Construction of infinite families of quadratic number fields with class number divisible by certain primes

Meinte Boersma

Supervisor: Dr. J. Top

RuG

Mathematics

Masters thesis

Construction of infinite families of quadratic number fields with class number divisible by certain primes

Meinte Boersma

Supervisor: Dr. J. Top

Rijksuniversiteit Groningen
Department of Mathematics
Postbus 800
9700 AV Groningen

August 2002

Contents

Chapter 1

Introduction

The notion from algebraic number theory of the *class group* of an algebraic number field is an important one. In (arithmetic) algebraic geometry the class group regularly forms an obstruction to algorithms and explicit methods. The presence of an obstruction often coincides with the divisibility of the *class number* by a certain prime.

1.1 The Cohen-Lenstra heuristic

The only proven general results (e.g. the Brauer-Siegel-theorem) on the behaviour of the class number deal with the size of it. In the 1980's H.W. Lenstra and H. Cohen (in [5]) formulated a conjecture concerning the *arithmetic* structure of the class group and arithmetic behavior of the class number of quadratic number fields, after studying tables. Assuming that class groups of quadratic number fields behave as weighted (by the number of their automorphisms) random abelian groups, they were able to make precise quantitative predictions about arithmetic properties of class numbers and structure of class groups.

We state only part of their conjecture here. If p is an odd prime and D a *fundamental discriminant* (i.e.: D is an integer which is square free, possibly apart from a single factor 4, such that $D \equiv 0$ or $1 \pmod 4$), then the probability that p divides the class number $h(D)$ is equal to

$$1 - (p)_\infty = \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^5} - \dots$$

if $D < 0$ and is equal to

$$1 - \frac{(p)_\infty}{1 - 1/p} = \frac{1}{p^2} + \frac{1}{p^3} + \frac{1}{p^4} - \dots$$

if $D > 0$. Here:

$$(p)_\infty = \prod_{r \geq 1} \left(1 - p^{-r}\right).$$

Note that in the *imaginary* quadratic case, the probability that a small odd prime p divides the class number is substantially greater than the naively expected value $1/p$. On the other hand, the probability that an odd prime p divides the class number of a *real* quadratic number field is substantially smaller than $1/p$. Here is a table for the first few primes:

p	$D<0$	$D>0$	$1/p$
3	0.4399	0.1598	0.3333
5	0.2397	0.04958	0.2000
7	0.1632	0.02374	0.1429

For a finite abelian group G, let $G[p]$ denote the subgroup of elements of order dividing p. The finite field $\mathbb{F}_p$ can be seen to act naturally on $G[p]$. We define the *p-rank of G*, denoted $r_p(G)$, to be the dimension $\dim_{\mathbb{F}_p} G[p]$ of $G[p]$ as a $\mathbb{F}_p$-vector space. Then the class number being divisible by p is the same as the p-rank of the class group being positive.

1.2 History of the problem

Although the Cohen-Lenstra heuristic is widely believed to be true and is supported by much numerical evidence, it seems the conjecture is still out of reach of today's mathematics. It has been generalized to number fields of higher degree.

In the literature many articles can be found in which quadratic number fields are constructed such that the class groups have certain properties. Several of these articles deal with case that the class groups have a certain p-rank or a lower bound for it, with p a small prime.

Sometimes an *infinite* number of quadratic number fields is obtained. See e.g. [3] and also §1.3.1. We also mention the articles of Mestre [11] and Schoof [12] which contain many, if not all, of the ideas used in this thesis.

1.3 Goal of the thesis

The goal of this thesis is to explicitly construct infinitely many (isomorphism classes of) quadratic number fields which have class numbers divisible by certain small, odd primes. Moreover, we'd like such a family to have a fairly nice form. By that we mean that we want it to have the form $\mathbb{Q}(\sqrt{\Delta(t)})$ where $\Delta(t) \in \mathbb{Q}[t]$ is a non-constant polynomial and t comes from some explicitly given infinite set $T \subset \mathbb{Q}$. We are going to be able to do this for the primes 3, 5 and 7. In fact, in all cases we find an infinite number of infinite families.

The prime 2 is not considered for a number of reasons. In the first place, this case is somewhat odd. For example, the precise statement of the Cohen-Lenstra heuristic is more intricate in this case than in the other cases. Secondly, this case has been the subject of a theory which was already (partly) developed by Gauß, called *genus theory*. Thirdly, the details of the construction are slightly different for 2 than for odd primes.

1.3.1 Granville's family

During a lecture, held May 21, 1999 at the University of Leiden, Andrew Granville of the University of Georgia, gave the following example which followed from joint work (which, to date, remains unpublished) of himself with Dinah Kahlil. Let

$$\Delta(t) = 4t^3 + 56t^2 + 220t + 121. \tag{1.1}$$

Then, with $t \in \mathbb{Z}$, $\mathbb{Q}(\sqrt{\Delta(t)})$ is a quadratic number field with class number divisible by 5 whenever each of the following conditions is met:

(*1*) $11 \nmid t$;
(*2*) $\Delta(t)$ is not a perfect square;
(*3*) $\Delta(t)$ is third-power-free.

We actually found this same family and were able to remove the third condition at the same time. Furthermore, it turns out that the second condition is equivalent to $t \neq 0, 11$ which was already precluded by the first condition.

1.4 Outline of the thesis

Chapter 2 rephrases the problem in terms of finding field extensions K/k with certain properties, using some class field theory. It also covers an approach to check certain conditions concerning ramification. Chapter 3 describes the arithmetic algebraic geometric machinery which enables our construction. Chapter 4 then further investigates the arithmetic algebraic geometry coming from the previous chapter locally. Finally, Chapter 5 pieces together the results from the previous chapters to give the general results we set out for. Also, we give several explicit examples of families.

Conclusions and suggestions for future work are to be found in Chapter 6.

Chapter 2

Algebraic results

In this chapter we state and prove several results that are essentially algebraic (number theoretic) in nature. For a compact introduction to algebraic number theory we refer to [15].

2.1 Class field theory

From class field theory we have the following result (see e.g. [15, §17]).

Theorem 2.1.1 (Hilbert class field) *Let k be a number field. Then there is an unique (up to isomorphism) algebraic field extension $\mathcal{H}_k$ of k with the following properties:*

(i) $\mathcal{H}_k$ is Abelian over k with Galois group isomorphic to the class group of k:

$$\mathrm{Gal}(\mathcal{H}_k/k) \cong \mathcal{C}\ell(k);$$

(ii) $\mathcal{H}_k$ is unramified at all finite places of k;

(iii) $\mathcal{H}_k$ is unramified at all infinite places of k as well, i.e.: the places of $\mathcal{H}_k$ above a real place of k are again real.

This extension $\mathcal{H}_k$ is called the Hilbert class field *for k.*

Suppose now that ℓ is a prime number, k is a number field and that we can find a Galois extension K of k with the following properties:

(*i*) $\mathrm{Gal}(K/k)$ is cyclic of order ℓ;
(*ii*) K is unramified at all places of k in the sense of Theorem 2.1.1 (*ii*) and (*iii*).

Then K is an intermediate field of $\mathcal{H}_k/k$. From the Galois correspondence we know that $\mathbb{Z}/\ell\mathbb{Z}$ is a quotient of $\mathrm{Gal}(K/k) \cong \mathcal{C}\ell(k)$, i.e.: there is a subgroup $H \subset \mathcal{C}\ell(k)$ such that $\mathcal{C}\ell(k)/H \cong \mathbb{Z}/\ell\mathbb{Z}$. Counting gives $\#\mathcal{C}\ell(k) = h(k) = \ell \cdot \#H$, hence $\ell \mid h(k)$. This observation was originally made by Kummer during his work on Fermat's Last Theorem. To sum up:

Corollary 2.1.2 *Let K be an Abelian extension of degree ℓ of a number field k such that K is unramified at all places of k (in the sense of Theorem 2.1.1 (ii) and (iii)). Then ℓ divides the class number of k.*

2.1.1 Outline of the construction

In view of Corollary 2.1.2, we can ask for an infinite family of extensions K/k with cyclic Galois group of prime order ℓ and k quadratic such that K/k is unramified at all (finite and infinite) places of k, in order to obtain an infinite family of quadratic number fields with class number divisible by ℓ.

