}} & C(K) & \xrightarrow{\delta_{\widehat{\phi}}} & H^1(K, D[\widehat{\phi}])
\end{array}$$

To define the Cassels-Tate pairing $S^{(\widehat{\phi})}(D/K) \times S^{(\widehat{\phi})}(D/K) \to \mathbf{Z}/n\mathbf{Z}$ we take a, $b \in S^{(\widehat{\phi})}(D/K) \subset H^1(K, D[\widehat{\phi}])$ and suppose given $a_1 \in H^1(K, C[n])$ lifting a. At each place v we choose $a_{v,1} \in \operatorname{im}\delta_n$ such that $\phi(a_{v,1}) = a_v$. Then $\phi(a_{v,1} - a_{1,v}) = 0$ and so there exists $c_v \in H^1(K_v, C[\phi])$ with $a_{v,1} - a_{1,v} = \iota(c_v)$. We now define

$$\langle a, b\rangle = \textstyle\sum_v (c_v, b_v)_v$$

where $(\cdot,\cdot)_v$ is the Tate pairing (22). It is easy to check that the definition is independent of all choices, and that $\langle a, b\rangle = 0$ whenever a is in the image of $\phi : S^{(n)}(C/K) \to S^{(\widehat{\phi})}(D/K)$. It is well known the Cassels-Tate pairing is alternating, and its kernel is precisely the image just described. This leads to the definition of an alternating pairing on Ш.

We should point out that from the computational point of view, the difficult part in the above construction is the lifting of a to a_1. In general the existence of such a lifting depends on the local triviality of the torsor described by a.

6.3 Split Torsion and Local Pairings

Let E/K to be an elliptic curve whose n-torsion splits as $E[n] = \langle P\rangle \oplus \langle Q\rangle$. Let $\phi : E \to E'$ and $\widehat{\psi} : E \to E''$ be the isogenies defined over K whose kernels are generated by P and Q respectively. We make the identifications

$$E[\phi] = \langle P\rangle = E[n]/\langle Q\rangle = E''[\psi]$$

$$E[\widehat{\psi}] = \langle Q\rangle = E[n]/\langle P\rangle = E'[\widehat{\phi}]$$

and so obtain a commutative diagram with exact diagonals

$$\begin{array}{ccccc} H^1(K, E[\phi]) & & = & & H^1(K, E''[\psi]) \\ & {\scriptstyle \iota_P}\searrow & & \nearrow{\scriptstyle \widehat{\psi}} & \\ & & H^1(K, E[n]) & & \\ & {\scriptstyle \iota_Q}\nearrow & & \searrow{\scriptstyle \phi} & \\ H^1(K, E[\widehat{\psi}]) & & = & & H^1(K, E'[\widehat{\phi}]). \end{array}$$

The key point is that ι_Q is a splitting of the map ϕ, and so may be used to help compute the Cassels-Tate pairing on $S^{(\widehat{\phi})}(E'/K)$. Indeed, as McCallum [Mc] explains we may write the pairing as a sum of local pairings

$$\langle a, b\rangle = \textstyle\sum_v \langle a_v, b_v\rangle_v. \tag{67}$$

Here we set $a_{1,v} = \iota_Q(a_v)$ and choose $a_{v,1} \in \operatorname{im}\delta_n$ with $\phi(a_{v,1}) = a_v$. Then the local pairing is given by $\langle a_v, b_v\rangle_v = (c_v, b_v)_v$ where $\iota_P(c_v) = a_{v,1} - a_{1,v}$ and $(\cdot,\cdot)_v$ is the Tate pairing.

We shall give a criterion for the local pairing $\langle\cdot,\cdot\rangle_v$ to be trivial. At each place v we have commutative diagrams

$$\begin{array}{ccccc} E(K_v) & \xrightarrow{\phi} & E'(K_v) & \xrightarrow{\delta_\phi} & H^1(K_v, E[\phi]) \\ \downarrow\widehat{\psi} & & \downarrow\widehat{\phi} & & || \\ E''(K_v) & \xrightarrow{\psi} & E(K_v) & \xrightarrow{\delta_\psi} & H^1(K_v, E''[\psi]) \end{array}$$

and

$$\begin{array}{ccccc} E(K_v) & \xrightarrow{\widehat{\psi}} & E''(K_v) & \xrightarrow{\delta_{\widehat{\psi}}} & H^1(K_v, E[\widehat{\psi}]) \\ \downarrow\phi & & \downarrow\psi & & || \\ E'(K_v) & \xrightarrow{\widehat{\phi}} & E(K_v) & \xrightarrow{\delta_{\widehat{\phi}}} & H^1(K_v, E'[\widehat{\phi}]) \end{array}$$

It is clear from the diagrams that $\operatorname{im}\delta_\phi \subset \operatorname{im}\delta_\psi$ and $\operatorname{im}\delta_{\widehat{\psi}} \subset \operatorname{im}\delta_{\widehat{\phi}}$. Tate local duality, specifically Proposition 1.17, tells us

$$\operatorname{im}\delta_\phi = \operatorname{im}\delta_\psi \iff \operatorname{im}\delta_{\widehat{\psi}} = \operatorname{im}\delta_{\widehat{\phi}}.$$

We call v a *switching place* if these equalities do *not* hold, and write $\mathcal{S}$ for the set of switching places. It is easy to see that $\mathcal{S}$ is a subset of the usual set of bad places, *i.e.* the infinite places, the primes of bad reduction for E and the primes dividing n. Indeed at the good primes it is well known [Si1] that the image of each map δ consists precisely of the unramified cocycles.

Lemma 6.4 *If $v \notin \mathcal{S}$ then the local pairing $\langle\cdot,\cdot\rangle_v$ vanishes.*

Proof. With the above notation describing the local pairing we have

$$\begin{array}{rrcll} & \iota_P(c_v) & = & a_{v,1} - a_{1,v} & \\ \Longrightarrow & c_v & = & \widehat{\psi}(a_{v,1}) & \text{since } \widehat{\psi}\,\iota_P = 1 \text{ and } \widehat{\psi}\,\iota_Q = 0 \\ \Longrightarrow & c_v & \in & \operatorname{im}\delta_\psi & \text{since } \delta_\psi = \widehat{\psi}\,\delta_n. \end{array}$$

We are assuming $\operatorname{im}\delta_\phi = \operatorname{im}\delta_\psi$. So we have $c_v \in \operatorname{im}\delta_\phi$ and $b_v \in \operatorname{im}\delta_{\widehat{\phi}}$. Tate local duality now gives $\langle a_v, b_v\rangle_v = (c_v, b_v)_v = 0$. □

We explain the method due to Beaver [Be] that allows us to compute the local pairing in many cases. From now on we assume n is prime. For the next three lemmas we fix a place v of K and suppose P, $Q \in E(K_v)$. Then $E[n] \subset E(K_v)$ and $H^1(K_v, E[n]) = \operatorname{Hom}(G_v, E[n])$.

Definition 6.5 *For $T \in E[n]$ a point of order n we write*

$$\delta_T : E(K_v) \to \mathrm{Hom}(G_v, E[n]/\langle T\rangle)$$

for the connecting homomorphism corresponding to the dual of the isogeny $E \to E/\langle T\rangle$. Equivalently δ_T is the composite

$$E(K_v) \xrightarrow{\delta_n} \mathrm{Hom}(G_v, E[n]) \longrightarrow \mathrm{Hom}(G_v, E[n]/\langle T\rangle).$$

Lemma 6.6 *There is at most one subgroup $\langle T\rangle \subset E[n]$ with $\delta_T = 0$.*

Proof. If $\delta_T = 0$ then $\mathrm{im}\,\delta_n \subset \mathrm{Hom}(G_v, \langle T\rangle)$. But $\mathrm{im}\,\delta_n$ is maximal isotropic in $\mathrm{Hom}(G_v, E[n])$, so by counting we have $\mathrm{im}\,\delta_n = \mathrm{Hom}(G_v, \langle T\rangle)$ and the subgroup $\langle T\rangle \subset E[n]$ is uniquely determined. □

Remark 6.7 We find there are examples where there is no subgroup $\langle T\rangle \subset E[n]$ with $\delta_T = 0$. However, for E with split multiplicative reduction, Beaver [Be] uses the Tate parametrisation to show that such a subgroup must exist.

Lemma 6.8 *Let $v \in \mathcal{S}$ be a switching place. Suppose $P, Q \in E(K_v)$ and that there exists $T \in E[n]$ with $\delta_T = 0$. Then the local pairing $\langle\cdot,\cdot\rangle_v$ may be computed via the formula*

$$\langle a_v, b_v\rangle_v = (-\rho(a_v), b_v)_v$$

where $\rho : \mathrm{Hom}(G_v, \langle Q\rangle) \to \mathrm{Hom}(G_v, \langle P\rangle)$ is projection along $\langle T\rangle$.

Proof. Since $v \in \mathcal{S}$ we know $\delta_P = \delta_{\widehat{\phi}} \neq 0$ and $\delta_Q = \delta_\psi \neq 0$, so the map ρ is well defined. Now $\langle a_v, b_v\rangle_v = (c_v, b_v)_v$ with $a_v \in \mathrm{Hom}(G_v, \langle Q\rangle)$ and $c_v \in \mathrm{Hom}(G_v, \langle P\rangle)$. But a_v and $-c_v$ differ by $a_{v,1} \in \mathrm{im}\,\delta_n = \mathrm{Hom}(G_v, \langle T\rangle)$ so the stated result is immediate. □

We write

$$\begin{aligned} \pi_P : \mathrm{Hom}(G_v, \langle Q\rangle) &\xrightarrow{\sim} K_v^\times/(K_v^\times)^n \\ \pi_Q : \mathrm{Hom}(G_v, \langle P\rangle) &\xrightarrow{\sim} K_v^\times/(K_v^\times)^n \end{aligned} \tag{68}$$

for the maps induced by $e_n(P,\cdot)$ and $e_n(Q,\cdot)$. The Tate pairing and norm residue symbol are related as follows.

Lemma 6.9 *For $x \in \mathrm{Hom}(G_v, \langle Q \rangle)$ and $y \in \mathrm{Hom}(G_v, \langle P \rangle)$ we have*

$$e_n(P,Q)^{(x,y)_v} = (\pi_P(x), \pi_Q(y))_v$$

where $(\cdot,\cdot)_v$ denotes the Tate pairing, respectively the norm residue symbol.

A convenient way to write this result is $(x,y)_v = \mathrm{Ind}_\zeta(\pi_P(x), \pi_Q(y))_v$ where $\zeta = e_n(P,Q)$ and $\mathrm{Ind}_\zeta : \boldsymbol{\mu}_n \xrightarrow{\sim} \mathbf{Z}/n\mathbf{Z}\,;\, \zeta \mapsto 1$. We are now ready to give Beaver's description of the Cassels-Tate pairing.

Proposition 6.10 *Let n be a prime and let E/K be an elliptic curve whose n-torsion splits as $E[n] = \langle P \rangle \oplus \langle Q \rangle$. Suppose that every switching place $v \in \mathcal{S}$ satisfies the hypotheses of Lemma 6.8, say with $T = i_v P + Q$. Let $\zeta = e_n(P,Q)$ and write $(\cdot,\cdot)_v$ for the norm residue symbol.*
(i) The Cassels-Tate pairing on $S^{(\widehat{\phi})}(E'/K)$ is given by

$$\langle a, b \rangle \;=\; \textstyle\sum_{v \in \mathcal{S}} \mathrm{Ind}_\zeta(\pi_P(a_v), \pi_P(b_v))_v^{i_v}.$$

(ii) The Cassels-Tate pairing on $S^{(\psi)}(E''/K)$ is given by

$$\langle a, b \rangle \;=\; \textstyle\sum_{v \in \mathcal{S}} \mathrm{Ind}_\zeta(\pi_Q(a_v), \pi_Q(b_v))_v^{-1/i_v}.$$

Proof. It suffices to prove (i), since (ii) follows by symmetry $P \leftrightarrow Q$. For $a, b \in S^{(\widehat{\phi})}(E'/K)$ we have

$$\begin{array}{rcll} \langle a, b \rangle & = & \sum_{v \in \mathcal{S}} \langle a_v, b_v \rangle_v & \text{by Lemma 6.4} \\ & = & \sum_{v \in \mathcal{S}} (-\rho(a_v), b_v)_v & \text{by Lemma 6.8} \\ & = & \sum_{v \in \mathcal{S}} \mathrm{Ind}_\zeta(\pi_Q(\rho(a_v)), \pi_P(b_v))_v & \text{by Lemma 6.9} \\ & = & \sum_{v \in \mathcal{S}} \mathrm{Ind}_\zeta(\pi_P(a_v), \pi_P(b_v))_v^{i_v} & \end{array}$$

where the last equality follows from $\rho(Q) = -i_v P$. □

6.4 Computation of the Cassels-Tate Pairing

We apply Proposition 6.10 in the case $K = \mathbf{Q}$ and $n = 5$. Since n is odd we may ignore the infinite places. We have $E[5] = \langle P \rangle \oplus \langle Q \rangle$ and further assume $\langle P \rangle \cong \boldsymbol{\mu}_5$ and $\langle Q \rangle \cong \mathbf{Z}/5\mathbf{Z}$ as Galois modules. Then $E \cong E_\tau$ for some $\tau \in \mathbf{Q}$ with $\tau \neq 0$ and we recall from §2.3 and §6.1 our short dictionary

$$\begin{array}{lcl} \phi : E \to E' & \leftrightarrow & \phi : C_{\tau^5} \to D_{\tau^5} \\ \psi : E'' \to E & \leftrightarrow & \phi : C_{\tau f(\tau)/g(\tau)} \to D_{\tau f(\tau)/g(\tau)}. \end{array}$$

The images of the connecting maps δ_ϕ and δ_ψ are given by Proposition 3.19 on taking $\lambda = \tau^5$ and $\lambda = \tau f(\tau)/g(\tau)$. By Lemma 2.12 the set of switching primes $\mathcal{S}$ is precisely the set of primes $\mathcal{Q}$. In particular 5 is never a switching prime. Our next task is to show that every prime $p \in \mathcal{Q}$ satisfies the hypotheses of Lemma 6.8 and to compute the switching exponent i_p.

Let p be a prime with $p \equiv 1 \pmod 5$ and fix an embedding $\mathbf{Q}(\boldsymbol{\mu}_5) \hookrightarrow \mathbf{Q}_p$. As explained in §6.3 we seek $\langle T \rangle \subset E[n]$ with $\delta_T = 0$. We find

$$\begin{aligned} \langle T \rangle = \langle P \rangle \quad &\Longleftrightarrow \quad \delta_{\widehat{\phi}} = 0 \\ &\Longleftrightarrow \quad p \in \mathcal{P} \\ &\Longleftrightarrow \quad \tau \equiv 0 \text{ or } \infty \pmod p \end{aligned} \tag{69}$$

and

$$\begin{aligned} \langle T \rangle = \langle Q \rangle \quad &\Longleftrightarrow \quad \delta_{\psi} = 0 \\ &\Longleftrightarrow \quad p \in \mathcal{R} \\ &\Longleftrightarrow \quad \tau \equiv \phi \text{ or } \overline{\phi} \pmod p. \end{aligned} \tag{70}$$

In §4.2 we saw that the action (16) of $\mathrm{PSL}_2(\mathbf{Z}/5\mathbf{Z})$ on $X(5)$ is generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : \tau \mapsto \zeta^{-1}\tau$ and $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} : \tau \mapsto (\phi\tau+1)/(\tau-\phi)$ where $\zeta = e_5(P,Q)$. From either (69) or (70) we deduce

$$\langle T \rangle = \langle i_p P + Q \rangle \iff \tau \equiv \zeta^{i_p}\phi \text{ or } \zeta^{i_p}\overline{\phi} \pmod p.$$

This description makes it easy to compute the switching exponent i_p. Since we fixed an embedding $\mathbf{Q}(\boldsymbol{\mu}_5) \hookrightarrow \mathbf{Q}_p$, we have really computed $i_\mathfrak{p}$ where $\mathfrak{p}|p$ is the corresponding prime of $\mathbf{Q}(\boldsymbol{\mu}_5)$. Writing $\psi : \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_5)/\mathbf{Q}) \xrightarrow{\sim} (\mathbf{Z}/5\mathbf{Z})^\times$ for the cyclotomic character, we find

$$i_{\sigma\mathfrak{p}} = \psi(\sigma) i_\mathfrak{p} \qquad \text{for all } \sigma \in \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_5)/\mathbf{Q}).$$

Proof of Proposition 6.1(iii), (iv). Let $K = \mathbf{Q}(\boldsymbol{\mu}_5)$ and recall our notation (58) for the restriction maps. For each rational prime p we choose $\mathfrak{p}$ a prime of K above p. It is to be understood that all our formulae are independent of these choices. The Tate pairing

$$(\cdot,\cdot)_p : H^1(\mathbf{Q}_p, \boldsymbol{\mu}_5) \times H^1(\mathbf{Q}_p, \mathbf{Z}/5\mathbf{Z}) \to \mathbf{Z}/5\mathbf{Z}$$

and the Hilbert norm residue symbol

$$(\cdot,\cdot)_\mathfrak{p} : K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^5 \times K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^5 \to \boldsymbol{\mu}_5$$

are related by

$$(a,b)_p = [K_{\mathfrak{p}} : \mathbf{Q}_p]^{-1} \operatorname{Ind}_\zeta(a, \pi b)_{\mathfrak{p}}. \tag{71}$$

We recall from §3.4 our notation $F^{(p)}$ for the degree n cyclic extension of $\mathbf{Q}$ unramified outside p. For $p \in \mathcal{Q} \cup \mathcal{R}$ we define

$$\chi_p : (\mathbf{Z}/p\mathbf{Z})^\times \to \mathbf{Z}/5\mathbf{Z}\,;\ a \mapsto (a, \xi^{(p)})_p$$

where $\xi^{(p)} \in H^1(\mathbf{Q}, \mathbf{Z}/5\mathbf{Z}) = \operatorname{Hom}(G_{\mathbf{Q}}, \mathbf{Z}/5\mathbf{Z})$ is some choice of generator for $\operatorname{Gal}(F^{(p)}/\mathbf{Q})$. For $p \in \mathcal{Q}$ we make our choice such that

$$\operatorname{ord}_{\mathfrak{p}}(\pi\xi^{(p)}) = -1/i_{\mathfrak{p}}. \tag{72}$$

This is possible since $\operatorname{im}\pi \subset (K^\times/(K^\times)^5)^\psi$ and $\pi\xi^{(p)}$ is a product of primes above p. Since $\xi^{(p)} \notin H^1_{\mathrm{nr}}(\mathbf{Q}_p, \boldsymbol{\mu}_5)$ it is clear that the characters χ_p are non-trivial. For $p \in \mathcal{Q}$ they are given by

$$\chi_p(a) = (a, \xi^{(p)})_p = \operatorname{Ind}_\zeta(a, \pi\xi^{(p)})_{\mathfrak{p}} = \operatorname{Ind}_\zeta(a/\mathfrak{p})^{-1/i_{\mathfrak{p}}}. \tag{73}$$

Euler's criterion asserts $(a/\mathfrak{p}) \equiv a^{(p-1)/5} \pmod{\mathfrak{p}}$. Thus the characters χ_p for $p \in \mathcal{Q}$ are compatible in the sense of Remark 2.16.

By the work of §3.4 the Selmer groups attached to ϕ, ψ and their duals correspond to the left and right kernels of the pairings

$$\begin{aligned} \Xi_\phi &: [\mathcal{P}] \times \langle \mathcal{Q} \cup \mathcal{R} \rangle \to \mathbf{Z}/5\mathbf{Z}\,; \quad (a,b) \mapsto \textstyle\sum_{p \in \mathcal{Q}\cup\mathcal{R}} (a,b)_p \\ \Xi_\psi &: [\mathcal{P} \cup \mathcal{Q}] \times \langle \mathcal{R} \rangle \to \mathbf{Z}/5\mathbf{Z}\,; \quad (a,b) \mapsto \textstyle\sum_{p \in \mathcal{R}} (a,b)_p. \end{aligned}$$

Proposition 6.10 describes the Cassels-Tate pairing on the Selmer groups $S^{(\widehat{\phi})}(E'/\mathbf{Q}) \cong \ker_R(\Xi_\phi)$ and $S^{(\psi)}(E''/\mathbf{Q}) \cong \ker_L(\Xi_\psi)$ as the restrictions of the pairings

$$\begin{aligned} \Psi_R &: \langle \mathcal{Q} \cup \mathcal{R} \rangle \times \langle \mathcal{Q} \cup \mathcal{R} \rangle \to \mathbf{Z}/5\mathbf{Z}\,; \quad (b_1,b_2) \mapsto \textstyle\sum_{p \in \mathcal{Q}} \operatorname{Ind}_\zeta(\pi b_1, \pi b_2)_{\mathfrak{p}}^{i_{\mathfrak{p}}} \\ \Psi_L &: [\mathcal{P} \cup \mathcal{Q}] \times [\mathcal{P} \cup \mathcal{Q}] \to \mathbf{Z}/5\mathbf{Z}\,; \quad (a_1,a_2) \mapsto \textstyle\sum_{p \in \mathcal{Q}} \operatorname{Ind}_\zeta(a_1,a_2)_{\mathfrak{p}}^{-1/i_{\mathfrak{p}}}. \end{aligned}$$

To complete our proof it remains to identify $[\mathcal{Q} \cup \mathcal{R}]$ with $\langle \mathcal{Q} \cup \mathcal{R} \rangle$ via $p \mapsto \xi^{(p)}$ and to check that the above pairings are represented by the matrices appearing in the statement of the proposition. This is immediate for the pairings Ξ_ϕ and Ξ_ψ.

For Ψ_L we take $p \in \mathcal{P}$ and $q \in \mathcal{Q}$ and compute

$$\begin{aligned} \Psi_L(p,q) &= \mathrm{Ind}_\zeta(p,q)_{\mathfrak{q}}^{-1/i_{\mathfrak{q}}} && \text{by definition} \\ &= \mathrm{Ind}_\zeta(p,\pi\xi^{(q)})_{\mathfrak{q}} && \text{by (72)} \\ &= \chi_q(p) && \text{by (73).} \end{aligned}$$

For Ψ_R we take $q \in \mathcal{Q}$ and $r \in \mathcal{R}$ and compute

$$\begin{aligned} \Psi_R(\xi^{(q)},\xi^{(r)}) &= \mathrm{Ind}_\zeta(\pi\xi^{(q)},\pi\xi^{(r)})_{\mathfrak{q}}^{i_{\mathfrak{q}}} && \text{by definition} \\ &= \mathrm{Ind}_\zeta(\pi\xi^{(r)},q)_{\mathfrak{q}} && \text{by (72)} \\ &= [K_{\mathfrak{q}} : \mathbf{Q}_q]^{-1}\,\mathrm{Ind}_\zeta(\pi\xi^{(r)},q)_{\mathfrak{q}} && \text{since } q \equiv 1 \pmod 5 \\ &= [K_{\mathfrak{r}} : \mathbf{Q}_r]^{-1}\,\mathrm{Ind}_\zeta(q,\pi\xi^{(r)})_{\mathfrak{r}} && \text{by the product formula} \\ &= \chi_r(q) && \text{by (71).} \end{aligned}$$

Similar calculations for $q, q' \in \mathcal{Q}$ with $q \neq q'$ give

$$\Psi_L(q,q') = \Psi_R(\xi^{(q)},\xi^{(q')}) = \chi_{q'}(q) - \chi_q(q').$$

This completes the proof of Proposition 6.1 and so of Theorem 2. □

Chapter 7

Application to the Curves of Conductor 11

The elliptic curves over $\mathbf{Q}$ with conductor 11 are

11A1	$y^2 + y = x^3 - x^2 - 10x - 20$	A_0	$E_1 = C_1 = D_{11}$
11A2	$y^2 + y = x^3 - x^2 - 7820x - 263580$	A_2	$E_1'' = C_{11}$
11A3	$y^2 + y = x^3 - x^2$	A_1	$E_1' = D_1$.

Here the labels 11A1-3 are the Cremona labels [Cr] and A_0, A_1, A_2 are the labels used in [CS] chosen such that $A_i = X_i(11)$ for $i = 0, 1$. We sometimes write A to denote any one of these curves. For these primeval elliptic curves we ask ourselves the following question.

> How does the Mordell-Weil rank of these curves behave as we pass up the tower of fields given by adjoining the 5-power division points?

We write $K = \mathbf{Q}(\boldsymbol{\mu}_5)$ and $L = \mathbf{Q}(A_1[5])$. In Example 5.6 we used Theorem 3 to show $\operatorname{rank} A(K) = 0$. In this chapter we show $\operatorname{rank} A(L) = 0$.

7.1 The Field $L = \mathbf{Q}(A_1[5])$

let ζ be a primitive 5th root of unity, and let $\phi = 1 + \zeta + \zeta^4$ be the golden ratio with conjugate $\overline{\phi}$. We recall that there is an involution

$$\eta : X_1(5) \to X_1(5)\,; \qquad \lambda \mapsto (\phi^5\lambda + 1)/(\lambda - \phi^5)$$

swapping over the rational and irrational cusps. Since $A_1 \cong C_{\eta(1)}$ over K, it follows by Remark 1.8 that $\eta(1)$ is a Kummer generator for L/K. In other words $L = K(\zeta, \alpha)$ with $\alpha^5 = \eta(1) = (1+\phi^5)/(1-\phi^5)$.

Manifestly $L/\mathbf{Q}$ in unramified outside 5 and 11. We describe the situation a little more precisely. Let $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ be the primes of K above 11 with $\mathfrak{p}_i = (\pi_i)$ and $\pi_i = 2 + \zeta^i$. Since $(\eta(1)) = \mathfrak{p}_1^{-1}\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4^{-1}$ the primes above 11 ramify in L/K, *i.e.*

$$(11) = \mathfrak{P}_1^5\mathfrak{P}_2^5\mathfrak{P}_3^5\mathfrak{P}_4^5$$

with $\mathfrak{P}_i | \mathfrak{p}_i$. Let $\mathfrak{l}$ be the prime of K above 5. Since $\eta(1) = \overline{\phi^5}(1+z)$ with $\mathrm{ord}_{\mathfrak{l}}(z) = \mathrm{ord}_{\mathfrak{l}}(\phi^5 - \overline{\phi^5}) = 6$ we may define

$$\alpha_0 := \overline{\phi}(1 + \tbinom{1/5}{1} z + \tbinom{1/5}{2} z^2 + \dots) \in K_{\mathfrak{l}}$$

such that $\alpha_0^5 = \eta(1)$. Thus $\mathfrak{l}$ splits in L/K, *i.e.*

$$(5) = \mathfrak{L}_0^4\mathfrak{L}_1^4\mathfrak{L}_2^4\mathfrak{L}_3^4\mathfrak{L}_4^4$$

with $\alpha \equiv \zeta^i\overline{\phi} \pmod{\mathfrak{L}_i^2}$.

We compute the units and class group using `pari`. Thus strictly speaking the following lemma has only be checked modulo the Generalised Riemann Hypothesis (GRH).

Lemma 7.1 *Let $L = \mathbf{Q}(\boldsymbol{\mu}_5, \alpha)$ with $\alpha^5 = (1+\phi^5)/(1-\phi^5)$.*
(i) The unit group of L is generated by ζ, ϕ, $(\phi\alpha+1)/(\alpha-\phi)$, $(\alpha+1)/(\alpha-1)$ and their Galois conjugates.
(ii) The class group of L is isomorphic to $\mathbf{Z}/5\mathbf{Z}$ as a $\mathrm{Gal}(L/\mathbf{Q})$-module, and is generated by the primes above 11.

Let us write $u_i = (\phi\zeta^i\alpha + 1)/(\zeta^i\alpha - \phi)$ and $v_i = (\zeta^i\alpha + 1)/(\zeta^i\alpha - 1)$. We check by hand that these are indeed units. The identity of Lemma 2.10 gives

$$u_i f(u_i)/g(u_i) = \eta(\varepsilon(u_i)^5) = \eta(\alpha^5) = 1$$

and so the u_i have minimal polynomial

$$xf(x) - g(x) = x^5 + 2x^4 + 6x^3 - 2x^2 + 4x - 1.$$

But also

$$(v_i+1)^5/(v_i-1)^5 = \alpha^5 = (1+\phi^5)/(1-\phi^5).$$

So the v_i are the roots of

$$\phi^5(x^5 + 10x^3 + 5x) - (5x^4 + 10x^2 + 1) = 0.$$

Lemma 7.1(i) is equivalent to the statement $\phi, u_1, u_2, u_3, u_4, v_1, v_2, v_3, v_4$ is a set of fundamental units. It is an easy exercise to describe the action of $\mathrm{Gal}(L/\mathbf{Q})$ on these units.

Let M be the composite of K and $\mathbf{Q}(\boldsymbol{\mu}_{11}) \cap \mathbf{R}$. Then L/K and M/K are both Kummer extensions of degree 5, ramified only at the primes above 11. It follows LM/L is unramified at all places. By properties of the Hilbert class field, this confirms that 5 divides the class number of L.

For our descent calculations we must consider the spaces

$$\begin{aligned} V_\emptyset &= \{\, \theta \in L^\times/(L^\times)^5 \mid \mathrm{ord}_{\mathfrak{P}}(\theta) \equiv 0 \pmod 5 \text{ for all } \mathfrak{P} \,\} \\ &= \langle \zeta, \phi, u_1, u_2, u_3, u_4, v_1, v_2, v_3, v_4, w \rangle \end{aligned}$$

where $w = 1 + \phi^5 \equiv 1 - \phi^5 \mod (L^\times)^5$ is a contribution from the class group, and

$$\begin{aligned} V_{11} &= \{\, \theta \in L^\times/(L^\times)^5 \mid \mathrm{ord}_{\mathfrak{P}}(\theta) \equiv 0 \pmod 5 \text{ for all } \mathfrak{P} \nmid 11 \,\} \\ &= \langle \zeta, \phi, u_1, u_2, u_3, u_4, v_1, v_2, v_3, v_4, w, \alpha, x, x' \rangle \end{aligned}$$

where

$$x = \tfrac{(\zeta^4+\zeta^2-\zeta)(\alpha^2-\alpha)-1}{(2\phi-1)(\zeta\alpha-1)} \quad \text{and} \quad x' = \tfrac{(\zeta^3+\zeta^4-\zeta^2)(1+\alpha)-\alpha^2}{(2\phi-1)\alpha(\zeta^3\alpha+1)}$$

have been chosen such that $(x) = \mathfrak{P}_1\mathfrak{P}_4^{-1}$ and $(x') = \mathfrak{P}_2\mathfrak{P}_3^{-1}$.

7.2 Estimating $\mathrm{rank}\, A(L)$ via First Descent

We begin with an elementary observation.

Lemma 7.2 $\mathrm{rank}\, A(L)$ *is a multiple of* 4.

Proof. Let ρ be a generator for $\mathrm{Gal}(L/K)$. Then the minimal polynomial for ρ acting on $A(L) \otimes \mathbf{Q}$ divides $x^5 - 1$. But $\mathrm{rank}\, A(K) = 0$ and the cyclotomic polynomial $x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbf{Q}$. So ρ has characteristic polynomial a power of $x^4 + x^3 + x^2 + x + 1$ and the lemma follows. □

Relabelling torsion gives an action of $\mathrm{PSL}_2(\mathbf{Z}/5\mathbf{Z})$ on $X(5) \cong \mathbf{P}^1$. This includes the maps $\tau \mapsto -1/\tau$ and $\tau \mapsto \zeta\tau$. So to describe an orbit it suffices

to list the values $\lambda = \tau^5$ and ignore repeats of the form $\lambda \leftrightarrow -1/\lambda$. We compute the orbits corresponding to A_0 and A_1. They are

$$\{1, -\phi^{15}, \pi_1^5, \pi_2^5, \pi_3^5, \pi_4^5\} \qquad \text{and} \qquad \{\eta(1), u_0^5, u_1^5, u_2^5, u_3^5, u_4^5\}.$$

Thus A_0 is 5-isogenous to A_1, A_2 and the 4 conjugates of $A_3 := D_{\pi_1^5}$. Similarly A_1 is 5-isogenous to A_0 and the 5 conjugates of $A_4 := D_{u_0^5}$. The aim of this section is to prove that the Selmer groups over L, attached to these isogenies and their duals, have the dimensions listed as follows.