Furthermore, we want that we actually have an infinite number of non-isomorphic k. It turns out that this can be dealt with in a number theoretic manner, because the family is going to be given by means of a polynomial (§5.2).

Notation 2.1.3 For convenience, we will fix the following notation ($m > 1$ is an integer):

C_m	the cyclic group of order m
D_m	the dihedral group with $2m$ elements

2.2 Ramification at infinite places

We have to be able to check whether a Galois extension K of k is unramified at all infinite places of k, in the sense of condition (*iii*) of Theorem 2.1.1. For that we are going to use the following well-known and elementary:

Lemma 2.2.1 *Let $L/\mathbb{Q}$ be Galois. Then L is either totally real (i.e. $\sigma(L) \subset \mathbb{R}$ for all embeddings $\sigma : L \to \mathbb{C}$) or totally complex (i.e. $\sigma(L) \not\subset \mathbb{R}$ for all embeddings σ).*

PROOF. If all embeddings of L are complex, then we are done. So, suppose that at least one embedding is real. Thus we can view L as a subfield of $\mathbb{R}$. Let α_1 be a primitive element of L, i.e., $L = \mathbb{Q}(\alpha_1)$. Let $f(X) \in \mathbb{Q}[X]$ be its minimal polynomial of degree $n = [L : \mathbb{Q}]$ and let $\alpha_2, \ldots, \alpha_n$ be the other roots of f in $\mathbb{C}$. The embeddings of $L \cong \mathbb{Q}[X]/(f(X))$ are generated by the α_i, i.e.: each embedding is the unique field homomorphism generated by $x \mapsto \alpha_i$ where x is the image of X in $\mathbb{Q}[X]/(f(X))$.

Because L is Galois, all conjugates of an element are again in L. In particular: $\alpha_2, \ldots, \alpha_n \in \mathbb{Q}(\alpha_1) \subset \mathbb{R}$, hence all embeddings are real. ⊠

This Lemma allows us to prove:

Corollary 2.2.2 *Let $K/k/\mathbb{Q}$ be a field tower such that $K/\mathbb{Q}$ and $k/\mathbb{Q}$ are both Galois extensions. Then K/k is unramified at all infinite places if K and k are either both (totally) real or both (totally) complex.*

PROOF. We have to check that all infinite places of K lying over real infinite places of k are again real. If k is complex (i.e., it has at least one complex embedding), then by the Lemma it is totally complex thus k has no real infinite places, so that the result is trivial.

If k is real (i.e., it has at least one real embedding), then by the Lemma it is totally real. By hypothesis, the same must then be true for K, i.e.: K is totally real. Hence all infinite places of both k and K are real, therefore K/k is unramified at all infinite places. ⊠

2.3 Ramification at finite places

An obvious manner to say something about ramification is through factorization of minimal polynomials *á la* Dedekind. This is an approach we will investigate in this section to conclude that it doesn't apply as easily as we'd like to. Instead, we turn to a more arithmetic geometrical approach in Chapter 4. However, that approach leaves one problem to be dealt with. It turns out (in proving Theorem 5.1.1) that the approach of this section is quite suitable for resolving that problem satisfactorily.

From algebraic number theory we have the following classical:

Theorem 2.3.1 *Suppose K and k are algebraic number fields (with ring of integers $\mathfrak{O}_K$ and $\mathfrak{o}_k$ respectively) such that K is normal (hence Galois) over k with $G = \mathrm{Gal}(K/k)$. Let $\mathfrak{p}$ be a prime ideal in k and let*

$$\mathfrak{p}\mathfrak{O}_k = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

be its factorization in K.

Then G acts transitively on the $\mathfrak{P}_i$, all the ramification indices e_i have the same value e, all the residual degrees $f_i = [\mathfrak{O}_K/\mathfrak{P}_i : \mathfrak{o}_k/\mathfrak{p}]$ have the same value f and

$$\#G = [K : k] = efg$$

where g is the number of distinct prime factors of $\mathfrak{p}$ in K.

PROOF. See e.g. [15, Theorem 13, p. 26–27]. ⊠

We are going to use this Theorem to try and say something specific about the ramification at finite places. Again, let k be a quadratic number field (which automatically is a Galois extension of $\mathbb{Q}$) and K a Galois extension of it with group $\mathrm{Gal}(K/k) \cong C_\ell$. If the extension $K/\mathbb{Q}$ is Galois as well, then its Galois group is isomorphic to either $C_{2\ell}$ or D_ℓ, depending on whether any automorphism of order 2 commutes with any automorphism of order ℓ, respectively. Note that $2 \mid \#Gal(K/\mathbb{Q})$, so there is at least one automorphism of order 2.

Let $\mathfrak{p}$ be a prime of k lying over the rational prime p and let $\mathfrak{P}$ be a (any) prime of K lying over $\mathfrak{p}$. Applying Theorem 2.3.1 to the normal extensions K/k and $K/\mathbb{Q}$, we see that the ramification index $e(\mathfrak{P}/\mathfrak{p})$ divides ℓ and $e(\mathfrak{P}/p)$ divides 2ℓ.

On the other hand we also have the fixed field $L := K^{\langle\sigma\rangle}$ as an intermediate field of $K/\mathbb{Q}$ where $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is any element of order 2. Let $\mathfrak{p}'$ be the unique prime of L lying under $\mathfrak{P}$, i.e. the prime dividing $\mathfrak{P} \cap L$. From the tower laws for ramification we have:

$$e(\mathfrak{P}/p) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/p) = e(\mathfrak{P}/\mathfrak{p}')e(\mathfrak{p}'/p).$$

We know that $e(\mathfrak{p}/p), e(\mathfrak{P}/\mathfrak{p}') \leq 2$ since the degree of the corresponding extensions is 2. We also know that $e(\mathfrak{P}/\mathfrak{p}) \mid \ell$. Hence, if $e(\mathfrak{p}'/p) < \ell$, then $\ell \nmid e(\mathfrak{P}/\mathfrak{p})$ and hence $\mathfrak{p}$ cannot ramify in K.

In the other direction: if $e(\mathfrak{p}'/p) = \ell$, then ℓ divides $e(\mathfrak{P}/p) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/p)$. The right most factor of this equation has value at most two, so ℓ must divide and subsequently equal $e(\mathfrak{P}/\mathfrak{p})$.

The discussion above proves the following:

Lemma 2.3.2 *Let ℓ be an odd prime. Let k be a quadratic number field and K a cyclic extension of it of degree ℓ such that $K/\mathbb{Q}$ is Galois. Let $L = K^{\langle\sigma\rangle}$ where $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is an element of order 2. Then a prime $\mathfrak{p}$ of k ramifies in K if and only if the rational prime p lying under $\mathfrak{p}$ ramifies completely in L.*

Let θ be a non-rational integral element of L. Since $[L : \mathbb{Q}] = \ell$ is prime, θ generates L: $L = \mathbb{Q}(\theta)$. Hence $L \cong \mathbb{Q}[X]/(\phi(X))$ where $\phi(X)$ is the minimal polynomial of θ over $\mathbb{Q}$. On the other hand, if $\phi(X) \in \mathbb{Z}[X]$ is a monic, irreducible polynomial of degree ℓ, such that K is a splitting field extension over $\mathbb{Q}$ for ϕ, then we can take $L = \mathbb{Q}[X]/(\phi(X))$. Unfortunately, we cannot apply Dedekind's criterion directly to $\phi(X)$ to determine whether the ramification index is equal to ℓ, since *a priori* we don't know whether p doesn't divide the *index* $[\mathfrak{O}_L : \mathbb{Z}[\theta]]$ of θ. However, we do not need the full strength of Dedekind's criterion. All we need to do is ascertain that the ramification index $e(\mathfrak{p}'/p) < \ell$.