$\phi : C_\lambda \to D_\lambda$	λ	$\eta(\lambda)$	$c_i(\lambda)$	$\dim_5 S(\phi)$	$\dim_5 S(\widehat{\phi})$
$A_0 \to A_1$	1	α^5	0	8	2
$A_0 \to A_2$	$-\phi^{15}$	11	6	0	14
$A_0 \to A_3$	π_1^5	$-\zeta^2\phi^3\pi_2\pi_3^{-1}\pi_4$	6	0	12
$A_1 \to A_4$	u_0^5	$u_1u_2^{-1}u_3^{-1}u_4\alpha$	0/6	0	10

For $\lambda \in L$ not a cusp of $X_1(n)$ we write

$$\begin{aligned} \mathcal{A} &= \{\ \mathfrak{P} \text{ prime } \mid \mathrm{ord}_{\mathfrak{P}}(\lambda) \neq 0\ \} \\ \mathcal{B} &= \{\ \mathfrak{P} \text{ prime } \mid \mathrm{ord}_{\mathfrak{P}}(\eta(\lambda)) \neq 0\ \}. \end{aligned}$$

We recall that in §1.1 and §5.1 we defined quantities $c(\lambda)$ and $d(\lambda)$ describing the behaviour of λ at the prime $\mathfrak{l}$. We now define $c_i(\lambda)$ and $d_i(\lambda)$ to be the corresponding quantities with $\mathfrak{l}$ replaced by $\mathfrak{L}_i$.

Proposition 7.3 *The map $\delta : D_\lambda(L_{\mathfrak{P}}) \to L_{\mathfrak{P}}^\times/(L_{\mathfrak{P}}^\times)^5$ has image*

$$\mathrm{im}\,\delta = \begin{cases} L_{\mathfrak{P}}^\times/(L_{\mathfrak{P}}^\times)^n & \text{if } \mathfrak{P} \in \mathcal{A} \\ \mathcal{O}_{\mathfrak{P}}^\times/(\mathcal{O}_{\mathfrak{P}}^\times)^n & \text{if } \mathfrak{P} \notin \mathcal{A} \cup \mathcal{B} \text{ and } \mathfrak{P} \nmid 5 \\ 0 & \text{if } \mathfrak{P} \in \mathcal{B}. \end{cases}$$

If $\mathfrak{p} \notin \mathcal{A} \cup \mathcal{B}$ and $\mathfrak{P} = \mathfrak{L}_i$ then $\mathrm{im}\,\delta = U_{d_i+1}(K_{\mathfrak{l}}^\times)^n/(K_{\mathfrak{l}}^\times)^n$.

Proof. This is immediate from Propositions 3.12 and 5.12. The key point is that $\mathfrak{l}$ splits in L/K, so there is no need to perform further Hensel lemma calculations at the primes above 5. Indeed the local fields $L_{\mathfrak{L}_i}$ are copies of the field $K_{\mathfrak{l}}$ we have already studied. □

Our labelling of the $\mathfrak{L}_i$ is such that

$$\mathrm{ord}_{\mathfrak{L}_i}(\alpha - \phi) = \begin{cases} 1 & i \neq 0 \\ 2 & i = 0. \end{cases}$$

Since $u_0 = \varepsilon(\alpha)$, an analogue of Lemma 1.5(iii) for the involution ε gives

$$\mathrm{ord}_{\mathfrak{L}_i}(u_0 - \phi) = \begin{cases} 1 & i \neq 0 \\ 0 & i = 0. \end{cases}$$

Thus $c_i(u_0^5) = 6$ if $i \neq 0$, and 0 if $i = 0$. As indicated in the above table, this is the only one of our examples where $c_i(\lambda)$ depends on i. We are now ready to show that the Selmer groups listed have the dimensions claimed. We write $S(C_\lambda \to D_\lambda/L)$ instead of $S^{(\phi)}(C_\lambda/L)$.

(i) $S(A_0 \to A_1/L) \cong \{\, \theta \in V_\emptyset \mid \theta \in (L_{\mathfrak{P}_i}^\times)^5 \text{ for } 1 \leq i \leq 4 \,\}$
We choose characters $(\mathcal{O}_L/\mathfrak{P}_i)^\times \to \mathbf{Z}/5\mathbf{Z}$ by composing the maps $x \mapsto x^2$ and $4 \mapsto 1$. Computing these characters on our basis for $V_\emptyset$ we obtain an 11×4 matrix.

	$\mathfrak{P}_1$	$\mathfrak{P}_2$	$\mathfrak{P}_3$	$\mathfrak{P}_4$
ζ	1	3	2	4
ϕ	2	3	3	2
u_1	2	2	2	2
u_2	2	2	2	2
u_3	2	2	2	2
u_4	2	2	2	2
v_1	0	0	0	0
v_2	0	0	0	0
v_3	0	0	0	0
v_4	0	0	0	0
w	1	1	1	1

This matrix has rank 3, so $S(A_0 \to A_1/L) \cong (\mathbf{Z}/5\mathbf{Z})^8$.

(ii) $S(A_1 \to A_0/L) \cong \{\, \theta \in V_{11} \mid \theta^4 \equiv 1 \pmod{\mathfrak{L}_i^5} \text{ for } 0 \le i \le 4 \,\}$
For each basis element of V_{11} we first substitute $\alpha \mapsto \zeta^i \alpha_0$ and then compute the characters $\chi_1, \chi_2, \chi_3, \chi_4$ defined by (50). We obtain a 14×20 matrix.

	$\alpha \mapsto \alpha_0$				$\alpha \mapsto \zeta\alpha_0$				$\alpha \mapsto \zeta^2\alpha_0$				$\alpha \mapsto \zeta^3\alpha_0$				$\alpha \mapsto \zeta^4\alpha_0$			
ζ	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0
ϕ	0	3	3	0	0	3	3	0	0	3	3	0	0	3	3	0	0	3	3	0
u_1	4	4	2	0	2	1	2	2	3	1	0	4	1	4	1	1	0	0	0	3
u_2	2	1	2	2	3	1	0	4	1	4	1	1	0	0	0	3	4	4	2	0
u_3	3	1	0	4	1	4	1	1	0	0	0	3	4	4	2	0	2	1	2	2
u_4	1	4	1	1	0	0	0	3	4	4	2	0	2	1	2	2	3	1	0	4
v_1	3	2	4	2	1	2	3	0	4	2	1	2	2	2	0	1	0	2	2	0
v_2	1	2	3	0	4	2	1	2	2	2	0	1	0	2	2	0	3	2	4	2
v_3	4	2	1	2	2	2	0	1	0	2	2	0	3	2	4	2	1	2	3	0
v_4	2	2	0	1	0	2	2	0	3	2	4	2	1	2	3	0	4	2	1	2
w	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
α	0	4	4	0	1	4	4	0	2	4	4	0	3	4	4	0	4	4	4	0
x	4	4	0	3	0	1	4	0	1	0	2	3	0	4	0	2	4	1	1	0
x'	0	1	4	1	4	0	1	4	0	4	4	0	2	4	3	4	2	1	4	0

This matrix has rank 12 so $S(A_1 \to A_0/L) \cong (\mathbf{Z}/5\mathbf{Z})^2$. It is spanned by $\zeta^4 u_1 u_2^2 u_3^3 u_4^4$ and $\phi u_0^3 u_1 u_4 \alpha$.

(iii) By considering an 11×16 submatrix of the above 14×20 matrix we learn

$$\{\, \theta \in V_\emptyset \mid \theta^4 \equiv 1 \pmod{\mathfrak{L}_i^5} \text{ for } 1 \le i \le 4 \,\}$$

is spanned by $\zeta^4 u_1 u_2^2 u_3^3 u_4^4$. Since this element is not a 5th power in $L_\mathfrak{P}$ for any of the primes $\mathfrak{P}|11$ we deduce that the Selmer groups

$$\begin{aligned}
S(A_0 \to A_2/L) &\cong \left\{ \theta \in V_\emptyset \;\middle|\; \begin{array}{l} \theta \in (L_{\mathfrak{P}_i}^\times)^5 \text{ for } 1 \le i \le 4 \\ \text{and } \theta^4 \equiv 1 \pmod{\mathfrak{L}_i^5} \text{ for } 0 \le i \le 4 \end{array} \right\} \\
S(A_0 \to A_3/L) &\cong \left\{ \theta \in V_\emptyset \;\middle|\; \begin{array}{l} \theta \in (L_{\mathfrak{P}_i}^\times)^5 \text{ for } 2 \le i \le 4 \\ \text{and } \theta^4 \equiv 1 \pmod{\mathfrak{L}_i^5} \text{ for } 0 \le i \le 4 \end{array} \right\} \\
S(A_1 \to A_4/L) &\cong \{\, \theta \in V_\emptyset \mid \theta^4 \equiv 1 \pmod{\mathfrak{L}_i^5} \text{ for } 1 \le i \le 4 \,\}
\end{aligned}$$

are all zero. Likewise we check that the Selmer groups

$$\begin{aligned}
S(A_2 \to A_0/L) &\cong V_{11} \\
S(A_3 \to A_0/L) &\cong \{\, \theta \in V_{11} \mid \theta \in (L_{\mathfrak{P}_1}^\times)^5 \,\} \\
S(A_4 \to A_1/L) &\cong \{\, \theta \in V_{11} \mid \theta^4 \equiv 1 \pmod{\mathfrak{L}_0^5} \,\}
\end{aligned}$$

have the dimensions claimed.

Our best upper bound for rank $A(L)$ obtained by first descent is 8, computed via the 5-isogeny $A_0 \to A_1$ and its dual. In the next section we improve on this by using the Cassels-Tate pairing to help perform a full 5-descent. We are in the habit of calling this a second descent.

7.3 Estimating rank $A(L)$ via Second Descent

To apply the results of Chapter 6 we work with the curves A whose 5-torsion is defined over L, namely A_0 and A_1. Proposition 6.10 gives two methods for computing $S^{(5)}(A/L)$ and we carry out both as a check.

(a) We apply Proposition 6.10 with $\tau = 1$ and aim to compute $S^{(5)}(A_0/L)$. We have isogenies $\phi : A_0 \to A_1$ and $\psi : A_2 \to A_0$ with

$$\operatorname{im}\left(\delta_\phi : A_1(L_\mathfrak{P}) \to L_\mathfrak{P}^\times/(L_\mathfrak{P}^\times)^5\right) = \begin{cases} \mathcal{O}_\mathfrak{P}^\times/(\mathcal{O}_\mathfrak{P}^\times)^5 & \text{if } \mathfrak{P}\nmid 11 \\ 0 & \text{if } \mathfrak{P}\mid 11 \end{cases}$$

$$\operatorname{im}\left(\delta_\psi : A_0(L_\mathfrak{P}) \to L_\mathfrak{P}^\times/(L_\mathfrak{P}^\times)^5\right) = \begin{cases} \mathcal{O}_\mathfrak{P}^\times/(\mathcal{O}_\mathfrak{P}^\times)^5 & \text{if } \mathfrak{P}\nmid 11 \\ L_\mathfrak{P}^\times/(L_\mathfrak{P}^\times)^5 & \text{if } \mathfrak{P}\mid 11. \end{cases}$$

Thus the switching primes are precisely the primes above 11. Since $1 \equiv \zeta^{3i}\phi$ or $\zeta^{3i}\overline{\phi}$ (mod $\mathfrak{p}_i$) the switching exponent at $\mathfrak{P}_i$ is $3i$.

(i) $0 \to S^{(\phi)}(A_0/L) \to S^{(5)}(A_0/L) \xrightarrow{\phi} S^{(\widehat{\phi})}(A_1/L)$
We already know $S^{(\phi)}(A_0/L) \cong (\mathbf{Z}/5\mathbf{Z})^8$ and $S^{(\widehat{\phi})}(A_1/L) \cong (\mathbf{Z}/5\mathbf{Z})^2$. Since $S^{(\widehat{\phi})}(A_1/L)$ contains a contribution from torsion it follows the Cassels-Tate pairing on this Selmer group is trivial. We deduce $S^{(5)}(A_0/L) \cong (\mathbf{Z}/5\mathbf{Z})^{10}$.

(ii) $0 \to S^{(\widehat{\psi})}(A_0/L) \to S^{(5)}(A_0/L) \xrightarrow{\widehat{\psi}} S^{(\psi)}(A_2/L)$
We already know $S^{(\widehat{\psi})}(A_0/L) = 0$ and $S^{(\psi)}(A_2/L) \cong V_{11} \cong (\mathbf{Z}/5\mathbf{Z})^{14}$. The Cassels-Tate pairing on $S^{(\phi)}(A_2/L)$ is given by

$$\langle \theta, \theta' \rangle \;=\; \textstyle\sum_{i=1}^{4} \operatorname{Ind}_\zeta(\theta, \theta')_{\mathfrak{P}_i}^{1/(2i)}$$

where $(\cdot,\cdot)_\mathfrak{P}$ is the norm residue symbol. We deduce that the pairing is represented by a matrix of the form

$$\begin{pmatrix} 0 & M \\ -M^T & * \end{pmatrix}$$

where M is an 11×3 matrix. By relating to the 11×4 matrix recorded above we see M has rank 2 and so the pairing has rank 4. Again we deduce $S^{(5)}(A_0/L) \cong (\mathbf{Z}/5\mathbf{Z})^{10}$.

(b) We apply Proposition 6.10 with $\tau = \alpha$ and aim to compute $S^{(5)}(A_1/L)$. We have isogenies $\phi : A_1 \to A_0$ and $\psi : A_4 \to A_1$ with

$$\mathrm{im}\left(\delta_\phi : A_0(L_\mathfrak{P}) \to L_\mathfrak{P}^\times/(L_\mathfrak{P}^\times)^5\right) = \begin{cases} L_\mathfrak{P}^\times/(L_\mathfrak{P}^\times)^5 & \text{if } \mathfrak{P}|11 \\ \mathcal{O}_\mathfrak{P}^\times/(\mathcal{O}_\mathfrak{P}^\times)^5 & \text{if } \mathfrak{P}\nmid 5, 11 \\ U_5(K_\mathfrak{l}^\times)^5/(K_\mathfrak{l}^\times)^5 & \text{if } \mathfrak{P}|5 \end{cases}$$

$$\mathrm{im}\left(\delta_\psi : A_4(L_\mathfrak{P}) \to L_\mathfrak{P}^\times/(L_\mathfrak{P}^\times)^5\right) = \begin{cases} L_\mathfrak{P}^\times/(L_\mathfrak{P}^\times)^5 & \text{if } \mathfrak{P}|11 \\ \mathcal{O}_\mathfrak{P}^\times/(\mathcal{O}_\mathfrak{P}^\times)^5 & \text{if } \mathfrak{P}\nmid 11,\ \mathfrak{P} \neq \mathfrak{L}_0 \\ U_5(K_\mathfrak{l}^\times)^5/(K_\mathfrak{l}^\times)^5 & \text{if } \mathfrak{P} = \mathfrak{L}_0. \end{cases}$$

Thus the switching primes are $\mathfrak{L}_1, \mathfrak{L}_2, \mathfrak{L}_3, \mathfrak{L}_4$. Unfortunately the hypotheses of Lemma 6.8 are not satisfied. However all our Selmer groups are contained in V_{11} and so consist of elements prime to 5. Working with the norm residue symbol on U_1/U_5 rather than the whole of $K_\mathfrak{l}^\times/(K_\mathfrak{l}^\times)^5$ it is clear that the formulae of Proposition 6.10 are still valid. Our labelling of the primes $\mathfrak{L}_i$ is such that $\mathfrak{L}_i$ has switching exponent i.

(i) $0 \to S^{(\phi)}(A_1/L) \to S^{(5)}(A_1/L) \xrightarrow{\phi} S^{(\widehat{\phi})}(A_0/L)$
We already know $S^{(\phi)}(A_1/L) \cong (\mathbf{Z}/5\mathbf{Z})^2$ and $S^{(\widehat{\phi})}(A_0/L) \cong (\mathbf{Z}/5\mathbf{Z})^8$. The Cassels-Tate pairing on $S^{(\widehat{\phi})}(A_0/L)$ is given by

$$\langle \theta, \theta' \rangle \;=\; \textstyle\sum_{i=1}^4 \mathrm{Ind}_\zeta(\theta, \theta')^i_{\mathfrak{L}_i}.$$

We compute $S^{(\widehat{\phi})}(A_0/L)$ using the 11×4 matrix, and then use the 14×20 matrix, together with the following numerical description [CF, Exercise 2.13] of the norm residue symbol $(\cdot,\cdot)_\mathfrak{l}$ on U_1/U_5, to compute the Cassels-Tate pairing. Here $\gamma = 1 - \zeta$.

	$1-\gamma$	$1-\gamma^2$	$1-\gamma^3$	$1-\gamma^4$
$1-\gamma$	1	ζ^4	ζ	ζ
$1-\gamma^2$	ζ	1	ζ^2	1
$1-\gamma^3$	ζ^4	ζ^3	1	1
$1-\gamma^4$	ζ^4	1	1	1

The Cassels-Tate pairing on $S^{(\widehat{\psi})}(A_0/L)$ is found to have rank 6. The kernel of the pairing is $\phi S^{(5)}(A_1/L) \cong (\mathbf{Z}/5\mathbf{Z})^2$ generated by $u_1u_2^2u_3^3u_4^4$ and $v_1v_2^2v_3^3v_4^4$. We deduce $S^{(5)}(A_1/L) \cong (\mathbf{Z}/5\mathbf{Z})^4$.

(ii) $0 \to S^{(\widehat{\psi})}(A_1/L) \to S^{(5)}(A_1/L) \xrightarrow{\widehat{\psi}} S^{(\psi)}(A_4/L)$
We already know $S^{(\widehat{\psi})}(A_1/L) = 0$ and $S^{(\psi)}(A_4/L) \cong (\mathbf{Z}/5\mathbf{Z})^{10}$. The Cassels-Tate pairing on $S^{(\psi)}(A_4/L)$ is given by

$$\langle \theta, \theta' \rangle \quad = \quad \sum_{i=1}^{4} \mathrm{Ind}_{\zeta} (\theta, \theta')_{\mathfrak{L}_i}^{-1/i}$$

where $(\cdot,\cdot)_{\mathfrak{P}}$ is the norm residue symbol. We compute $S^{(\psi)}(A_4/L)$ using the first 4 columns of the 14×20 matrix, and then compute the Cassels-Tate pairing using the remaining 16 columns. The kernel of the pairing is $\widehat{\psi} S^{(5)}(A_1/L) \cong (\mathbf{Z}/5\mathbf{Z})^4$ generated by $\zeta^4 u_1 u_2^2 u_3^3 u_4^4$, $\phi u_0^3 u_2 u_3$, $\phi^2 \alpha$ and $v_0 v_2^2 v_3^2 w$. Again we deduce $S^{(5)}(A_1/L) \cong (\mathbf{Z}/5\mathbf{Z})^4$.

Thus the estimate for $\mathrm{rank}\, A(L)$ given by second descent is 2. But by Lemma 7.2 the rank is a multiple of 4. We deduce $\mathrm{rank}\, A(L) = 0$ and

$$\begin{aligned} Ш(A_0/L)[5] &\cong (\mathbf{Z}/5\mathbf{Z})^8 \\ Ш(A_1/L)[5] &\cong (\mathbf{Z}/5\mathbf{Z})^2. \end{aligned}$$

It remains an open problem to determine whether the curves A have a single point of infinite order over the tower of number fields defined by their 5-power division points.

Appendix A

Varieties defined by Pfaffians

The following theorem of Buchsbaum and Eisenbud [BE] applies to projectively Gorenstein varieties over any field K. It is well known that elliptic normal curves satisfy this condition.

Theorem A.1 *Let $X \hookrightarrow \mathbf{P}^r$ be projectively Gorenstein of codimension 3 and let $I \lhd R = K[x_0, \ldots, x_r]$ be the corresponding homogeneous ideal. Then the minimal free resolution for R/I is self-dual and takes the form*

$$0 \to R \to R^n \xrightarrow{f} R^n \to R$$

for some $n \geq 3$ odd. The map f determines a skew symmetric form and so may be represented by an $n \times n$ skew symmetric matrix M. The ideal I is minimally generated by the $(n-1) \times (n-1)$ leading Pfaffians of M.

In Chapter 4 we took K an algebraically closed field and $n \geq 5$ odd. We saw that any elliptic curve $E \hookrightarrow \mathbf{P}^{n-1}$ is defined by quadrics, and these quadrics may be written as the 4×4 leading Pfaffians of an $n \times n$ matrix.

In the case $n = 5$, the point $(a : b)$ on $Y(5)$ yields a 5×5 matrix

$$M_5 = \begin{pmatrix} 0 & -ax_1 & -bx_2 & bx_3 & ax_4 \\ ax_1 & 0 & -ax_3 & -bx_4 & bx_0 \\ bx_2 & ax_3 & 0 & -ax_0 & -bx_1 \\ -bx_3 & bx_4 & ax_0 & 0 & -ax_2 \\ -ax_4 & -bx_0 & bx_1 & ax_2 & 0 \end{pmatrix}.$$

It is readily checked that this is the matrix M appearing in Theorem A.1.

In the case $n = 7$, the point $(a : b : c)$ on $Y(7)$ yields a 7×7 matrix

$$M_7 = \begin{pmatrix} 0 & -ax_1 & -bx_2 & cx_3 & -cx_4 & bx_5 & ax_6 \\ ax_1 & 0 & -ax_3 & -bx_4 & cx_5 & -cx_6 & bx_0 \\ bx_2 & ax_3 & 0 & -ax_5 & -bx_6 & cx_0 & -cx_1 \\ -cx_3 & bx_4 & ax_5 & 0 & -ax_0 & -bx_1 & cx_2 \\ cx_4 & -cx_5 & bx_6 & ax_0 & 0 & -ax_2 & -bx_3 \\ -bx_5 & cx_6 & -cx_0 & bx_1 & ax_2 & 0 & -ax_4 \\ -ax_6 & -bx_0 & cx_1 & -cx_2 & bx_3 & ax_4 & 0 \end{pmatrix}.$$

Let $\Sigma \hookrightarrow \mathbf{P}^6$ be defined by the 6×6 leading Pfaffians of M_7. We claim Σ is the secant variety of E. Since the sum of two rank 2 matrices has rank at most 4 it is clear $\operatorname{Sec} E \subset \Sigma$. The next two lemmas show $\operatorname{Sec} E$ and Σ both have dimension 3 and degree 14. Since $\operatorname{Sec} E$ is irreducible and all components of Σ have codimension at most 3, it follows $\operatorname{Sec} E = \Sigma$ as claimed.

Lemma A.2 *Let $n \geq 5$ and let $E \hookrightarrow \mathbf{P}^{n-1}$ be an elliptic normal curve of degree n. Then $\operatorname{Sec} E \hookrightarrow \mathbf{P}^{n-1}$ has dimension 3 and degree $n(n-3)/2$.*

Proof. We check that the degree is as stated. Projecting away from a general $(n-4)$-plane, E is mapped to a plane curve E' with d nodes. Then E' has arithmetic genus $1 + d = (n-1)(n-2)/2$, and $\operatorname{Sec} E$ meets the $(n-4)$-plane in $d = n(n-3)/2$ points. □

Lemma A.3 *Let $X \hookrightarrow \mathbf{P}^r$ be the variety described in Theorem A.1 with M a matrix of linear forms. Then X has degree $n(n^2-1)/24$.*

Proof. We may read off the Hilbert polynomial from the minimal resolution, see *e.g.* [Ha, Lecture 13]. Writing $n = 2k + 1$,

$$\begin{aligned} h_X(t) &= \tbinom{t+2k}{2k} - n\tbinom{t+k}{2k} + n\tbinom{t+k-1}{2k} - \tbinom{t-1}{2k} \\ &= \tfrac{n(n^2-1)}{24(n-4)!}t^{n-4} + \dots \end{aligned}$$

Thus X has degree $n(n^2-1)/24$. □

Remark A.4 It's easy to see that if E is a Néron polygon of degree 7 then Σ consists of 14 3-planes.

We write $\mathrm{Gr}(k,n)$ for the Grassmannian of k-dimensional subspaces of an n-dimensional vector space V. For $k=2$ the Plücker embedding is given by $\mathrm{Gr}(2,n) \hookrightarrow \mathbf{P}(\wedge^2 V)$; $\langle u, v\rangle \mapsto u \wedge v$.

Proposition A.5 *Let $n \geq 5$ odd. Let $E \hookrightarrow \mathbf{P}^{n-1}$ be an elliptic normal curve of degree n. Then E is (set-theoretically) a linear section of the Grassmannian $\mathrm{Gr}(2,n) \hookrightarrow \mathbf{P}^N$ where $N = \binom{n}{2} - 1$.*

Proof. The image of $\mathrm{Gr}(2,n)$ under the Plücker embedding is given by the vanishing of the 4×4 leading Pfaffians of a general $n \times n$ skew symmetric matrix. Thus our claim is that E is defined by the vanishing of the 4×4 leading Pfaffians of an $n \times n$ skew symmetric matrix M with entries linear forms on $\mathbf{P}^{n-1}$. This was proved in Chapter 4. □

In the cases $n = 5, 7$ we may compute the matrix M by computing the minimal resolution for E, respectively $\operatorname{Sec} E$. This approach has the fortunate consequence that Proposition A.5 remains true over a non-algebraically closed field. For example, we may express the equations for $T[\lambda; \tau_0, \ldots, \tau_{n-1}]$ as defined in §3.1 as the 4×4 leading Pfaffians of an $n \times n$ matrix M. To find M we could compute minimal resolutions as suggested above, but there is no need since we already know the answer in the case $\tau_0 = \tau_1 = \ldots = \tau_{n-1}$ and the general case follows by rescaling our co-ordinates as described in Lemma 3.5.

We would like to use the above observations to write down further examples of smooth curves of genus 1 and degree n in $\mathbf{P}^{n-1}$. This is possible in the case $n = 5$ since $\mathrm{Gr}(2,5) \hookrightarrow \mathbf{P}^9$ has dimension 6, degree 5 and canonical divisor $K = -5H$, so a general $\mathbf{P}^4$ slice is indeed a smooth curve of genus 1. In the case $n = 7$, $\mathrm{Gr}(2,7) \hookrightarrow \mathbf{P}^{20}$ has dimension 10, degree 42 and canonical divisor $K = -7H$. A general $\mathbf{P}^6$ does not even meet the Grassmannian. A description of the linear subspaces $\mathbf{P}^6$ that cut out a smooth curve of genus 1 is still sought.

Appendix B

Descent by n-isogeny

Let $n = 5$ or 7. Let M_1 be a Galois module of order n and let $M_2 = M_1^\vee$. Let χ_1 and χ_2 be the corresponding characters $G_{\mathbf{Q}} \to (\mathbf{Z}/n\mathbf{Z})^\times$ with $\chi_1\chi_2$ the cyclotomic character. We consider pairs of n-isogenous elliptic curves $\phi : E \to E'$ over $\mathbf{Q}$ with $E[\phi] \cong M_1$ and $E'[\widehat{\phi}] \cong M_2$. For fixed M_1 and M_2 these pairs are parametrised by some twist of $Y_1(n)$. We believe it should be possible to prove an analogue of Theorem 1 for any pair of Galois modules M_1 and M_2 in place of $\boldsymbol{\mu}_n$ and $\mathbf{Z}/n\mathbf{Z}$. We discuss two approaches.

Let K_1 and K_2 be the fixed fields of $\ker\chi_1$ and $\ker\chi_2$. The restriction map gives an isomorphism $H^1(\mathbf{Q}, M_1) \xrightarrow{\sim} (K_2^\times/(K_2^\times)^n)^{\chi_2}$. We explain a method for writing down equations over $\mathbf{Q}$ for the torsor under E described by $\theta \in (K_2^\times/(K_2^\times)^n)^{\chi_2}$. For simplicity we suppose $n = 5$ and $[K_2 : \mathbf{Q}] = 4$ with $\chi_2 : \sigma \mapsto 2$. Then $E \cong C_\lambda$ for some $\lambda \in K_2$ with $\sigma(\lambda) = -1/\lambda$. We write $\varepsilon = 4 + 2\sigma + \sigma^2 + 3\sigma^3$ for the idempotent in the group ring $\mathbf{Z}/5\mathbf{Z}[\mathrm{Gal}(K_2/\mathbf{Q})]$ with $\sigma\varepsilon = 2\varepsilon$. Then $\theta = \varepsilon\theta = \theta^4\sigma(\theta)^2\sigma^2(\theta)\sigma^3(\theta)^3$. We take V a 5-dimensional vector space over $\mathbf{Q}$ and choose $x_0, \ldots, x_4$ a basis for $V \otimes K_2$ with $\sigma(x_i) = x_{2i}$. Then the curve

$$T[\lambda; \lambda\tfrac{\sigma(\theta)\sigma^3(\theta)}{\theta\sigma^2(\theta)}, \theta, \tfrac{-1}{\sigma(\theta)}, \tfrac{-1}{\sigma^3(\theta)}, \sigma^2(\theta)] \subset \mathbf{P}(V \otimes K_2)$$

is defined over $\mathbf{Q}$. By construction it is the torsor under E described by θ. In the other cases, *i.e.* for $n = 7$ and for other values of $[K_2 : \mathbf{Q}]$ dividing $n - 1$, a similar treatment is easily given.

We give an example with M_1 the 5-twist of $\boldsymbol{\mu}_5$. So here χ_1 is the inverse of the cyclotomic character and $K_2 = \mathbf{Q}(\sqrt{5})$.

Example B.1 *In §5.2 we saw* $Ш(C_{11}^*/\mathbf{Q})[5] \cong (\mathbf{Z}/5\mathbf{Z})^2$. *In particular the*

curve $T = T[11; -11, \phi, 1, 1, \overline{\phi}]$, *where* $\phi = (1+\sqrt{5})/2$ *and* $\overline{\phi} = (1-\sqrt{5})/2$, *is a counter-example to the Hasse Principle. To obtain a model over* $\mathbf{Q}$ *we make the substitution*

$$x_0 = y_0, \quad x_1 = y_1 + \sqrt{5}y_2, \quad x_2 = y_3 + \sqrt{5}y_4,$$
$$x_3 = y_3 - \sqrt{5}y_4, \quad x_4 = y_1 - \sqrt{5}y_2$$

and obtain equations

$$\begin{aligned}
0 &= 11y_0^2 - y_1^2 + 5y_2^2 + y_3^2 - 5y_4^2 \\
0 &= y_1^2 + 10y_1y_2 + 5y_2^2 + 2y_0y_3 - y_1y_3 - 5y_2y_3 - 5y_1y_4 - 5y_2y_4 \\
0 &= y_1^2 + 2y_1y_2 + 5y_2^2 + y_1y_3 + y_2y_3 + 2y_0y_4 + y_1y_4 + 5y_2y_4 \\
0 &= 11y_0y_1 + 55y_0y_2 + 2y_1y_3 + 2y_3^2 - 10y_2y_4 + 10y_4^2 \\
0 &= 11y_0y_1 + 11y_0y_2 - 2y_2y_3 + 2y_1y_4 - 4y_3y_4.
\end{aligned}$$

As our example shows, this approach is rather unsatisfactory in that although we obtain equations over $\mathbf{Q}$, these equations tend to be rather unwieldy. This may be viewed as a consequence of the many arbitrary choices made in the above construction.

A related problem is that of determining the Jacobian of a curve of genus 1 and degree n in $\mathbf{P}^{n-1}$. No general procedure is known, but for $n \leq 4$ the problem may be resolved by writing down invariants. See [AKMMMP] for a recent account. For $n \geq 5$ we suspect that even if the corresponding invariants were found, they would be too large to write down. See [O'N] for the treatment of some special cases.

Our second approach is to work more directly over the fields K_1 and K_2. Assuming we have some way of treating the primes above n, Proposition 3.12 shows how to compute $S^{(\phi)}(E/K_2)$ and $S^{(\widehat{\phi})}(E/K_1)$. Since the field extensions $K_1/\mathbf{Q}$ and $K_2/\mathbf{Q}$ are of degree prime to n, it is then straightforward to determine the Selmer groups over $\mathbf{Q}$.

We are left with the problem of resolving local solubility at the primes above n. This we know how to do for the field $K = \mathbf{Q}(\boldsymbol{\mu}_n)$. Unfortunately is not clear how to extend our results to a general number field. However, it is easy enough to make progress for certain specific choices of M_1 and M_2. For example, if the prime above n splits in K_1K_2/K then Proposition 5.12 suffices to determine local solubility.

We give an example in the case $n = 7$ with M_1 the Galois module defined by the inverse of the cyclotomic character $\psi : G_{\mathbf{Q}} \to (\mathbf{Z}/7\mathbf{Z})^{\times}$.