Therefore, it is enough to ask for a *necessary* condition on $\phi(X)$ for $e(\mathfrak{P}/p)$ to be divisible by ℓ which is implied by $e(\mathfrak{p}'/p) = \ell$, by virtue of Lemma 2.3.2. We can use the following Lemma (which is a Dedekind-like criterion) to derive such a condition.

Lemma 2.3.3 *Let $L = \mathbb{Q}(\theta)$ be a number field with θ an algebraic integer. Let $\phi(X)$ be the minimal polynomial of θ. Let p be a rational prime. Suppose $\phi(X)$ factors modulo p as*

$$\phi(X) \equiv \prod_{i=1}^{g} (\phi_i(X))^{e_i} \pmod{p} \tag{2.1}$$

where the $\phi_i(X) \bmod p$ are pairwise distinct, monic and irreducible polynomials of degree $n_i > 0$. Let $\mathfrak{O}_L$ be the ring of integers of L. Then we have that

$$p\mathfrak{O}_L = \prod_{i=1}^{g} \mathfrak{a}_i \tag{2.2}$$

where the $\mathfrak{a}_i$ are pairwise coprime ideals in $\mathfrak{O}_L$ with the property that all prime ideals dividing $\mathfrak{a}_i$ have residual degree divisible by n_i.

PROOF. Proposition 6.2.1 or Exercise 5 of [4, §6.2]. ⊠

Proposition 2.3.4 *Let ℓ be an odd prime. Let $\phi(X) \in \mathbb{Z}[X]$ be monic, irreducible and of degree ℓ. Let $L = \mathbb{Q}[X]/(\phi(X))$. Let p be a rational prime and $\mathfrak{p}$ a prime of L lying over p. If $e(\mathfrak{p}/p) = \ell$, i.e., p ramifies completely in L, then $\phi(X)$ factors modulo p as*

$$\phi(X) \equiv (X + c)^{\ell} \pmod{p} \tag{2.3}$$

for some $c \in \mathbb{F}_p$.

PROOF. Suppose that p ramifies completely in L. Then there is precisely one prime $\mathfrak{p}$ of L lying over p and it necessarily has residual degree 1. Since the $\mathfrak{a}_i$ in Lemma 2.3.3 are to be coprime, we must have $g = 1$ in (2.2). Since $\mathfrak{p}$ is of degree 1 and n_1 divides the degrees of all prime ideals dividing $\mathfrak{a}_1$, necessarily: $n_1 = 1$. Comparing degrees then gives $e_1 = \ell$. Therefore $\phi(X)$ factors modulo p as stated. ⊠

Hence the condition that $\phi(X)$ doesn't factor modulo p as (2.3) is *sufficient* for p not to be completely ramified in L, hence sufficient for primes $\mathfrak{p}$ of k lying over p not to ramify in K. The reverse of Proposition 2.3.4 is not true. Keeping the general construction in mind, this might mean that we throw away too many examples, but as long as we are left with a sufficiently large family, we don't mind too much.

Suppose that K is given as the splitting field over $\mathbb{Q}$ of an irreducible polynomial $\phi(X) = X^\ell + a_{\ell-1}X^{\ell-1} + \cdots + a_0 \in \mathbb{Z}[X]$ (which will be the case in later Chapters). Then in order to use Proposition 2.3.4 to avoid ramification in K/k, we would have to check whether (2.3) holds for any prime p. This amounts to solving the following system of equations:

$$\binom{\ell}{i} c^{\ell-i} \equiv a_i \pmod{p}, \quad i = 1, \ldots, \ell - 1.$$

Not only is this quite difficult to do (certainly when $\phi(X)$ varies over an infinite family), there is an alternative route (explained in Chapter 4), specific to the construction in Chapter 3, to treat all primes $p \neq \ell$. The case $p = \ell$ can be treated by means of Proposition 2.3.4 since then (2.3) reduces to

$$\phi(X) \equiv X^\ell + c \pmod{\ell} \tag{2.4}$$

for some $c \in \mathbb{F}_\ell$.

Chapter 3

Isogenies of prime degree

It is not trivial to construct infinitely many (non-isomorphic) Galois extensions K/k of algebraic number fields such that the Galois group is cyclic of prime order ℓ for every extension. Sometimes such extensions K/k can be realized as specializations of (Galois) coverings of curves. This is precisely what we are going to do here using *elliptic curves*. A thorough introduction to the theory of elliptic curves can be found in [14] of which especially Chapters III, IV and VII are especially relevant here.

3.1 The construction using elliptic curves

Suppose E is an elliptic curve defined over $\mathbb{Q}$ with a finite, rational subgroup Φ, i.e.: if $T \in \Phi$, then $T^\sigma \in \Phi$ for all $\sigma \in \mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then there is a unique (up to isomorphism) elliptic curve $E'/\mathbb{Q}$ and a separable isogeny $\varphi : E \longrightarrow E'$ which is defined over $\mathbb{Q}$ as well such that $\ker\varphi = \Phi$, cf. [14, Prop. 4.12, Remark 4.13.2, p. 78]. This isogeny can be seen as "dividing the group E out by the finite subgroup Φ".

We can assume that E and E' are both given by Weierstraß equations:

$$E/\mathbb{Q}: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.1}$$

$$E'/\mathbb{Q}: \quad y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6. \tag{3.2}$$

For our purposes we require Φ to be generated by a rational point T of order ℓ, so Φ certainly is finite and rational. Let $t \in \mathbb{Q}$. Then there is either one point on E' with x-coordinate equal to t or two points which are opposite of each other (for the group law). More precisely: let be $P = (t, s)$ be such a point, then by completing the square in (3.2) and multiplying by 4, we see that s satisfies the following equation:

$$\left(2s + (a'_1t + a'_3)\right)^2 = 4t^3 + b'_2t^2 + 2b'_4t + b'_6, \tag{3.3}$$

where

$$\begin{aligned} b'_2 &= (a'_1)^2 + 4a'_2, \\ b'_4 &= a'_1a'_3 + 2a'_4, \\ b'_6 &= (a'_3)^2 + 4a'_6, \end{aligned} \tag{3.4}$$

are standard quantities associated to E' (cf. [14, p. 46]). The case that s is rational is not interesting, so we assume that s is quadratic, which is equivalent to: $(t, s) \notin E'(\mathbb{Q})$.

Let $k = \mathbb{Q}(P)$ be the *field of definition* of the point P, i.e., the extension of $\mathbb{Q}$ generated by the coordinates of P. By assumption it is the quadratic number field $\mathbb{Q}(s)$. The preimage of P under φ is non-empty since φ is a morphism of algebraic curves and therefore surjective when considered as a map from $E(\overline{\mathbb{Q}})$ to $E'(\overline{\mathbb{Q}})$. Let $Q \in E(\overline{\mathbb{Q}})$ be any point in that preimage and let $K = \mathbb{Q}(Q)$ be the field of definition of that point. It is a finite extension of $\mathbb{Q}(P)$, since $Q \in E(\overline{\mathbb{Q}})$ and φ is defined over $\mathbb{Q}(P) \supset \mathbb{Q}$.