Let B_ρ be the elliptic curve with Weierstrass equation

$$y^2 = x^3 - 27c_4x - 54c_6$$

where

$$\begin{aligned} c_4 &= 7(\rho^2-\rho+1)(\rho^2-3\rho-3)(3\rho^2-9\rho+5)(5\rho^2-\rho-1), \\ c_6 &= 49(\rho^4-6\rho^3+17\rho^2-24\rho+9) \\ &\qquad (3\rho^4-4\rho^3-5\rho^2-2\rho-1)(9\rho^4-12\rho^3-\rho^2+8\rho-3), \end{aligned}$$

and

$$\Delta(B_\rho) = -343(\rho^3-\rho^2-2\rho+1)^7(\rho^3-2\rho^2-\rho+1).$$

We find $B_\rho \cong D_{\nu(\rho)}$ over $\mathbf{Q}(\boldsymbol{\mu}_7)$ where ν is the involution of $\mathbf{P}^1$ exchanging

$$\begin{aligned} 0, 1, \infty &\leftrightarrow \text{roots of } \rho^3-\rho^2-2\rho+1=0 \\ \text{roots of } \lambda^3-8\lambda^2+5\lambda+1=0 &\leftrightarrow \text{roots of } \rho^3-2\rho^2-\rho+1=0. \end{aligned}$$

Indeed this is how we constructed the family B_ρ. By keeping track of the torsion, we see B_ρ is the universal family of elliptic curves containing a labelled copy of the Galois module M_1. Thus $B_\rho \cong B_{(\rho-1)/\rho}$ over $\mathbf{Q}$ and there is a 7-isogeny $\phi : B_\rho \to B^*_{1-\rho}$ defined over $\mathbf{Q}$. Here we recall our notation E^* for the -7-twist of an elliptic curve E over $\mathbf{Q}$.

We give an analogue of Theorem 1 for the isogeny $\phi : B_\rho \to B^*_{1-\rho}$.

Proposition B.2 *Let $\rho \in \mathbf{Q}$ and put*

$$\begin{aligned} \mathcal{A} &= \{\, p \text{ prime} \mid \rho^3-2\rho^2-\rho+1 \equiv 0 \pmod p \,\} \\ \mathcal{B} &= \{\, p \text{ prime} \mid \rho^3-\rho^2-2\rho+1 \equiv 0 \pmod p \text{ and } p \equiv 1 \pmod 7 \,\}. \end{aligned}$$

Then there is a pairing Ξ on $\mathbf{Z}/7\mathbf{Z}$-vector spaces of dimensions $|\mathcal{A}|$ and $|\mathcal{B}|$ such that $S^{(\phi)}(B_\rho/\mathbf{Q}) \cong \ker_L(\Xi)$ and $S^{(\widehat{\phi})}(B^*_{1-\rho}/\mathbf{Q}) \cong \ker_R(\Xi)$.

Proof. Apply Theorem 3 with $\lambda = \eta(\nu(\rho))$ and consider the action of $\mathrm{Gal}(K/\mathbf{Q})$ on the Selmer groups. □

Remark B.3 The proposition gives $|\mathcal{A}|+|\mathcal{B}|-2\,\mathrm{rank}(\Xi)$ as an upper bound for the rank. A computation of reduction types shows that the places with root number -1 are $(\mathcal{A}\Delta\{7\}) \cup \mathcal{B} \cup \{\infty\}$ where Δ denotes symmetric difference. As in §2.2 we recover a parity result.

It is hoped that by studying further examples of Galois modules M_1 and M_2 we might generalise Theorem 1 to any pair of n-isogenous elliptic curves. Such curves are parametrised by $X_0(n) \cong \mathbf{P}^1$ for $n = 5, 7$ and 13. This raises the hope of performing yet higher descents.

Appendix C

Explicit covering maps

Let $n = 5$ or 7. We recall from §1.2 our notation $C_{\lambda,\theta}$ for certain twists of C_λ. The isogeny $\phi : C_\lambda \to D_\lambda$ induces a map $\phi : C_{\lambda,\theta} \to D_\lambda$. After all $C_{\lambda,\theta}$ is described by a cocycle taking values in $\boldsymbol{\mu}_n \hookrightarrow C_\lambda$ and ϕ quotients out by this action. We obtain a commutative diagram

$$\begin{array}{ccc} C_{\lambda,\theta} & & \\ \| & \searrow & \\ C_\lambda & \longrightarrow & D_\lambda \end{array}$$

where both degree n maps ϕ are defined over K. If we give equations for $C_{\lambda,\theta}$ via push-out, then the map $\phi : C_{\lambda,\theta} \to D_\lambda$ is trivial to write down. In contrast, if we use the projective method then describing the map ϕ is somewhat more involved. We arrive at some equations by following the proof of [V2, Théorème 9.13].

Case $n = 5$. Let $\lambda, \tau_0, \ldots, \tau_4 \in K$ with $\lambda = \prod \tau_i$. We recall that the curve $T = T[\lambda; \tau_0, \ldots, \tau_4]$ lies on the quadrics

$$\begin{aligned} A &= \tau_0 x_0^2 + x_1 x_4 - \tau_2\tau_3 x_2 x_3 \\ B &= \tau_4 x_4^2 + x_0 x_3 - \tau_1\tau_2 x_1 x_2 \\ C &= \tau_2 x_2^2 + x_1 x_3 - \tau_0\tau_4 x_0 x_4. \end{aligned}$$

The map $\phi : T \to D_\lambda$ is given by $(x_0 : \ldots : x_4) \mapsto (X/Z, Y/Z)$ where

$$X = \lambda\tau_0\tau_1 x_0 x_1 x_4, \quad Y = \lambda^2 x_2 x_4^2, \quad Z = -\tau_0^2\tau_1 x_0^3.$$

We justify this assertion by recording the identity

$$\begin{aligned} -\lambda^3\tau_0^3\tau_1^2 x_0^3 x_4^2\big((\tau_1 x_1^2 + x_0 x_2)A + \tau_2\tau_3 x_2^2 B + \tau_1\tau_2\tau_3 x_1 x_2 C\big) \\ = Y^2 Z + (1-\lambda)XYZ - \lambda Y Z^2 - X^3 + \lambda X^2 Z. \end{aligned}$$

Case $n=7$. Let $\lambda, \tau_0, \ldots, \tau_6 \in K$ with $\lambda^4(\lambda-1) = \prod \tau_i$. We recall that the curve $T = T[\lambda; \tau_0, \ldots, \tau_6]$ lies on the quadrics

$$\begin{aligned} A &= \tau_0 x_0^2 + x_1 x_6 - (1/\lambda^2)\tau_2\tau_3\tau_4\tau_5 x_2 x_5 \\ B &= \tau_6 x_6^2 + x_0 x_5 - (1/\lambda^2)\tau_1\tau_2\tau_3\tau_4 x_1 x_4 \\ C &= (1/\lambda)\tau_2\tau_3\tau_4 x_2 x_4 + \lambda x_1 x_5 - \tau_0\tau_6 x_0 x_6. \end{aligned}$$

The map $\phi : T \to D_\lambda$ is given by $(x_0 : \ldots : x_6) \mapsto (X/Z, Y/Z)$ where

$$X = \lambda^2(\lambda-1)\tau_0\tau_1 x_0 x_1 x_6, \quad Y = \lambda^4(\lambda-1)^2 x_2 x_6^2, \quad Z = -\tau_0^2\tau_1 x_0^3.$$

We justify this assertion by recording the identity

$$\begin{aligned} -\lambda^3(\lambda-1)^3\tau_0^3\tau_1^2 x_0^3 x_6^2\big(\lambda^3(\tau_1 x_1^2 + x_0 x_2)A + \lambda\tau_2\tau_3\tau_4\tau_5 x_2^2 B + \tau_1\tau_2\tau_3\tau_4\tau_5 x_1 x_2 C\big) \\ = Y^2 Z + (1+\lambda-\lambda^2)XYZ + (\lambda^2-\lambda^3)YZ^2 - X^3 - (\lambda^2-\lambda^3)X^2 Z. \end{aligned}$$

Although not required for the proof of any of our descent theorems, these formulae serve a number of purposes. They enable us to exhibit elements of the Tate-Shafarevich group from an elementary point of view. This we did in the introduction with $n = 5$, $\lambda = 30$ and $T = T[30; 1, 1, 2, 3, 5]$. The formulae may also be used to turn knowledge of $\mathbf{Q}$-points on the torsors $C_{\lambda,\theta}$ into knowledge of generators for $D_\lambda(\mathbf{Q})/\phi C_\lambda(\mathbf{Q})$. As explained in [Cr, §3.6] it is often a good idea to search for rational points on the torsors covering an elliptic curve, rather than on the curve itself. However, in our case it seems likely the lack of a convenient algorithm searching for points on $T[\lambda; \tau_0, \ldots, \tau_{n-1}]$ will more than outweigh the advantage that the points sought have smaller height.

Appendix D

Tables

The construction of tables of examples has played an important role in the development of our descent theorems. We now illustrate Theorems 1–3 by reproducing some of these tables. Many of the examples listed are accessible to calculation by hand. However we have constructed the tables electronically, not least in the hope of keeping them free from errors.

Where possible we identify the curves listed with those in Cremona's tables [Cr]. 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. In the construction of our tables we also use Cremona's programs `mwrank`, which performs a 2-descent, and `findinf`, which searches for points of infinite order. The L-values listed are those computed by `pari`. In the interests of clear presentation, if not of rigour, we have recorded the L-value as 0 whenever the computed value vanishes to 20 decimal places.

The reader's attention is drawn to Remark 1.2 to explain why, for instance, the entries $\lambda = \pm 1$ in Table 1 are identical. The tables have been constructed so as not to contain repeats of this form.

Table 1 ($n=5$) and Table 2 ($n=7$)

We apply Theorem 1 for $\lambda \in \mathbf{Z}$ with $|\lambda| \leq 50$. For each pair of n-isogenous curves C_λ and D_λ we list 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_ϕ for the rank obtained by descent via n-isogeny. Finally we compare with $r = \operatorname{rank} D_\lambda(\mathbf{Q})$ as computed by `mwrank` and $L(D_\lambda, 1)$ as computed by `pari`. For

$n = 5$ and $\lambda = -47, -46, -31, -19, 38$, `mwrank` fails to completely determine $\operatorname{rank} D_\lambda(\mathbf{Q})$ since there are elements of order 2 in the Tate-Shafarevich group. In these cases our descent via 5-isogeny suffices to determine the rank. For $n = 7$ many of the curves considered are too large for us to run `mwrank` and we omit the column r accordingly.

Table 3 ($n=5$) and Table 4 ($n=7$)

We apply Theorem 1 for $\lambda \in \mathbf{Q}$ with C_λ and D_λ curves of conductor $N \leq 5300$. The list of curves considered is taken from Cremona's tables by searching for curves with rational torsion of order 5, 7 or 10. The quantities tabulated are as described for Tables 1 and 2, except that $r = \operatorname{rank} D_\lambda(\mathbf{Q})$ is taken directly from Cremona's tables, and we omit the L-value.

Table 5 ($n=5$)

We apply Theorem 2 for $\tau \in \mathbf{Z}$ with $|\tau| \leq 15$. For each example we list the sets of primes $\mathcal{P}$, $\mathcal{Q}$ and $\mathcal{R}$, the rank of the pairing Ψ and the estimates r_ϕ, r_ψ and r_5 for $\operatorname{rank} E_\tau(\mathbf{Q})$. The estimates r_ϕ and r_ψ are the Selmer ranks (30) obtained by applying Theorem 1 with $\lambda = \tau^5$ respectively $\lambda = \tau f(\tau)/g(\tau)$. The estimate $r_5 \leq \min\{r_\phi, r_\psi\}$ is the Selmer rank (31) obtained by applying Theorem 2. Finally we record $L(E_\tau, 1)$ as computed by `pari`. Nearly all the curves in this table are too large for us to run `mwrank`.

The remaining tables give details of descent calculations over $K = \mathbf{Q}(\boldsymbol{\mu}_n)$. For E an elliptic curve over $\mathbf{Q}$ we recall our notation E^* for the 5- respectively -7-twist of E.

Table 6 ($n=5$) and Table 7 ($n=7$)

We apply Theorem 3 for $\lambda \in \mathbf{Z}$ with $-15 \leq \lambda \leq 20$. The quantities tabulated are the conductor N and Cremona labels # for C_λ and D_λ, the conductor N^* and Cremona labels $\#^*$ for C_λ^* and D_λ^*, the sets of rational primes $\mathcal{A}\downarrow$ and $\mathcal{B}\downarrow$ below $\mathcal{A}$ and $\mathcal{B}$, the numbers of primes $a = |\mathcal{A}|$ and $b = |\mathcal{B}|$, the cusp number $c = c(\lambda)$, the rank of the pairing Ξ, the dimensions of the Selmer groups $S^{(\phi)}(C_\lambda/K)$ and $S^{(\widehat{\phi})}(D_\lambda/K)$ and finally our estimates r, r^* and R for $\operatorname{rank} D_\lambda(\mathbf{Q})$, $\operatorname{rank} D_\lambda^*(\mathbf{Q})$ and $\operatorname{rank} D_\lambda(K)$ obtained by descent via n-isogeny. The estimate R is the Selmer rank (52) computed using Theorem 3. The estimates r and r^* are computed by considering the action of $\operatorname{Gal}(K/\mathbf{Q})$ on the Selmer groups $S^{(\phi)}(C_\lambda/K)$ and $S^{(\widehat{\phi})}(D_\lambda/K)$. Notice that care must be taken here to allow for the Galois twist involved when we identify $S^{(\widehat{\phi})}(D_\lambda/K)$ as a subgroup of $H^1(K, \boldsymbol{\mu}_n) = K^\times/(K^\times)^n$. Clearly

we have $r + r^* \leq R$, and the same inequality holds for the true ranks. An entry in bold indicates an estimate we know to be equal to the true rank, *e.g.* by running `findinf` to exhibit sufficiently many points of infinite order. An entry in italics indicates an estimate we know to be larger than the true rank, *e.g.* by running `mwrank` or by computing an L-value. For reasons of space we omit the columns a and b in Table 6 and the columns N^* and $\#^*$ in Table 7.

Table 8 ($n=7$)

We apply Theorem 3 for some values $\lambda = \eta(\nu(\rho))$ with $\rho \in \mathbf{Q}$. Here ν is the involution of $\mathbf{P}^1$ described in Appendix B. This choice is made so that over K we may identify $\phi : B_\rho \to B^*_{1-\rho}$ with $\phi : C_\lambda \to D_\lambda$. The quantities tabulated are the conductor N for B_ρ and B^*_ρ, the sets of rational primes $\mathcal{A}\downarrow$ and $\mathcal{B}\downarrow$ below $\mathcal{A}$ and $\mathcal{B}$, the numbers of primes $a = |\mathcal{A}|$ and $b = |\mathcal{B}|$, the cusp number $c = c(\lambda)$, the rank of the pairing Ξ, the dimension of the Selmer groups $S^{(\phi)}(C_\lambda/K)$ and $S^{(\widehat{\phi})}(D_\lambda/K)$ and finally our estimates r, r^* and R for $\operatorname{rank} B_\rho(\mathbf{Q})$, $\operatorname{rank} B^*_\rho(\mathbf{Q})$ and $\operatorname{rank} B_\rho(K)$ obtained by descent via 7-isogeny. The entries in bold and italics have the same meanings as described for Tables 6 and 7.

Table 9 ($n=5$) and Table 10 ($n=7$)

We apply Theorem 3 for some values $\lambda \in K$ chosen such that $\mathcal{A} = \emptyset$ and D_λ admits a model E over $\mathbf{Q}$. For each example we list λ, $\eta(\lambda)$, the conductor N and Cremona label $\#$ for E, the set of rational primes $\mathcal{B}\downarrow$ below $\mathcal{B}$, the number of primes $b = |\mathcal{B}|$, the cusp number $c = c(\lambda)$, the rank of the pairing Ξ, the dimension of the Selmer groups $S^{(\phi)}(C_\lambda/K)$ and $S^{(\widehat{\phi})}(D_\lambda/K)$ and finally our estimates r, r^* and R for $\operatorname{rank} E(\mathbf{Q})$, $\operatorname{rank} E^*(\mathbf{Q})$ and $\operatorname{rank} E(K)$ obtained by descent via n-isogeny. The entries in bold and italics have the same meaning as described for Tables 6 and 7.

In the case $n = 5$ we write ϕ for the golden ratio, and take $\lambda = \phi^j$ for j an odd integer. In each example we have taken $E = C_{\eta(\lambda)}$.

In the case $n = 7$ we take $\lambda = u_t$ a root of

$$\lambda^3 - t\lambda^2 + (t-3)\lambda + 1 = 0$$

for some $t \in \mathbf{Z}$. The only values $t \in \mathbf{Z}$ for which this polynomial splits over K are $t = 1, 2, -5, 8, -12, 15, -1259, 1262$. For the entries above the line we have taken $E = C_{-2}$, C_5 and $C_{22/3}$. For the entries below the line we have taken $E = B_1$, B_2, B_3 and $B_{9/4}$.

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	$L(D_\lambda, 1)$
-50	30490		$\{2,5\}$	$\emptyset$	0	2	0	1	1	0
-49	20573		$\{7\}$	$\emptyset$	0	1	0	0	0	0.30766099
-48	16986		$\{2,3\}$	$\emptyset$	0	2	0	1	1	0
-47	128075		$\{47\}$	$\emptyset$	0	1	0	0		0.63400946
-46	120566		$\{2,23\}$	$\{2621\}$	1	1	0	0		3.21920195
-45	37785		$\{3,5\}$	$\{11\}$	1	1	0	0	0	1.63505070
-44	53218		$\{2,11\}$	$\{41\}$	1	1	0	0	0	1.66142256
-43	99803		$\{43\}$	$\{11,211\}$	0	1	2	2	2	0
-42	93450		$\{2,3,7\}$	$\emptyset$	0	3	0	2	0	4.29287969
-41	87371		$\{41\}$	$\{2131\}$	0	1	1	1	1	0
-40	20390		$\{2,5\}$	$\emptyset$	0	2	0	1	1	0
-39	76011		$\{3,13\}$	$\emptyset$	0	2	0	1	1	0
-38	70718		$\{2,19\}$	$\{1861\}$	1	1	0	0	0	0.92118046
-37	65675		$\{37\}$	$\{71\}$	0	1	1	1	1	0
-36	10146		$\{2,3\}$	$\emptyset$	0	2	0	1	1	0
-35	56315		$\{5,7\}$	$\emptyset$	0	2	0	1	1	0
-34	51986		$\{2,17\}$	$\{11\}$	1	1	0	0	0	0.99514042
-33	47883		$\{3,11\}$	$\{1451\}$	1	1	0	0	0	1.01579851
-32	550	K2, 3	$\{2\}$	$\{5,11\}$	1	0	1	0	0	2.07491286
-31	40331		$\{31\}$	$\{1301\}$	0	1	1	1		0
-30	36870		$\{2,3,5\}$	$\emptyset$	0	3	0	2	0	5.42048094
-29	33611		$\{29\}$	$\{61\}$	0	1	1	1	1	0
-28	15274		$\{2,7\}$	$\{1091\}$	1	1	0	0	0	2.27161017
-27	3075	L2, 1	$\{3\}$	$\{41\}$	0	1	1	1	1	0
-26	806	F2, 1	$\{2,13\}$	$\{31\}$	1	1	0	0	0	2.38703680
-25	4495	D2, 1	$\{5\}$	$\{31\}$	0	1	1	1	1	0
-24	5034	E2, 1	$\{2,3\}$	$\emptyset$	0	2	0	1	1	0
-23	17963		$\{23\}$	$\{11,71\}$	0	1	2	2	2	0
-22	15950		$\{2,11\}$	$\emptyset$	0	2	0	1	1	0
-21	14091		$\{3,7\}$	$\{11,61\}$	1	1	1	1	1	0
-20	6190		$\{2,5\}$	$\emptyset$	0	2	0	1	1	0
-19	10811		$\{19\}$	$\emptyset$	0	1	0	0		1.17090283
-18	3126	C2, 1	$\{2,3\}$	$\{521\}$	1	1	0	0	0	3.02909724
-17	8075		$\{17\}$	$\emptyset$	0	1	0	0	0	0.31396220

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	$L(D_\lambda, 1)$
-16	862	E2, 1	$\{2\}$	$\{431\}$	0	1	1	1	1	0
-15	5835		$\{3, 5\}$	$\emptyset$	0	2	0	1	1	0
-14	4886	F2, 1	$\{2, 7\}$	$\emptyset$	0	2	0	1	1	0
-13	4043	A2, 1	$\{13\}$	$\{311\}$	0	1	1	1	1	0
-12	1650	S2, 1	$\{2, 3\}$	$\{11\}$	1	1	0	0	0	3.87816291
-11	2651	C2, 1	$\{11\}$	$\{241\}$	0	1	1	1	1	0
-10	2090	N2, 1	$\{2, 5\}$	$\{11\}$	1	1	0	0	0	2.15518557
-9	537	E2, 1	$\{3\}$	$\emptyset$	0	1	0	0	0	0.91494535
-8	302	A2, 1	$\{2\}$	$\{151\}$	0	1	1	1	1	0
-7	175	A1, 2	$\{7\}$	$\{5\}$	0	1	1	1	1	0
-6	606	F2, 1	$\{2, 3\}$	$\{101\}$	1	1	0	0	0	2.84676247
-5	395	C2, 1	$\{5\}$	$\emptyset$	0	1	0	0	0	0.62499546
-4	118	B2, 1	$\{2\}$	$\emptyset$	0	1	0	0	0	1.39538063
-3	123	A2, 1	$\{3\}$	$\{41\}$	0	1	1	1	1	0
-2	50	B3, 1	$\{2\}$	$\emptyset$	0	1	0	0	0	0.95681123
± 1	11	A1, 3	$\emptyset$	$\{11\}$	0	0	1	0	0	0.25384186
2	38	B2, 1	$\{2\}$	$\emptyset$	0	1	0	0	0	0.81924563
3	75	C2, 1	$\{3\}$	$\emptyset$	0	1	0	0	0	0.62723493
4	58	B2, 1	$\{2\}$	$\emptyset$	0	1	0	0	0	1.03320751
5	155	A2, 1	$\{5\}$	$\{31\}$	0	1	1	1	1	0
6	186	B2, 1	$\{2, 3\}$	$\{31\}$	1	1	0	0	0	1.95289767
7	203	A2, 1	$\{7\}$	$\emptyset$	0	1	0	0	0	0.35054172
8	50	B4, 2	$\{2\}$	$\emptyset$	0	1	0	0	0	0.95681123
9	57	C2, 1	$\{3\}$	$\emptyset$	0	1	0	0	0	0.58650959
10	110	A2, 1	$\{2, 5\}$	$\{11\}$	1	1	0	0	0	1.35954181
11	11	A2, 1	$\{11\}$	$\emptyset$	0	1	0	0	0	0.25384186
12	66	C3, 1	$\{2, 3\}$	$\{11\}$	1	1	0	0	0	1.19161482
13	325	E2, 1	$\{13\}$	$\emptyset$	0	1	0	0	0	0.44965292
14	574	J2, 1	$\{2, 7\}$	$\{41\}$	1	1	0	0	0	2.12965065
15	885	D2, 1	$\{3, 5\}$	$\emptyset$	0	2	0	1	1	0
16	158	C2, 1	$\{2\}$	$\emptyset$	0	1	0	0	0	1.54436244
17	1717	C2, 1	$\{17\}$	$\{101\}$	0	1	1	1	1	0
18	150	A2, 4	$\{2, 3\}$	$\{5\}$	1	1	0	0	0	1.76925925
19	2869	B2, 1	$\{19\}$	$\{151\}$	0	1	1	1	1	0

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	$L(D_\lambda, 1)$
20	1790	D2, 1	$\{2,5\}$	$\emptyset$	0	2	0	1	1	0
21	4389	K2, 1	$\{3,7\}$	$\{11\}$	1	1	0	0	0	1.57719020
22	5302		$\{2,11\}$	$\{241\}$	0	2	1	2	2	0
23	6325		$\{23\}$	$\{11\}$	0	1	1	1	1	0
24	1866	I2, 1	$\{2,3\}$	$\{311\}$	1	1	0	0	0	4.28015800
25	1745	E2, 1	$\{5\}$	$\emptyset$	0	1	0	0	0	0.55338675
26	10114		$\{2,13\}$	$\emptyset$	0	2	0	1	1	0
27	1293	E2, 1	$\{3\}$	$\{431\}$	0	1	1	1	1	0
28	6650		$\{2,7\}$	$\emptyset$	0	2	0	1	1	0
29	15109		$\{29\}$	$\{521\}$	0	1	1	1	1	0
30	17070		$\{2,3,5\}$	$\emptyset$	0	3	0	2	0	6.02423606
31	19189		$\{31\}$	$\emptyset$	0	1	0	0	0	0.23502226
32	1342	C2, 1	$\{2\}$	$\{11,61\}$	1	0	1	0	0	1.14697681
33	23925		$\{3,11\}$	$\emptyset$	0	2	0	1	1	0
34	26554		$\{2,17\}$	$\{11,71\}$	1	1	1	1	1	0
35	29365		$\{5,7\}$	$\emptyset$	0	2	0	1	1	0
36	5394		$\{2,3\}$	$\{31\}$	1	1	0	0	0	4.19212658
37	1147	B2, 1	$\{37\}$	$\{31\}$	0	1	1	1	1	0
38	38950		$\{2,19\}$	$\{41\}$	1	1	0	0		4.02140423
39	42549		$\{3,13\}$	$\{1091\}$	0	2	1	2	2	0
40	11590		$\{2,5\}$	$\{61\}$	1	1	0	0	0	2.89912975
41	50389		$\{41\}$	$\emptyset$	0	1	0	0	0	0.18962514
42	54642		$\{2,3,7\}$	$\{1301\}$	1	2	0	1	1	0
43	11825		$\{43\}$	$\{5,11\}$	0	1	2	2	2	0
44	31922		$\{2,11\}$	$\{1451\}$	1	1	0	0	0	1.79541292
45	22935		$\{3,5\}$	$\{11\}$	1	1	0	0	0	1.76439797
46	74014		$\{2,23\}$	$\emptyset$	0	2	0	1	1	0
47	79477		$\{47\}$	$\emptyset$	0	1	0	0	0	0.17058134
48	10650		$\{2,3\}$	$\{71\}$	1	1	0	0	0	3.35622748
49	13027		$\{7\}$	$\{1861\}$	0	1	1	1	1	0
50	19490		$\{2,5\}$	$\emptyset$	0	2	0	1	1	0

Table 2 ($n=7$) Descent via $\phi : C_\lambda \to D_\lambda$ over $\mathbf{Q}$

λ	N	$\mathcal{A}$	$\mathcal{B}$	Ξ	ϕ	$\widehat{\phi}$	r_ϕ	$L(D_\lambda, 1)$
-50	74076990	$\{2,3,5,17\}$	$\{11173\}$	1	3	0	2	2.05696503
-49	9597070	$\{2,5,7\}$	$\{71\}$	1	2	0	1	0
-48	5429046	$\{2,3,7\}$	$\{129263\}$	1	2	0	1	0
-47	34327578	$\{2,3,47\}$	$\{2969\}$	1	2	0	1	0
-46	247533866	$\{2,23,47\}$	$\{114493\}$	1	2	0	1	0
-45	74208810	$\{2,3,5,23\}$	$\emptyset$	0	4	0	3	0
-44	33294030	$\{2,3,5,11\}$	$\{7,29,71\}$	3	1	0	0	5.11304620
-43	89409298	$\{2,11,43\}$	$\emptyset$	0	3	0	2	0
-42	159666654	$\{2,3,7,43\}$	$\{211\}$	1	3	0	2	5.53178972
-41	142190706	$\{2,3,7,41\}$	$\{71,1163\}$	2	2	0	1	0
-40	31569590	$\{2,5,41\}$	$\{5923\}$	1	2	0	1	0
-39	27955590	$\{2,3,5,13\}$	$\{43,1667\}$	2	2	0	1	0
-38	98720466	$\{2,3,13,19\}$	$\{29,2297\}$	2	2	0	1	0
-37	86875334	$\{2,19,37\}$	$\{7\}$	1	2	0	1	0
-36	12699066	$\{2,3,37\}$	$\emptyset$	0	3	0	2	9.21681632
-35	11098290	$\{2,3,5,7\}$	$\{1289\}$	1	3	0	2	7.51425902
-34	57977990	$\{2,5,7,17\}$	$\emptyset$	0	4	0	3	0
-33	50280186	$\{2,3,11,17\}$	$\{1093\}$	1	3	0	2	2.07210713
-32	2713854	$\{2,3,11\}$	$\emptyset$	0	3	0	2	6.23082208
-31	2333246	$\{2,31\}$	$\{37633\}$	1	1	0	0	0.93821430
-30	31944570	$\{2,3,5,31\}$	$\{7,701\}$	2	2	0	1	0
-29	27197070	$\{2,3,5,29\}$	$\{43\}$	1	3	0	2	23.0964755
-28	11515378	$\{2,7,29\}$	$\{113\}$	1	2	0	1	0
-27	1077258	$\{2,3,7\}$	$\emptyset$	0	3	0	2	2.47367425
-26	1802814	$\{2,3,13\}$	$\{29\}$	1	2	0	1	0
-25	2697370	$\{2,5,13\}$	$\{20749\}$	1	2	0	1	0
-24	556530	$\{2,3,5\}$	$\emptyset$	0	3	0	2	11.9897036
-23	2278794	$\{2,3,23\}$	$\{7,337\}$	2	1	0	0	6.42266497
-22	7402274	$\{2,11,23\}$	$\emptyset$	0	3	0	2	2.30008612
-21	5956566	$\{2,3,7,11\}$	$\emptyset$	0	4	0	3	0
-20	2372790	$\{2,3,5,7\}$	$\{11299\}$	1	3	0	2	9.37961008
-19	1869790	$\{2,5,19\}$	$\{757\}$	1	2	0	1	0
-18	970482	$\{2,3,19\}$	$\{8513\}$	1	2	0	1	0
-17	745518	$\{2,3,17\}$	$\{7309\}$	1	2	0	1	0

Table 2 ($n=7$) Descent via $\phi : C_\lambda \to D_\lambda$ over $\mathbf{Q}$

λ	N	#	$\mathcal{A}$	$\mathcal{B}$	Ξ	ϕ	$\widehat{\phi}$	r_ϕ	r	$L(D_\lambda, 1)$
-16	211582		$\{2, 17\}$	$\{7, 127\}$	1	1	1	1		0
-15	157470		$\{2, 3, 5\}$	$\{29\}$	1	2	0	1		0
-14	920010		$\{2, 3, 5, 7\}$	$\{337\}$	1	3	0	2		8.20530033
-13	657566		$\{2, 7, 13\}$	$\{3613\}$	1	2	0	1		0
-12	229242		$\{2, 3, 13\}$	$\emptyset$	0	3	0	2		2.96566337
-11	155298		$\{2, 3, 11\}$	$\emptyset$	0	3	0	2		3.37997297
-10	4730	K2, 1	$\{2, 5, 11\}$	$\{43\}$	1	2	0	1	1	0
-9	42630		$\{2, 3, 5\}$	$\{7, 29\}$	2	1	0	0	0	4.54417718
-8	6378		$\{2, 3\}$	$\emptyset$	0	2	0	1	1	0
-7	10766		$\{2, 7\}$	$\emptyset$	0	2	0	1	1	0
-6	22386		$\{2, 3, 7\}$	$\emptyset$	0	3	0	2	0	4.02654416
-5	10470		$\{2, 3, 5\}$	$\emptyset$	0	3	0	2	0	5.14484219
-4	2110	H2, 1	$\{2, 5\}$	$\{211\}$	1	1	0	0	0	1.96226711
-3	678	D2, 1	$\{2, 3\}$	$\{113\}$	1	1	0	0	0	2.79409146
-2	294	B1, 2	$\{2, 3\}$	$\{7\}$	1	1	0	0	0	2.21206490
$-1, 2$	26	B2, 1	$\{2\}$	$\emptyset$	0	1	0	0	0	0.62096535
3	174	B2, 1	$\{2, 3\}$	$\{29\}$	1	1	0	0	0	1.85980396
4	258	F2, 1	$\{2, 3\}$	$\{43\}$	1	1	0	0	0	2.13616829
5	490	K1, 2	$\{2, 5\}$	$\{7\}$	1	1	0	0	0	1.40933201
6	1230	K2, 1	$\{2, 3, 5\}$	$\emptyset$	0	3	0	2	0	3.53252671
7	546	F2, 1	$\{2, 3, 7\}$	$\emptyset$	0	3	0	2	0	2.67156776
8	574	I2, 1	$\{2, 7\}$	$\emptyset$	0	2	0	1	1	0
9	762	G2, 1	$\{2, 3\}$	$\{127\}$	1	1	0	0	0	2.91591947
10	7530		$\{2, 3, 5\}$	$\emptyset$	0	3	0	2	0	5.63627952
11	46090		$\{2, 5, 11\}$	$\emptyset$	0	3	0	2	0	2.37770891
12	42042		$\{2, 3, 11\}$	$\{7\}$	1	2	0	1	1	0
13	71058		$\{2, 3, 13\}$	$\{911\}$	1	2	0	1	1	0
14	226954		$\{2, 7, 13\}$	$\{29, 43\}$	2	1	0	0		1.54832039
15	346710		$\{2, 3, 5, 7\}$	$\{127\}$	1	3	0	2		9.58816728
16	63870		$\{2, 3, 5\}$	$\{2129\}$	1	2	0	1		0
17	91358		$\{2, 17\}$	$\emptyset$	0	2	0	1		0
18	339762		$\{2, 3, 17\}$	$\emptyset$	0	3	0	2		7.92763280
19	463638		$\{2, 3, 19\}$	$\{7\}$	1	2	0	1		0
20	71630		$\{2, 5, 19\}$	$\{29\}$	1	2	0	1		0