The field K is independent from the choice of Q, since for any other Q' in the preimage of P we have that $Q - Q' = T \in \ker\varphi$. Because T is a rational point and the group law on E is defined over $\mathbb{Q}$, we have that $\mathbb{Q}(Q) = \mathbb{Q}(Q' + T)$. Hence $\mathbb{Q}(\varphi^{-1}(P)) = \mathbb{Q}(Q)$.

We summarize the above in the following:

Theorem 3.1.1 *Let $E/\mathbb{Q}$ be an elliptic curve with a rational point T of prime order ℓ.*

(a) There is a unique (up to isomorphism) elliptic curve $E'/\mathbb{Q}$ and a separable, unramified isogeny $\varphi : E \longrightarrow E'$ of degree ℓ, which is also defined over $\mathbb{Q}$, such that $\ker\varphi = \Phi := \langle T \rangle$.

(b) Let $t \in \mathbb{Q}$ and let $P = (t, s)$ be a point of E'. The field $\mathbb{Q}(P)$ is a quadratic number field precisely if $P \notin E'(\mathbb{Q})$.

(c) $\mathbb{Q}(\varphi^{-1}(P))$ is a finite extension of $\mathbb{Q}(P)$ and $\mathbb{Q}(\varphi^{-1}(P)) = \mathbb{Q}(Q)$ for any $Q \in \varphi^{-1}(P)$.

PROOF. We already proved everything except for *(a)*. The proof consists of that of [14, Prop. 4.12] with all occurrences of $\overline{K}$ replaced by $\mathbb{Q}$. Note that one has to use the full statement of [14, Thm. II.2.4 (c), p. 25], not only the reference to Hartshorne which treats only the algebraically closed situation. ⊠

Remark 3.1.2 It is not true that the extension K/k obtained in this manner, is automatically cyclic of order ℓ. We return to this matter in §3.1.2.

The purpose of this approach is that we would like to use the theory of elliptic curves to derive conditions on P to ensure that the extension $\mathbb{Q}(\varphi^{-1}(P))/\mathbb{Q}(P)$ is unramified. This is precisely what we are going to do in Chapter 4.

3.1.1 Function fields

Next, we are going to prove some properties of the isogeny φ which we will use in §3.1.2.

Proposition 3.1.3 *Let E be an elliptic curve defined over $\mathbb{Q}$, given by a Weierstraß equation (3.1). Let $\mathbb{Q}(E)$ be the function field of $E/\mathbb{Q}$. Then:*

(a) any $f \in \mathbb{Q}(E)$ can be written in the form

$$f = \frac{g_1 + yg_2}{h}$$

with $g_1, g_2, h \in \mathbb{Q}[x]$ and $h \neq 0$;

(b) $f \in \mathbb{Q}(E)$ is even *(i.e. $f(P) = f([-1]P)$ for all $P \in E$) if and only if $f \in \mathbb{Q}(x)$.*

PROOF.

(a) The function field $\mathbb{Q}(E)$ is equal to $\mathbb{Q}(x)[Y]/(F(x,Y))$ with $F(x,Y) = Y^2 + a_1xY + a_3Y - (x^3 + a_2x^2 + a_4x + a_6)$, hence we can any write $f \in \mathbb{Q}(E)$ as $f_1 + yf_2$ with $f_1, f_2 \in \mathbb{Q}(x)$. Clearing denominator gives the result.

(b) Consider the automorphism $[-1]^*$ of $\mathbb{Q}(E)$ induced by the group automorphism $[-1]$ on E. It is completely determined by

$$[-1]^*x = x,$$
$$[-1]^*y = -y - a_1x - a_3.$$

If we consider $\mathbb{Q}(E)$ as a $\mathbb{Q}(x)$-linear space, then it is clear that $[-1]^*$ is $\mathbb{Q}(x)$-linear and has matrix

$$\begin{pmatrix} 1 & -(a_1x + a_3) \\ 0 & -1 \end{pmatrix}$$

with respect to the basis 1, y of $\mathbb{Q}(E)$. A function $f \in \mathbb{Q}(E)$ is even precisely if $[-1]^*f = f$, thus if and only f is in the $[-1]^*$-invariant subspace. From the matrix it is clear that $\mathbb{Q}(E)$ has only $\mathbb{Q}(x)$ itself as $[-1]^*$-invariant subspace.

⊠

The above proposition allows us to prove the following:

Theorem 3.1.4 *Let hypotheses and notation be as in Theorem 3.1.1. Then the isogeny φ can be written as a rational map $(\psi(x,y), \xi(x,y))$ where $\psi, \xi \in \mathbb{Q}(E)$ with the following properties:*

(i) the denominator of ψ is (up to a constant factor) the square of the polynomial

$$\prod_{\alpha \in x(\Phi \setminus \{O\})} (x - \alpha) \tag{3.5}$$

of degree $(\ell - 1)/2$ and the denominator of ξ is the third power of that polynomial;

(ii) the numerator of ψ is (up to constant factor) a polynomial in x of degree ℓ which has none of the points $P \in \Phi \setminus \{O\}$ as zeroes;

(iii) the numerator of ξ is a polynomial in which y appears with non-zero coefficient.

PROOF. For an arbitrary elliptic curve F given by a Weierstraß equation, let $\pi : F \longrightarrow \mathbb{P}^1$ be the 2 : 1-morphism defined by $\pi(x,y) = x$.

Let $O \neq P \in E$, then there is at most one other point on E with the same x-coordinate as P and it is the opposite $[-1]P$ of it. So $\pi \circ \varphi(P) = \pi \circ \varphi([-1]P)$, therefore $\pi \circ \varphi = \psi(x,y)$ is an even function. From Proposition 3.1.3 (c): $\psi \in \mathbb{Q}(x)$.

We now have the following commutative diagram:

$$\begin{array}{ccc} E & \xrightarrow[\ell:1]{\varphi=(\psi,\xi)} & E' \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \mathbb{P}^1 & \xrightarrow{\psi} & \mathbb{P}^1 \end{array}$$

Comparing degrees of maps gives that ψ is a ℓ : 1-map. Hence the maximum of the degrees of the numerator and denominator of ψ is ℓ.

Since E is a smooth curve we have for every $Q \in E(\overline{\mathbb{Q}})$ a discrete valuation ord_Q on the local ring $\overline{\mathbb{Q}}[E]_P$ (cf. [14, Proposition 1.1 and Definition, p. 21–22]) which extends canonically to the function field $\overline{\mathbb{Q}}(E)$. This valuation satisfies the *ultrametric law*

$$\mathrm{ord}_Q(f_1 + f_2) \geq \min(\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2)), \quad f_1, f_2 \in \overline{\mathbb{Q}}(E) \setminus \{0\}$$

with equality if $\mathrm{ord}_Q(f_1) \neq \mathrm{ord}_Q(f_2)$. Naturally: $\mathrm{ord}_Q(a) = 0$ for any $a \in \overline{\mathbb{Q}} \setminus \{0\}$ and $\mathrm{ord}_Q(0) = \infty$.

First, suppose that $Q \in E(\overline{\mathbb{Q}})$ is a pole of ψ, i.e. $n := \mathrm{ord}_Q(\psi) < 0$ and that $\mathrm{ord}_Q(\xi) \geq n$. Let t_Q be a uniformizer for Q. Since φ is a morphism, we can evaluate φ at Q by using homogeneous coordinates:

$$\varphi(Q) = (t_Q^{-n}\psi : t_Q^{-n}\xi : t_Q^{-n})(Q).$$

If $\mathrm{ord}_Q(\xi) \geq n$, then $\varphi(Q) = (* : 0 : 0)$ which is not on E' in any case. Hence: if $\mathrm{ord}_Q(\psi) < 0$, then $\mathrm{ord}_Q(\xi) \leq \mathrm{ord}_Q(\psi)$.