Table 2 ($n=7$) Descent via $\phi : C_\lambda \to D_\lambda$ over $\mathbf{Q}$

λ	N	$\mathcal{A}$	$\mathcal{B}$	Ξ	ϕ	$\widehat{\phi}$	r_ϕ	$L(D_\lambda, 1)$
21	1226190	$\{2,3,5,7\}$	$\{5839\}$	1	3	0	2	10.5517170
22	3181794	$\{2,3,7,11\}$	$\{71\}$	1	3	0	2	4.85751653
23	4073806	$\{2,11,23\}$	$\emptyset$	0	3	0	2	2.56499226
24	1288506	$\{2,3,23\}$	$\emptyset$	0	3	0	2	7.13460156
25	322530	$\{2,3,5\}$	$\{827\}$	1	2	0	1	0
26	1598870	$\{2,5,13\}$	$\{7\}$	1	2	0	1	0
27	1090986	$\{2,3,13\}$	$\{71,197\}$	2	1	0	0	1.44673411
28	664482	$\{2,3,7\}$	$\emptyset$	0	3	0	2	2.71225343
29	7229642	$\{2,7,29\}$	$\emptyset$	0	3	0	2	0.84937377
30	17357370	$\{2,3,5,29\}$	$\{71,281\}$	2	2	0	1	0
31	20700870	$\{2,3,5,31\}$	$\emptyset$	0	4	0	3	0
32	1533694	$\{2,31\}$	$\{29\}$	1	1	0	0	1.01837396
33	1807806	$\{2,3,11\}$	$\{7,43\}$	2	1	0	0	6.74846858
34	33914694	$\{2,3,11,17\}$	$\emptyset$	0	4	0	3	0
35	39568690	$\{2,5,7,17\}$	$\emptyset$	0	4	0	3	0
36	7658490	$\{2,3,5,7\}$	$\emptyset$	0	4	0	3	0
37	8854914	$\{2,3,37\}$	$\{39887\}$	1	2	0	1	0
38	61176466	$\{2,19,37\}$	$\{3347\}$	1	2	0	1	0
39	70168254	$\{2,3,13,19\}$	$\{113\}$	1	3	0	2	1.75363708
40	20046390	$\{2,3,5,13\}$	$\{7\}$	1	3	0	2	20.1140714
41	22828390	$\{2,5,41\}$	$\emptyset$	0	3	0	2	2.74954086
42	103642014	$\{2,3,7,41\}$	$\emptyset$	0	4	0	3	0
43	117265386	$\{2,3,7,43\}$	$\{29\}$	1	3	0	2	1.47312805
44	66141482	$\{2,11,43\}$	$\emptyset$	0	3	0	2	0.40395817
45	24799830	$\{2,3,5,11\}$	$\{337\}$	1	3	0	2	5.43281068
46	55640910	$\{2,3,5,23\}$	$\{6203\}$	1	3	0	2	2.61176176
47	186768694	$\{2,23,47\}$	$\{7,43\}$	2	1	0	0	0.71807052
48	26057082	$\{2,3,47\}$	$\{92401\}$	1	2	0	1	0
49	4144854	$\{2,3,7\}$	$\{29\}$	1	2	0	1	0
50	7367570	$\{2,5,7\}$	$\emptyset$	0	3	0	2	0.64283549

Table 3 ($n=5$) 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	$\emptyset$	{11}	0	0	1	0	0
11	11	A2, 1	{11}	$\emptyset$	0	1	0	0	0
2	38	B2, 1	{2}	$\emptyset$	0	1	0	0	0
−2	50	B3, 1	{2}	$\emptyset$	0	1	0	0	0
8	50	B4, 2	{2}	$\emptyset$	0	1	0	0	0
9	57	C2, 1	{3}	$\emptyset$	0	1	0	0	0
4	58	B2, 1	{2}	$\emptyset$	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}	$\emptyset$	0	1	0	0	0
10	110	A2, 1	{2, 5}	{11}	1	1	0	0	0
−4	118	B2, 1	{2}	$\emptyset$	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}	$\emptyset$	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}	$\emptyset$	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}	$\emptyset$	0	1	0	0	0
3/2	366	B2, 1	{2, 3}	{61}	1	1	0	0	0
−5	395	C2, 1	{5}	$\emptyset$	0	1	0	0	0
−3/2	426	A2, 1	{2, 3}	{71}	1	1	0	0	0
−9	537	E2, 1	{3}	$\emptyset$	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}	$\emptyset$	0	3	0	2	0
100/9	570	L4, 2	{2, 3, 5}	$\emptyset$	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

Table 3 ($n=5$) Descent via $\phi : C_\lambda \to D_\lambda$ over $\mathbf{Q}$

λ	N	#	$\mathcal{A}$	$\mathcal{B}$	Ξ	ϕ	$\widehat{\phi}$	r_ϕ	r
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
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

Table 3 ($n=5$) Descent via $\phi : C_\lambda \to D_\lambda$ over $\mathbf{Q}$

λ	N	#	$\mathcal{A}$	$\mathcal{B}$	Ξ	ϕ	$\widehat{\phi}$	r_ϕ	r
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
−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}	∅	0	2	0	1	1
15/2	3270	H2, 1	{2, 3, 5}	∅	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}	∅	0	2	0	1	1
−25	4495	D2, 1	{5}	{31}	0	1	1	1	1

Table 3 ($n=5$) Descent via $\phi : C_\lambda \to D_\lambda$ over $\mathbf{Q}$

λ	N	#	$\mathcal{A}$	$\mathcal{B}$	Ξ	ϕ	$\widehat{\phi}$	r_ϕ	r
$-16/3$	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 4 ($n=7$) Descent via $\phi : C_\lambda \to D_\lambda$ over $\mathbf{Q}$

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

Table 5 ($n=5$) Descent via $[5] : E_\tau \to E_\tau$ over $\mathbf{Q}$

τ	$\mathcal{P}$	$\mathcal{Q}$	$\mathcal{R}$	Ψ	r_ϕ	r_ψ	r_5	$L(E_\tau, 1)$
-15	$\{3,5\}$	$\{11,3761,58321\}$	$\emptyset$	4	0	4	0	
-14	$\{2,7\}$	$\{41,1091,30941\}$	$\{11\}$	4	1	3	1	0
-13	$\{13\}$	$\{11,3061,22621\}$	$\{181\}$	4	2	2	0	
-12	$\{2,3\}$	$\{11,41,3221\}$	$\{5,31\}$	4	2	2	2	0
-11	$\{11\}$	$\{41,71,251,271\}$	$\{131\}$	4	3	3	1	0
-10	$\{2,5\}$	$\{11,31,61,401\}$	$\emptyset$	4	1	5	1	0
-9	$\{3\}$	$\{11,31,151,761\}$	$\emptyset$	4	2	4	0	0.09302147
-8	$\{2\}$	$\{11,491,2801\}$	$\{71\}$	2	2	2	2	0
-7	$\{7\}$	$\{311,661\}$	$\{5,11\}$	4	2	0	0	1.15762623
-6	$\{2,3\}$	$\{11,31,61,71\}$	$\{41\}$	4	2	4	2	0
-5	$\{5\}$	$\{11,31,991\}$	$\emptyset$	2	1	3	1	0
-4	$\{2\}$	$\{11,461\}$	$\emptyset$	2	0	2	0	1.08064637
-3	$\{3\}$	$\{31,181\}$	$\{11\}$	2	1	1	1	0
-2	$\{2\}$	$\{11\}$	$\{5\}$	2	0	0	0	2.07491286
± 1	$\emptyset$	$\{11\}$	$\emptyset$	0	0	0	0	0.25384186
2	$\{2\}$	$\{11,61\}$	$\emptyset$	2	0	2	0	1.14697681
3	$\{3\}$	$\{11,41\}$	$\{5\}$	2	1	1	1	0
4	$\{2\}$	$\{181,521\}$	$\{11\}$	2	1	1	1	0
5	$\{5\}$	$\{11,101,461\}$	$\emptyset$	2	1	3	1	0
6	$\{2,3\}$	$\{11,191,991\}$	$\emptyset$	4	0	4	0	0.28811770
7	$\{7\}$	$\{11,31,61,331\}$	$\{41\}$	4	3	3	1	0
8	$\{2\}$	$\{661,1181\}$	$\{5,11\}$	4	2	0	0	0.47598299
9	$\{3\}$	$\{11,491,9091\}$	$\{71\}$	2	2	2	2	2.32573719
10	$\{2,5\}$	$\{11,761,13421\}$	$\emptyset$	4	0	4	0	4.14475951
11	$\{11\}$	$\{31,401,19141\}$	$\emptyset$	2	1	3	1	0
12	$\{2,3\}$	$\{11,71,251,2411\}$	$\{131\}$	6	2	4	0	
13	$\{13\}$	$\{11,41,71,101\}$	$\{5,31\}$	4	4	2	2	0
14	$\{2,7\}$	$\{11,31,1531,3061\}$	$\{181\}$	4	2	4	2	
15	$\{3,5\}$	$\{41,1091,61681\}$	$\{11\}$	4	1	3	1	0

Table 6 ($n=5$) Descent via $\phi : C_\lambda \to D_\lambda$ over $K = \mathbf{Q}(\mu_5)$

λ	N	#	N^*	$\#^*$	$\mathcal{A}\downarrow$	$\mathcal{B}\downarrow$	c	Ξ	ϕ	$\widehat{\phi}$	r	r^*	R
-15	5835		29175		$\{3,5\}$	$\{389\}$	0	1	3	1	**1**	**1**	**2**
-14	4886	F2, 1	122150		$\{2,7\}$	$\{349\}$	0	0	4	2	**1**	**1**	4
-13	4043	A2, 1	101075		$\{13\}$	$\{311\}$	0	2	1	2	**1**	**0**	**1**
-12	1650	S2, 1	1650	D1, 2	$\{2,3\}$	$\{11\}$	4	3	1	4	**0**	**1**	3
-11	2651	C2, 1	66275		$\{11\}$	$\{241\}$	0	2	4	2	**1**	**1**	4
-10	2090	N2, 1	10450		$\{2,5\}$	$\{11,19\}$	0	3	1	3	**0**	**0**	2
-9	537	E2, 1	13425		$\{3\}$	$\{179\}$	0	1	2	1	**0**	**1**	**1**
-8	302	A2, 1	7550		$\{2\}$	$\{151\}$	0	1	2	3	**1**	**0**	3
-7	175	A1, 2	175	C1, 2	$\{7\}$	$\emptyset$	6	2	1	2	**1**	**0**	**1**
-6	606	F2, 1	15150		$\{2,3\}$	$\{101\}$	0	2	2	2	**0**	**0**	2
-5	395	C2, 1	1975	D2, 1	$\{5\}$	$\{79\}$	0	1	2	1	**0**	**1**	**1**
-4	118	B2, 1	2950	A2, 1	$\{2\}$	$\{59\}$	0	1	2	1	**0**	**1**	**1**
-3	123	A2, 1	3075	D2, 1	$\{3\}$	$\{41\}$	0	2	1	2	**1**	**0**	**1**
-2	50	B3, 1	50	A1, 3	$\{2\}$	$\emptyset$	4	2	1	1	**0**	**0**	**0**
± 1	11	A1, 3	275	B2, 1	$\emptyset$	$\{11\}$	0	2	0	2	**0**	**0**	**0**
2	38	B2, 1	950	A2, 1	$\{2\}$	$\{19\}$	0	1	2	1	**0**	**1**	**1**
3	75	C2, 1	75	A1, 2	$\{3\}$	$\emptyset$	4	2	1	1	**0**	**0**	**0**
4	58	B2, 1	1450	A2, 1	$\{2\}$	$\{29\}$	0	1	2	1	**0**	**1**	**1**
5	155	A2, 1	775	C2, 1	$\{5\}$	$\{31\}$	0	2	1	2	**1**	**0**	**1**
6	186	B2, 1	4650	E2, 1	$\{2,3\}$	$\{31\}$	0	3	1	1	**0**	**0**	**0**
7	203	A2, 1	5075	C2, 1	$\{7\}$	$\{29\}$	0	1	2	1	**0**	**1**	**1**
8	50	B4, 2	50	A2, 4	$\{2\}$	$\emptyset$	4	2	1	1	**0**	**0**	**0**
9	57	C2, 1	1425	B2, 1	$\{3\}$	$\{19\}$	0	1	2	1	**0**	**1**	**1**
10	110	A2, 1	550	B2, 1	$\{2,5\}$	$\{11\}$	0	3	1	1	**0**	**0**	**0**
11	11	A2, 1	275	B3, 2	$\{11\}$	$\emptyset$	0	0	6	0	**0**	*2*	*4*
12	66	C3, 1	1650	B3, 1	$\{2,3\}$	$\{11\}$	0	3	1	1	**0**	**0**	**0**
13	325	E2, 1	325	D1, 2	$\{13\}$	$\emptyset$	4	2	1	1	**0**	**0**	**0**
14	574	J2, 1	14350		$\{2,7\}$	$\{41\}$	0	3	1	1	**0**	**0**	**0**
15	885	D2, 1	4425	C2, 1	$\{3,5\}$	$\{59\}$	0	1	3	1	**1**	**1**	**2**
16	158	C2, 1	3950	A2, 1	$\{2\}$	$\{79\}$	0	1	2	1	**0**	**1**	**1**
17	1717	C2, 1	42925		$\{17\}$	$\{101\}$	0	1	2	3	**1**	**0**	3
18	150	A2, 4	150	B2, 4	$\{2,3\}$	$\emptyset$	6	3	1	1	**0**	**0**	**0**
19	2869	B2, 1	71725		$\{19\}$	$\{151\}$	0	1	3	3	**1**	**1**	4
20	1790	D2, 1	8950		$\{2,5\}$	$\{179\}$	0	1	3	1	**1**	**1**	**2**

Table 7 ($n=7$) Descent via $\phi : C_\lambda \to D_\lambda$ over $K = \mathbf{Q}(\mu_7)$

λ	N	#	$\mathcal{A}\downarrow$	$\mathcal{B}\downarrow$	a	b	c	Ξ	ϕ	$\widehat{\phi}$	r	r^*	R
-15	157470		$\{2,3,5\}$	$\{29,181\}$	4	9	0	5	2	4	**1**	1	4
-14	920010		$\{2,3,5,7\}$	$\{13,337\}$	5	9	0	5	3	4	*2*	1	*5*
-13	657566		$\{2,7,13\}$	$\{3613\}$	6	6	0	4	5	2	**1**	*2*	*5*
-12	229242		$\{2,3,13\}$	$\{2939\}$	6	3	0	1	8	2	*2*	**0**	*8*
-11	155298		$\{2,3,11\}$	$\{13,181\}$	5	6	0	3	5	3	*2*	**0**	*6*
-10	4730	K2, 1	$\{2,5,11\}$	$\{43\}$	5	6	0	5	3	1	**1**	1	2
-9	42630		$\{2,3,5\}$	$\{29\}$	4	6	4	6	1	6	**0**	1	5
-8	6378		$\{2,3\}$	$\{1063\}$	3	3	0	2	4	1	**1**	**0**	3
-7	10766		$\{2,7\}$	$\{769\}$	3	3	0	2	4	1	**1**	**0**	3
-6	22386		$\{2,3,7\}$	$\{13,41\}$	4	6	0	2	5	4	*2*	**1**	*7*
-5	10470		$\{2,3,5\}$	$\{349\}$	4	3	0	2	5	1	*2*	**0**	*4*
-4	2110	H2, 1	$\{2,5\}$	$\{211\}$	3	6	0	5	1	1	**0**	**0**	**0**
-3	678	D2, 1	$\{2,3\}$	$\{113\}$	3	6	0	5	1	1	**0**	**0**	**0**
-2	294	B1, 2	$\{2,3\}$	$\emptyset$	3	0	4	5	1	1	**0**	**0**	**0**
$-1,2$	26	B2, 1	$\{2\}$	$\{13\}$	2	3	0	2	3	1	**0**	**0**	2
3	174	B2, 1	$\{2,3\}$	$\{29\}$	3	6	0	5	1	1	**0**	**0**	**0**
4	258	F2, 1	$\{2,3\}$	$\{43\}$	3	6	0	5	1	1	**0**	**0**	**0**
5	490	K1, 2	$\{2,5\}$	$\emptyset$	3	0	4	5	1	1	**0**	**0**	**0**
6	1230	K2, 1	$\{2,3,5\}$	$\{41\}$	4	3	0	2	5	1	*2*	**0**	*4*
7	546	F2, 1	$\{2,3,7\}$	$\{13\}$	4	3	0	2	5	1	*2*	**0**	*4*
8	574	I2, 1	$\{2,7\}$	$\{41\}$	3	3	0	2	4	1	**1**	**0**	3
9	762	G2, 1	$\{2,3\}$	$\{127\}$	3	6	0	5	1	1	**0**	**0**	**0**
10	7530		$\{2,3,5\}$	$\{251\}$	4	3	0	2	5	1	*2*	**0**	*4*
11	46090		$\{2,5,11\}$	$\{419\}$	5	3	0	2	6	1	*2*	1	*5*
12	42042		$\{2,3,11\}$	$\{13\}$	5	3	4	6	2	3	**1**	**0**	3
13	71058		$\{2,3,13\}$	$\{911\}$	6	6	0	5	4	1	**1**	**0**	3
14	226954		$\{2,7,13\}$	$\{29,43\}$	6	12	0	8	1	4	**0**	1	3
15	346710		$\{2,3,5,7\}$	$\{13,127\}$	5	9	0	5	3	4	*2*	1	*5*
16	63870		$\{2,3,5\}$	$\{2129\}$	4	6	0	4	3	2	**1**	**0**	3
17	91358		$\{2,17\}$	$\{2687\}$	3	3	0	2	4	1	**1**	**0**	3
18	339762		$\{2,3,17\}$	$\{3331\}$	4	3	0	1	6	2	*2*	**0**	*6*
19	463638		$\{2,3,19\}$	$\{83\}$	4	3	4	5	2	4	**1**	1	4
20	71630		$\{2,5,19\}$	$\{13,29\}$	4	9	0	5	2	4	**1**	1	4