Now, φ is a rational map from E to E', so the following is an identity in the function field $\overline{\mathbb{Q}}(E)$:

$$\xi^2 + a_1'\psi\xi + a_3'\xi = \psi^3 + a_2'\psi^2 + a_4'\psi + a_6'. \tag{3.6}$$

Let Q be a pole of ξ. Note that then $\mathrm{ord}_Q(\psi) > \mathrm{ord}_Q(\xi)$. This implies that:

$$\mathrm{ord}_Q(\xi^2) = 2\,\mathrm{ord}_Q(\xi) < \mathrm{ord}_Q(a_1'\psi\xi) = \mathrm{ord}_Q(\psi) + \mathrm{ord}_Q(\xi) < \mathrm{ord}_Q(a_3'\xi).$$

From this we see that the valuation at Q of the left hand side of (3.6) equals $2\,\mathrm{ord}_Q(\xi) < 0$. Hence the valuation of the right hand side of (3.6) must be negative as well and then $\mathrm{ord}_Q(\psi^3 + a_2'\psi^2 + a_4'\psi + a_6') = 3\,\mathrm{ord}_Q(\psi)$. Now, $2\,\mathrm{ord}_Q(\xi) = 3\,\mathrm{ord}_Q(\psi) < 0$, hence a positive integer r exist such that:

$$\mathrm{ord}_Q(\psi) = -2r \quad \text{and} \quad \mathrm{ord}_Q(\xi) = -3r. \tag{3.7}$$

Evaluating φ at Q gives:

$$\varphi(Q) = (t_Q^{3r}\psi : t_Q^{3r}\xi : t_Q^{3r})(Q) = (0 : 1 : 0) = O \iff Q \in \ker\varphi.$$

If, however, Q is not a pole of ξ, then Q isn't a pole of ψ either and we can simply evaluate $\varphi(Q) = (\psi(P), \xi(P)) \neq O \Leftrightarrow Q \notin \ker\varphi$. Hence: the poles of ψ, ξ are exactly the points in the kernel Φ of φ and subsequently $\mathrm{numer}(\psi)$ has none of the kernel points as zero.

Further: $\ell \geq \deg\mathrm{numer}(\psi) > \deg\mathrm{denom}(\psi)$ since otherwise $\mathrm{ord}_O(\psi) = -\deg\mathrm{numer}(\psi) + \deg\mathrm{denom}(\psi) \geq 0$, which is impossible since O is a pole of ψ. But $\mathrm{denom}(\psi)$ is divisible by the following polynomial of degree $\ell - 1$

$$\prod_{P \in \Phi \setminus \{O\}} (x - x(P))$$

which is a square since $P \neq [-1]P$ for all non-zero P in the kernel. Hence, up to a constant factor, $\mathrm{denom}(\psi)$ is the square of (3.5). Together with (3.7) with $r = 1$ this immediately implies that, again up to a constant factor, $\mathrm{denominator}(\xi)$ is the third power of (3.5). This gives *(i)*.

Since the maximum of the degrees of the numerator and denominator equals ℓ and $\deg\mathrm{denom}(\psi) < \deg\mathrm{numer}(\psi)$, we must have that $\deg\mathrm{numer}(\psi) = \ell$. This gives *(ii)*.

Finally, it is clear that $\xi(x, y)$ is not an even function and since its denominator equals (3.5) up to a constant factor, the numerator of ξ must be strictly linear in y. This gives *(iii)*. ⊠

3.1.2 The field tower $\mathbb{Q}(\varphi^{-1}(P))/\mathbb{Q}(P)/\mathbb{Q}$

Proposition 3.1.5 *Let hypotheses and notation be as in Theorem 3.1.1. If $P \notin E'[2]$, then:*

$$\mathbb{Q}(\varphi^{-1}(P)) = (\mathbb{Q}(P))(x(Q)) \quad \textit{for any} \quad Q \in \varphi^{-1}(P).$$

PROOF. In view of Theorem 3.1.1 *(c)* it suffices to show that $\mathbb{Q}(Q) = \mathbb{Q}(x(Q))$ for any $Q \in \varphi^{-1}(P)$. Recall from Proposition 3.1.3 that $\varphi(x,y) = (\psi(x,y), \xi(x,y))$ (as a rational map) where $\xi(x,y)$ can be written as

$$\frac{f_1 + yf_2}{g^3}$$

with $f_1, f_2, g \in \mathbb{Q}[x]$ such that $f_2, g \neq 0$. Evaluating at Q and equating with s, the y-coordinate of P, gives:

$$y(Q) = \frac{s \cdot g(x(Q))^3 - f_1(x(Q))}{f_2(x(Q))}$$

so that $y \in \mathbb{Q}(s, x(Q)) = (\mathbb{Q}(P))(x(Q))$.

This goes awry only if $f_2(x(Q)) = 0$. But that would imply that $\varphi(Q) = \varphi([-1]Q) \Longleftrightarrow \varphi([2]Q) = [2]\varphi(Q) = [2]P = O$, contradicting the hypotheses. ⊠

Remark 3.1.6 Note that if $P = (t,s) \in E'[2]$ with $t \in \mathbb{Q}$, then $[-1]P = P \Longleftrightarrow (t, -s - a_1t - a_3) = (t,s) \Longleftrightarrow 2s + a_1t + a_3 = 0$ hence s is rational a well. Hence:

$$P = (t,s) \in E'[2] \text{ with } t \in \mathbb{Q} \Longrightarrow P \in E'(\mathbb{Q}).$$

Lemma 3.1.7 *Let hypotheses and notation be as in Theorem 3.1.1. Let ψ be the function field element from Theorem 3.1.4 and define*

$$\lambda_t := \text{numerator}(\psi) - t \cdot \text{denominator}(\psi) \in \mathbb{Q}[x]$$

where numerator(ψ) *is taken to be monic. Then λ_t is monic. If $P \notin E'[2]$ and λ_t is irreducible over $\mathbb{Q}$, then*

- *the extension $\mathbb{Q}(\varphi^{-1}(P))/\mathbb{Q}(P)$ is cyclic of order ℓ;*
- *the extension $\mathbb{Q}(\varphi^{-1}(P))/\mathbb{Q}$ is Galois as well.*

PROOF. Let $Q \in \varphi^{-1}(P)$ be arbitrary.

$$\boxed{\mathbb{Q}(Q) \text{ is a splitting field for } \lambda_t \text{ over } \mathbb{Q}(P)}$$

From Theorem 3.1.4 (a) and (b) we know that $\deg \text{numer}(\psi) = \ell$ and $\deg \text{denom}(\psi) = \ell - 1$, so λ_t is monic (by choice of numer(ψ)) and of degree ℓ. By clearing the denominator of the left hand side of the equality $\psi(x(Q)) = t$, we see that $x(Q)$ is a zero of λ_t, which is a polynomial in x with rational coefficients since $\psi \in \mathbb{Q}(x)$. The preimage $\varphi^{-1}(P)$ equals $\{Q + [i]T \mid 0 \leq 0 < \ell\}$ where $\Phi = \langle T \rangle$. So, if $x(\varphi^{-1}(P))$ contains precisely ℓ elements, then λ_t splits completely over $\mathbb{Q}(Q)$.

We know that two points on E have the same x-coordinate if and only if they are equal or opposites of each other. This leads us to consider the equation $x(Q) = x(Q + [i]T) \Longleftrightarrow Q = [\pm 1](Q + [i]T)$ with $0 < i < \ell$. For the plus-sign this reduces to $O = [i]T$ which is never satisfied with $0 < i < \ell$ because T has order ℓ. For the minus-sign, the equation reduces to $[2]Q = [i]T$. Applying φ to both sides of the equation then gives $[2]P = O$, which contradicts the first hypothesis.

$$\boxed{\mathbb{Q}(Q)/\mathbb{Q}(P) \text{ is cyclic of order } \ell \text{ iff } \lambda_t \text{ is irreducible over } \mathbb{Q}(P)}$$

Since $\mathbb{Q}(Q)/\mathbb{Q}(P)$ is a splitting field extension for λ_t and λ_t has precisely as many distinct zeroes as its degree, we see that $\mathbb{Q}(Q)/\mathbb{Q}(P)$ is a Galois extension, thus: $\#\operatorname{Gal}(\mathbb{Q}(Q)/\mathbb{Q}(P)) = [\mathbb{Q}(Q) : \mathbb{Q}(P)]$. If λ_t is irreducible in $(\mathbb{Q}(P))[x]$, then $\mathbb{Q}(Q) \cong (\mathbb{Q}(P))[x]/(\lambda_t(x))$ and $[\mathbb{Q}(Q) : \mathbb{Q}(P)] = \ell$, hence $\operatorname{Gal}(\mathbb{Q}(Q)/\mathbb{Q}(P))$ is cyclic of order ℓ.

On the other hand, if $\operatorname{Gal}(\mathbb{Q}(Q)/\mathbb{Q}(P)) \cong C_\ell$ then $\mathbb{Q}(Q)/\mathbb{Q}(P)$ has no intermediate fields. But any non-trivial factor of λ_t in $(\mathbb{Q}(P))[x]$ gives rise to an intermediate field of degree between 1 and ℓ. Hence λ_t is irreducible in $\mathbb{Q}[x]$.

$$\boxed{\lambda_t \text{ irreducible in } \mathbb{Q}[x] \iff \lambda_t \text{ irreducible over } \mathbb{Q}(P)}$$

If $\lambda_t \in \mathbb{Q}[x]$ is reducible over $\mathbb{Q}$, then it certainly is reducible over $\mathbb{Q}(P)$. For the other direction, suppose that λ_t is reducible in $(\mathbb{Q}(P))[x]$ by writing

$$\lambda_t = \prod_{i=1}^{n} f_i^{n_i}$$

where the $f_i \in (\mathbb{Q}(P))[x]$ are distinct, irreducible polynomials and n_i are positive integers. Let σ be the non-trivial element of $\operatorname{Gal}(\mathbb{Q}(P)/\mathbb{Q})$, which acts trivially on $\lambda_t \in \mathbb{Q}[x]$, hence

$$\prod_{i=1}^{n} f_i^{n_i} = \prod_{i=1}^{n} (f_i^\sigma)^{n_i}.$$

From this we see that σ induces a permutation τ of $\{1, \ldots, n\}$, given by $f_i^\sigma = f_{\tau(i)}$. Now consider the following decomposition:

$$\lambda_t = \left(\prod_{i\,:\, f_i^\sigma = f_i} f_i^{n_i} \right) \left(\prod_{i\,:\, f_i^\sigma \neq f_i} f_i^{n_i} \right). \tag{3.8}$$

Both the left hand side and the first factor of right hand side are left invariant by σ, so the second factor on the right must be σ-invariant as well. Also, since σ has order 2, the permutation τ must have order 1 or 2. Hence the second factor of the right hand side of (3.8) is of even degree (note that necessarily $\deg f_{\tau(i)} = \deg f_i$ and $n_{\tau(i)} = n_i$ for all $i = 1, \ldots, n$). The degree of λ_t is ℓ which is odd, so the factor $\prod_{i\,:\, f_i^\sigma = f_i} f_i^{n_i}$ is non-constant. It cannot be equal to λ_t itself, since that would contradict the assumption that λ_t factors over $\mathbb{Q}(P)$. So λ_t factors over $\mathbb{Q}$. Hence: if λ_t is irreducible over $\mathbb{Q}$, then it is irreducible in $(\mathbb{Q}(P))[x]$.

$$\boxed{\mathbb{Q}(\varphi^{-1}(P))/\mathbb{Q} \text{ is Galois}}$$

We already proved that $\mathbb{Q}(\varphi^{-1}(P))$ is a splitting field over $\mathbb{Q}(P)$ for the separable polynomial λ_t. Since λ_t has all its coefficients in $\mathbb{Q}$, $\mathbb{Q}(\varphi^{-1}(P))$ is also a splitting field for λ_t over $\mathbb{Q}$. Hence $\mathbb{Q}(\varphi^{-1}(P))/\mathbb{Q}$ is Galois as well.

⊠

Hilbert's irreducibility theorem (see e.g. [7, Chapter 9, p. 225–]) says that, provided that λ_t is irreducible in $\mathbb{Q}[x,t]$, "for almost all" rational values of t the corresponding extension $\mathbb{Q}(Q)/\mathbb{Q}(P)$ will be a Galois extension with the same group as the Galois extension $\mathbb{Q}(E)/\mathbb{Q}(E') \cong C_\ell$. Combining this with the results in §4.3, it is thus likely that this strategy will produce many quadratic number fields with class number divisible by ℓ.

3.2 Rational isogenies of prime degree

The results in the previous section lead us to classify elliptic curves $E/\mathbb{Q}$ with a rational point of finite order. This was done in 1977 by Mazur, see e.g. [10].

Notation 3.2.1 Throughout this section (§3.2), K is an *arbitrary* number field.

3.2.1 The modular curves $X_0(\ell)$, $X_1(\ell)$

Let $\ell \geq 2$ be a (any) prime number. It turns out that the pairs (E, G) where E is an elliptic curve over $\mathbb{C}$ and G is subgroup of E of order ℓ are parametrized (modulo ($\mathbb{C}$-)isomorphism) by certain smooth projective curves $X_0(\ell)/\mathbb{Q}$, $X_1(\ell)/\mathbb{Q}$ in the following manner (see [13, §6.7]):

1. Every point $\tau \in X_0(\ell)(K)$, not a cusp, gives an elliptic curve E_τ/K and a subgroup of $E_\tau(\overline{K})$ of order ℓ which is invariant under the action of $G_K = \mathrm{Gal}(\overline{K}/K)$.

2. Every point $\tau \in X_1(\ell)(K)$, not a cusp, gives an elliptic curve E_τ/K and a point $P \in E_\tau(K)$ of (exact) order ℓ.

(For our purposes, it is not necessary to know what it means for a point of $X_i(\ell)$, $i = 0, 1$ to be a cusp.)

The structure of $X_0(\ell)(\mathbb{Q})$ has been determined completely and is given by the following table (see e.g. [10]) in which g is the genus of $X_0(p)$ and ν is the number of non-cuspidal points of $X_0(\ell)(\mathbb{Q})$.

ℓ	g	ν	ℓ	g	ν
≤ 10	0	∞	37	2	2
11	1	3	43	3	1
13	0	∞	67	5	1
17	1	2	163	13	1
19	1	1			

Moreover, the j-invariants of the elliptic curves corresponding to non-cuspidal points of $X_0(\ell)(\mathbb{Q})$ for the cases where $g > 0$ are known. Finally, it is not very difficult to show that the genus of $X_1(\ell)$ is 0 precisely if ℓ is equal to 2, 3, 5 or 7 and contains infinitely many non-cuspidal rational points. Therefore, only in these cases will we be able to find families of elliptic curves having a rational point of prime order ℓ.

For a thorough introduction and proofs to this, we refer to [13].

3.2.2 Points of order 3, 5 or 7

Since $X_1(\ell)$ is isomorphic over $\mathbb{Q}$ to $\mathbb{P}^1$ (for ℓ prime) precisely when $\ell = 2, 3, 5$ or 7, we should be able to produce pairs (E, E') by constructing elliptic curves E over $\mathbb{Q}$ with a subgroup of rational points of order ℓ and subsequently dividing out E by that subgroup to obtain E'. For our purposes, it is only necessary to do this for $\ell \neq 2$. The following is adapted from [8, §1.2], but see also [9].