Table 8 ($n=7$) Descent via $\phi : B_\rho \to B^*_{1-\rho}$ over $K = \mathbf{Q}(\boldsymbol{\mu}_7)$

ρ	N	$\mathcal{A}\!\downarrow$	$\mathcal{B}\!\downarrow$	a	b	c	Ξ	ϕ	$\widehat{\phi}$	r	r^*	R
1	49	$\emptyset$	$\emptyset$	0	0	2	2	1	1	**0**	**0**	**0**
2	49	$\emptyset$	$\emptyset$	0	0	2	2	1	1	**0**	**0**	**0**
3	637	$\emptyset$	$\{13\}$	0	3	0	1	2	2	**1**	**1**	**2**
4	58261	$\{29\}$	$\{41\}$	6	3	2	4	5	2	**1**	**0**	5
5	45227	$\{71\}$	$\{13\}$	6	3	4	7	2	2	1	**1**	2
6	88543	$\{139\}$	$\{13\}$	3	3	2	2	4	4	1	**1**	6
7	3290791	$\{239\}$	$\{281\}$	6	6	2	7	2	2	2	**0**	2
8	7998809	$\{13, 29\}$	$\{433\}$	9	3	2	5	7	1	*2*	**0**	*6*
9	17283721	$\{13, 43\}$	$\{631\}$	9	6	2	8	4	1	1	**0**	3
10	4878097	$\{113\}$	$\{881\}$	6	3	0	2	7	1	2	**0**	6
11	62863619	$\{13, 83\}$	$\{29, 41\}$	6	9	2	5	4	7	1	**2**	9
12	15614683	$\{1429\}$	$\{223\}$	6	3	4	7	2	2	1	1	2
13	181277509	$\{1847\}$	$\{2003\}$	3	6	2	5	1	4	**0**	1	3
14	288934331	$\{2339\}$	$\{2521\}$	6	6	2	7	2	2	**0**	2	2
15	445176319	$\{41, 71\}$	$\{3121\}$	9	3	2	4	8	2	2	2	8
16	666121729	$\{43, 83\}$	$\{13, 293\}$	9	6	2	5	7	4	*2*	1	*9*
17	138799703	$\{617\}$	$\{4591\}$	6	3	0	2	7	1	*2*	**0**	*6*
18	1385670559	$\{5167\}$	$\{13, 421\}$	6	9	2	8	1	4	**0**	**1**	3
5/2	27391	$\{13\}$	$\{43\}$	3	6	2	4	2	5	**2**	**1**	5
7/3	61789	$\{13\}$	$\{97\}$	3	3	2	2	4	4	1	**1**	6
9/4	8869	$\emptyset$	$\{181\}$	0	3	2	2	1	4	**0**	1	3
11/5	61103	$\{29\}$	$\{43\}$	6	6	4	8	1	4	**0**	**1**	3
13/6	1883021	$\{83\}$	$\{463\}$	3	6	2	4	2	5	2	1	5
15/7	5507159	$\{167\}$	$\{673\}$	3	6	2	5	1	4	**0**	1	3
17/8	1882433	$\{41\}$	$\{937\}$	3	3	0	1	5	2	2	**1**	5
19/9	27743261	$\{449\}$	$\{13, 97\}$	6	6	2	5	4	4	1	**1**	6
21/10	53312441	$\{659\}$	$\{13, 127\}$	6	9	2	7	2	5	**0**	**1**	5
23/11	95564651	$\{13, 71\}$	$\{2113\}$	9	3	2	4	8	2	*2*	**0**	*8*
25/12	23158037	$\{29, 43\}$	$\{379\}$	12	6	4	10	5	2	3	**0**	5
27/13	262858001	$\{1637\}$	$\{29, 113\}$	3	12	2	5	1	10	**1**	2	9
29/14	410478341	$\{2099\}$	$\{13, 307\}$	3	6	2	2	4	7	1	*2*	*9*
31/15	88688873	$\{13, 29\}$	$\{4801\}$	9	3	0	2	10	1	3	**0**	9
33/16	913434431	$\{13, 251\}$	$\{29, 197\}$	6	12	2	8	1	7	**0**	*2*	*6*
35/17	1312079909	$\{41, 97\}$	$\{6733\}$	6	3	2	2	7	4	*2*	1	*9*

Table 9 ($n=5$) Descent via $\phi : C_\lambda \to D_\lambda$ over $K = \mathbf{Q}(\boldsymbol{\mu}_5)$

λ	$\eta(\lambda)$	N	#	$\mathcal{B}\downarrow$	b	c	Ξ	ϕ	$\widehat{\phi}$	r	r^*	R
ϕ^{-23}	$377/34$	320450		$\{2,13,17,29\}$	5	2	1	1	5	3	1	4
ϕ^{-21}	$521/47$	612175		$\{47,521\}$	5	0	1	1	4	**0**	1	3
ϕ^{-19}	$144/13$	1950	Y2	$\{2,3,13\}$	3	2	1	1	3	*2*	**0**	*2*
ϕ^{-17}	$199/18$	29850		$\{2,3,199\}$	4	0	1	1	3	**1**	1	2
ϕ^{-15}	11	11	A2	$\{11\}$	4	6	2	0	6	**0**	*2*	*4*
ϕ^{-13}	$76/7$	6650		$\{2,7,19\}$	4	0	1	1	3	**1**	**1**	**2**
ϕ^{-11}	$21/2$	1050	O2	$\{2,3,7\}$	3	2	1	1	3	*2*	**0**	*2*
ϕ^{-9}	$29/3$	2175	J1	$\{3,29\}$	3	0	1	1	2	**0**	**1**	**1**
ϕ^{-7}	8	50	B4	$\{2\}$	1	2	1	1	1	**0**	**0**	**0**
ϕ^{-5}	$11/2$	550	K1	$\{2,11\}$	5	0	2	0	3	**0**	**1**	**1**
ϕ^{-3}	3	75	C2	$\{3\}$	1	2	1	1	1	**0**	**0**	**0**
ϕ^{-1}	$4/3$	150	A1	$\{2,3\}$	2	0	1	1	1	**0**	**0**	**0**
ϕ	-2	50	B3	$\{2\}$	1	2	1	1	1	**0**	**0**	**0**
ϕ^3	-7	175	A1	$\{7\}$	1	0	0	2	1	**1**	**0**	**1**
ϕ^5	$0,\infty$											
ϕ^7	18	150	A2	$\{2,3\}$	2	0	1	1	1	**0**	**0**	**0**
ϕ^9	13	325	E2	$\{13\}$	1	2	1	1	1	**0**	**0**	**0**
ϕ^{11}	$47/4$	2350	N1	$\{2,47\}$	2	0	1	1	1	**0**	**0**	**0**
ϕ^{13}	$34/3$	2550	EE2	$\{2,3,17\}$	3	2	1	1	3	*2*	**0**	*2*
ϕ^{15}	$123/11$	33825		$\{3,11,41\}$	9	0	2	0	7	**1**	*2*	*5*
ϕ^{17}	$89/8$	4450	K2	$\{2,89\}$	3	2	1	1	3	**1**	**1**	**2**
ϕ^{19}	$322/29$	233450		$\{2,7,23,29\}$	5	0	1	1	4	*2*	1	*3*
ϕ^{21}	$233/21$	122325		$\{3,7,233\}$	3	2	1	1	3	*2*	**0**	*2*
ϕ^{23}	$843/76$	800850		$\{2,3,19,281\}$	8	0	1	1	7	*2*	*2*	*6*

Table 10 ($n=7$) Descent via $\phi : C_\lambda \to D_\lambda$ over $K = \mathbf{Q}(\boldsymbol{\mu}_7)$

λ	$\eta(\lambda)$	N	#	$\mathcal{B}\downarrow$	b	c	Ξ	ϕ	$\widehat{\phi}$	r	r^*	R
u_2	-2	294	B1	$\{2,3\}$	3	0	2	1	1	**0**	**0**	**0**
u_{-12}	5	490	K1	$\{2,5\}$	3	0	2	1	1	**0**	**0**	**0**
u_{1262}	$22/3$	61446		$\{2,3,11,19\}$	6	0	2	1	4	*2*	**1**	*3*
u_1	u_1	49	A1	$\emptyset$	0	2	2	1	1	**0**	**0**	**0**
u_{15}	u_{15}	49	A2	$\emptyset$	0	2	2	1	1	**0**	**0**	**0**
u_{-5}	$u_{55/13}$	637	A2	$\{13\}$	3	0	1	2	2	**1**	**1**	**2**
u_{-1259}	$u_{1441/181}$	8869		$\{181\}$	3	2	2	1	4	**0**	1	3

References

[AR] A. Adler and S. Ramanan, *Moduli of Abelian Varieties*, Lect. Notes in Math. **1644** Springer (1996).

[AKMMMP] S.Y. An, S.Y. Kim, D.C. Marshall, S.H. Marshall, W.G. McCallum, A.R. Perlis, Jacobians of Genus One Curves.

[Be] C.D. Beaver, 5-Torsion in the Shafarevich-Tate Group of a Family of Elliptic Curves, *Journal of Number Theory* **82** (2000) 25-46.

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

[BE] D.A. Buchsbaum and D. Eisenbud, Algebra structures for finite free resolutions, and some structure theorems for ideals of codimension 3, *Amer. J. Math.* **99** (1977) 447-485.

[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** (1964), 65-70.

[Ca2] J.W.S. Cassels, *Lectures on Elliptic Curves*, Cambridge (1991).

[Ca3] J.W.S. Cassels, Second descents for elliptic curves, *J. Reine Angew. Math.* **494** (1998) 101-127.

[CF] J.W.S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press (1967).

[CS] J. Coates and R. Sujatha, *Galois Cohomology of Elliptic Curves*, TIFR Lect. on Math. **88** Narosa (2000).

[Coh] H. COHEN, *A Course in Computational Algebraic Number Theory*, Springer GTM **138** (1996).

[Con] I. CONNELL, Calculating Root Numbers of Elliptic Curves over **Q**, *Manuscripta Math.* **82** (1994) 93-104.

[CM] J.E. CREMONA AND B. MAZUR, Visualizing Elements in the Shafarevich-Tate Group, *Experimental Mathematics* **9**:1, (2000) 13-28.

[Cr] J.E. CREMONA, *Algorithms for modular elliptic curves (Second Edition)*, Cambridge (1997). See also "Electronic References".

[DR] P. DELIGNE AND M. RAPOPORT Les schémas de modules de courbes elliptiques *Modular Functions of One Variable II*, P. Deligne and W. Kuyk (eds.), Lect. Notes in Math. **349** Springer (1973) 143-316.

[E] N.D. ELKIES, The Klein Quartic in Number Theory, in [Le] 51-101.

[HR] H. HALBERSTAM AND H.-E. RICHERT, *Sieve Methods*, Academic Press (1974).

[Ha] R. HARTSHORNE, *Algebraic Geometry*, Springer GTM **52** (1977).

[Hu] K. HULEK, *Projective Geometry of Elliptic Curves*, Soc. Math. de France, Astérisque **137** (1986).

[K1] F. KLEIN, Über die Transformation siebenter Ordnung der elliptischen Funktionen *Math. Ann.* **14** (1879) 428-471. English translation in [Le] 287-331.

[K2] F. KLEIN, *Gesammelte Mathematische Abhandlungen, 3: Elliptische Funktionen etc.*, R. Fricke et al (eds.) Springer (1923).

[Ko] V. KOLYVAGIN, Euler Systems, *The Grothendieck Festscrift* vol 2, Progress in Math., Birkhaüser (1990) 435-483.

[Kr] K. KRAMER, A Family of Semistable Elliptic Curves with Large Tate-Shafarevich Groups, *Proc. American Math. Society* **89** (1983) 379-386.

[Le] S. LEVY (ED.), *The Eightfold Way, The Beauty of Klein's Quartic Curve*, MSRI Publications **35** (1999).

[Ma1] B. MAZUR, Arithmetic on Curves, *Bull. American Math. Soc.* **14** (1986) 207-259.

[Ma2] B. MAZUR, On the Passage from Local to Global in Number Theory, *Bull. American Math. Soc.* **29** (1993) 14-50.

[Mc] W.G. MCCALLUM, On the Tate-Shafarevich group of the jacobian of a quotient of the Fermat curve, *Invent. Math.* **93** (1988) 637-666.

[Mi] J.S. MILNE, *Arithmetic Duality Theorems*, Persp. in Math, vol 1, Academic Press (1986).

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

[Mu1] D. MUMFORD, On the Equations Defining Abelian Varieties. I, *Invent. Math.* **1** (1966) 287-354.

[Mu2] D. MUMFORD, *Abelian Varieties*, Oxford (1970).

[Na] T. NAGELL, Sur un type particulier d'unités algébriques, *Arkiv f. Matem* **8** (1969) 163-184.

[Ni] G. NIKLASCH, Counting exceptional units, *Collect. Math.* **48** 1-2 (1997) 195-207.

[O'N] C.H. O'NEIL, *Jacobians of Curves of Genus One*, Harvard PhD thesis (1999).

[Ro] D.E. ROHRLICH, Variation of Root Numbers in Families of Elliptic Curves, *Compositio Mathematica* **87** (1993) 119-151.

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

[Se2] J.-P. SERRE, *Local Fields*, Springer GTM **67** (1979).

[Si1] J.H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Springer GTM **106** (1986).

[Si2] J.H. SILVERMAN, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer GTM **151** (1994).

[Sm] N.P. Smart, *The Algorithmic Resolution of Diophantine Equations*, Cambridge (1998).

[Sw] H.P.F. Swinnerton-Dyer, The solubility of diagonal cubic surfaces. Submitted for publication.

[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** (1974) 179-206.

[V1] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sc. Paris*, **273** (1971) 238-241.

[V2] J. Vélu, Courbes elliptique munies d'un sous-group $\mathbf{Z}/n\mathbf{Z} \times \boldsymbol{\mu}_n$, *Bull. Soc. Math. France*, Mémoire **57** (1978).

[W] L. C. Washington, *Introduction to Cyclotomic Fields (Second Edition)*, Springer GTM **83** (1997).

Electronic References

C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier
`pari/gp` A semi-general computer algebra package, implementing almost all the algorithms presented in [Coh].
`http://www.parigp-home.de`

J.E. Cremona
`mwrank` A program for 2-descent on elliptic curves over $\mathbf{Q}$.
`findinf` Searches for rational points on elliptic curves over $\mathbf{Q}$.
`http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs`

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

Wolfram Research Inc.
`mathematica` A general computer algebra package.
`http://www.wolfram.com`