Proposition 3.2.2 *Let E/K be an elliptic curve with a point $P \in E(K)$ of order $l = 3$, 5 or 7. Then E is isomorphic over K to an elliptic curve E_ℓ in Table 3.1 with parameter(s) lying in K such that $\Delta(E_\ell) \neq 0$ (see Table 3.2 for the discriminants). The isomorphism is such that P on the original curve corresponds to $(0, 0)$ on the isomorphic curve.*

PROOF. We can suppose that E/K is given by a Weierstraß equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.9}$$

This equation is unique (over K) up to transformations (which are isomorphisms over K) of the form

$$\begin{aligned} x &= u^2x' + r, \\ y &= u^3y' + u^2sx' + t, \end{aligned}$$

with $u, r, s, t \in K$, $u \neq 0$.

First, we translate the point $P \in \mathbb{A}^2_K$ to $(0,0)$ by the transformation with $(r,s,t,u) = (a,0,b,1)$. From (3.9) we see that $a_6 = 0$.

If $a_3 = 0$, then $-(0,0) = (0,0)$, hence $(0,0)$ would be a point of order 2. Since $[2]P \neq O$, we see that $a_3 \neq 0$.

Secondly, we apply the transformation with $(r,s,t,u) = (0, a_4/a_3, 0, 1)$. From [14, Table 1.2, p. 49] we see that $a_6' = 0$, $a_3' \neq 0$, so these assumptions continue to hold. Furthermore, $a_4' = a_4 - a_4 = 0$, so the equation is now reduced to the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2$.

Suppose P has order 3: $[3]P = (0,0)$. This is equivalent to: $[-1](0,0) = [2](0,0) \iff (0,-a_3) = (-a_2, a_1a_2 - a_3) \iff a_2 = 0$. So $(0,0)$ has order 3 if and only if $a_2 = 0$. Relabeling $a_1 = w$, $a_3 = v$ then accounts for the E_3-entry in Table 3.1.

Now we suppose that the order of P exceeds 3, thus $a_2 \neq 0$. Then applying the transformation with $(r,s,t,u) = (0,0,0,a_3/a_2)$ yields an equation with $a_2' = a_3'$. After relabeling $a_1 = w$ and $a_2 = a_3 = w$, we can suppose that E can be given by a Weierstraß equation of the form:

$$y^2 + wxy + vy = x^3 + vx^2, \quad w, v \in K. \tag{3.10}$$

All the isomorphisms were defined over K and the point P landed after one transformation in $(0,0)$ and remained there under the subsequent transformations. From now on we assume E is given by an equation (3.10) and that $P = (0,0)$.

Since P has order greater than 2, there is precisely one other point with the same x-coordinate and that point is $[-1]P$. In other words:

$$P = [\pm 1]Q \iff x(P) = x(Q). \tag{3.11}$$

Since P is a point of order ℓ:

$$[\ell]P = \left[\frac{\ell-1}{2} + \frac{\ell+1}{2}\right]P = O \iff \left[\frac{\ell-1}{2}\right]P = \left[-\frac{\ell+1}{2}\right]P$$

$$\overset{(3.11)}{\iff} x\left(\left[\frac{\ell-1}{2}\right]P\right) = x\left(\left[\frac{\ell+1}{2}\right]P\right).$$

We compute the orbit of P up to the $(7+1)/2 = 4$-th multiple:

$$\begin{aligned}
[2]P &= (-v, v(w-1)),\\
[3]P &= (1-w, w-v-1),\\
[4]P &= \left(\frac{v(1+v-w)}{(w-1)^2}, \frac{-v^2(w^2-3w+v+2)}{(w-1)^3}\right).
\end{aligned}$$

(The formula for $[4]P$ is only correct if $w \neq 1$ which is thus equivalent to P not having order 4.)

Now suppose that P has order 5. Then:

$$x([2]P) = x([3]P) \iff (-v, v(w-1)) = (1-w, w-v-1) \iff w = v+1$$

so after relabeling v as d, we get the equation for E_5 in Table 3.1.

Finally, suppose that P has order 7. Note that $w \neq 1$, since otherwise P would have order 4 instead of 7. Thus:

$$x([3]P) = x([4]P) \iff 1-w = \frac{v(1+v-w)}{(w-1)^2} \iff v^2 + (1-w)v + (w-1)^3 = 0.$$

If we regard this as an equation in v, then it has as solutions:

$$v = (w-1)\frac{1 \pm \sqrt{5-4w}}{2}.$$

Since $v, w \in K$, we must require $d := (1 \pm \sqrt{5-4w})/2$ to lie in K as well. Thus:

$$4d^2 - 4d + 1 = 5 - 4w \iff w = -d^2 + d + 1$$

and $v = (w-1)d = (-d^2+d)d = d^2 - d^3$ which gives the equation for E_7 in Table 3.1.

Since the E we started with is an elliptic curve its discriminant has to be non-zero, hence the isomorphic curve given by E_ℓ has a non-zero discriminant as well. ⊠

After having found the families with rational point of order 3, 5 or 7, we can proceed by computing a model for the quotient curves E'_ℓ. For that we used the Maple-package aPecs by Ian Connell [1] which sports (among many other features) a function for computing an explicit Weierstrass equation for E'. The results are again found in Table 3.1. It also computes explicit expressions for ψ and ξ. From these expressions we read off another important property of ψ:

Fact 3.2.3 Let A be the set of parameters for the families, i.e.:

$$A = \begin{cases} \{v, w\}, & \ell = 3; \\ \{d\}, & \ell = 3 \text{ or } 5. \end{cases}$$

Then

$$\psi = \frac{f}{g^2}$$

with $f, g \in \mathbb{Z}[A][x]$ *monic*.

We will need the expressions for the various ψ later on to be able to apply Lemma 3.1.7 and to compute explicit families.

We conclude this chapter with the following useful:

Proposition 3.2.4 *Let $\ell = 3$, 5 or 7 and let $E = E_\ell$ be an elliptic curve in Table 3.1 with* integral *parameters. Then the cyclic subgroup Φ of E of order ℓ is integral, i.e.: $\Phi \subset E(\mathbb{Z})$.*

PROOF. Use [14, Theorem 7.1, p. 220] and note that $[1/(\ell - 1)] = 0$ for $\ell > 2$. ⊠

$$
\begin{aligned}
E_3 &: && y^2 + wxy + vy = x^3 \\
E_3' &: && y^2 + wxy + vy = x^3 - 5wvx - v(w^3 + 7v) \\
E_5 &: && y^2 + (d+1)xy + dy = x^3 + dx^2 \\
E_5' &: && y^2 + (d+1)xy + dy = x^3 + dx^2 + 5d(d^2 - 2d - 1)x + \\
& && \qquad d(d^4 - 10d^3 - 5d^2 - 15d - 1) \\
E_7 &: && y^2 + (1 + d - d^2)xy + (d^2 - d^3)y = x^3 + (d^2 - d^3)x^2 \\
E_7' &: && y^2 + (1 + d - d^2)xy + (d^2 - d^3)y = x^3 + (d^2 - d^3)x^2 \\
& && \qquad - 5d(d-1)(d^2 - d + 1)(d^3 + 2d^2 - 5d + 1)x \\
& && \qquad - d(d-1)(d^9 + 9d^8 - 37d^7 + 70d^6 - 132d^5 + \\
& && \qquad\quad 211d^4 - 182d^3 + 76d^2 - 18d + 1)
\end{aligned}
$$

Table 3.1: Families of elliptic curves

ℓ	$\Delta(E_\ell)$	$\Delta(E_\ell')$
3	$v^3(w^3 - 27v)$	$v(w^3 - 27v)^3$
5	$-d^5(d^2 + 11d - 1)$	$-d(d^2 + 11d - 1)^5$
7	$d^7(d-1)^7(d^3 - 8d^2 + 5d + 1)$	$d(d-1)(d^3 - 8d^2 + 5d + 1)^7$

Table 3.2: Discriminants of the elliptic curves in Table 3.1

Chapter 4

Local considerations

Recall the notation and hypothesis from Proposition 3.2.4 and in Theorem 3.1.1. The question is whether the extension $\mathbb{Q}(Q)/\mathbb{Q}(P)$ is unramified. We first deal with the finite places in the next section and then with the infinite places in §4.2.

4.1 Ramification at finite places

Suppose p is a rational prime, v is a place of $\mathbb{Q}(P)$ lying over p and w is a prolongation of v to $\mathbb{Q}(Q)$. Let K_v be the completion of $\mathbb{Q}(P)$ at v and let K_w be the completion of $\mathbb{Q}(Q)$ at w. The question whether $\mathbb{Q}(Q)/\mathbb{Q}(P)$ is unramified at v translates to whether $K_w \subset K_v^{\mathrm{unr}}$, the maximal unramified extension of K_v. In turn, this is equivalent to $Q \in E(K_v^{\mathrm{unr}})$. So, we have that:

$$\mathbb{Q}(Q)/\mathbb{Q}(P) \text{ is unramified over } v \iff Q \in E(K_v^{\mathrm{unr}}).$$

Notation 4.1.1 For ease of notation, set $L_v := K_v^{\mathrm{unr}}$. We use a tilde ($\tilde{\cdot}$) to denote reduction modulo the maximal ideal of L_v. Note that the residue field of L_v equals $\overline{\mathbb{F}}_p$.

We are going to decide this matter first in a slightly broader view. Suppose that E, E' are elliptic curves, defined over L_v, which are given by Weierstraß equations which are minimal with respect to v (cf. the Definition on p. 172 of [14] with $R = \mathcal{O}_{L_v}$), so that reduction makes sense. (Here v is actually the prolongation of the discrete valuation on K_v to L_v. Note that since L_v is unramified, $v : L_v \longrightarrow \mathbb{Z}$.)

Notation 4.1.2 Let E be an elliptic curve defined over a local, complete field K with residue field k. We recall the following notation from [14, §VII 2, p. 173]:

$\widetilde{E}_{\mathrm{ns}}(k)$ the group of non-singular points on $\widetilde{E}$.
$E_0(K)$ $= \{P \in E(K) \mid \widetilde{P} \in \widetilde{E}_{\mathrm{ns}}\}$ is the subgroup of non-singular reduction.
$E_1(K)$ $= \{P \in E(K) \mid \widetilde{P} = \widetilde{O}\}$ is the kernel of reduction.

From the theory of elliptic curves (see e.g. [14, Prop. 2.1, p. 175]), we have the following two *exact* sequences:

$$0 \longrightarrow E_1(L_v) \longrightarrow E_0(L_v) \longrightarrow \widetilde{E}_{\mathrm{ns}}(\overline{\mathbb{F}_p}) \longrightarrow 0$$

$$0 \longrightarrow E_1'(L_v) \longrightarrow E_0'(L_v) \longrightarrow \widetilde{E}_{\mathrm{ns}}'(\overline{\mathbb{F}_p}) \longrightarrow 0.$$

We also have the following two (canonical) exact sequences:

$$0 \longrightarrow E_0(L_v) \longrightarrow E(L_v) \longrightarrow E(L_v)/E_0(L_v) \longrightarrow 0$$

$$0 \longrightarrow E'_0(L_v) \longrightarrow E'(L_v) \longrightarrow E'(L_v)/E'_0(L_v) \longrightarrow 0.$$

From these two sequences we will build up two commutative and exact diagrams of groups ($\mathbb{Z}$-modules), which will allow us to answer the above question. For this we need the following:

Lemma 4.1.3 (The "snake lemma") *Suppose we are given a* commutative *diagram of Abelian groups of the following form, in which the horizontal sequences are* exact*:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_3 & \longrightarrow & N_3 & \longrightarrow & 0. \end{array}$$

Define (for $i = 1, 2, 3$) the kernels $\ker_i := \ker \varphi_i$ *and the* cokernels $\operatorname{coker}_i := N_i/\varphi_i(M_i)$. *Then there is a group homomorphism $\delta : \ker_3 \to \operatorname{coker}_1$ such that we have the following exact sequence:*

$$0 \longrightarrow \ker_1 \longrightarrow \ker_2 \longrightarrow \ker_3 \xrightarrow{\delta} \operatorname{coker}_1 \longrightarrow \operatorname{coker}_2 \longrightarrow \operatorname{coker}_3 \longrightarrow 0.$$

PROOF. (The proof is elementary but quite lengthy and understanding is not really essential for understanding the rest of this chapter, so the reader might skip this proof.)

Any homomorphism of abelian groups

$$A \xrightarrow{f} B$$

can be (canonically) extended to the following exact sequence:

$$0 \longrightarrow \ker f \longrightarrow A \longrightarrow B \longrightarrow \operatorname{coker} f \longrightarrow 0.$$

Label the map from M_i to M_{i+1} as f_i and label the map from N_i to N_{i+1} as g_i (for $i = 1, 2$).

Define (for $i = 1, 2$) the homomorphisms f'_i as the restriction of f_i to $\ker_i$. Let $m_i \in \ker_i$, then $\varphi_{i+1}(f_i(m_i)) = g_i(\varphi_i(m_i)) = g_i(0) = 0$, because of commutativity. Hence $f_i(m_i) \in \ker_{i+1}$ and $f_i : \ker_i \longrightarrow \ker_{i+1}$.

First, we want to prove that the following sequence is exact:

$$0 \longrightarrow \ker_1 \xrightarrow{f'_1} \ker_2 \xrightarrow{f'_2} \ker_3 .$$

Since f_1 injects into M_2, the restriction f'_1 of f_1 to $\ker_1$ injects into $\ker_2$, so we have exactness on the left. To show that $\operatorname{im} f'_1 = \ker f'_2 \Leftrightarrow f'_2 \circ f'_1 = 0$ we simply note that already $f_2 \circ f_1 = 0$ because of exactness at M_1, so the restriction of $f_2 \circ f_1$ to $\ker_1$, which is the same as the map $f'_2 \circ f'_1$, is the zero map as well. Hence we have exactness in the middle (at $\ker_2$).

Define the following homomorphisms (for $i = 1, 2$):

$$\begin{array}{rccc} g'_i & : & \operatorname{coker}_i & \longrightarrow & \operatorname{coker}_{i+1} \\ & & n_i + \varphi_i(M_i) & \longmapsto & g_i(n_i) + \varphi_{i+1}(M_{i+1}), \qquad n_i \in N_i. \end{array}$$

To show that this is well-defined, we have to prove that the definition is independent of the choice for the representant $n_i \in N_i$ of the coset. Let $n_i' \in N_i$ such that $n_i' - n_i \in \varphi_i(M_i)$, thus n_i', n_i represent the same coset of coker_i, i.e. $n_i' - n_i \in \varphi_i(M_i)$. Hence an $m_i \in M_i$ exists such that $n_i' - n_i = \varphi_i(m_i)$. Now $g_i(n_i') - g_i(n_i) = g_i(n_i' - n_i) = (g_i \circ \varphi_i)(m_i) = (\varphi_{i+1} \circ f_i)(m_i)$ because of commutativity, so $g_i(n_i') - g_i(n_i) \in \varphi_{i+1}(M_{i+1})$. Therefore $g_i'(n_i' + \varphi_i(M_i)) = g_i'(n_i + \varphi_i(M_i))$.

Secondly, we want to prove the following sequence to be exact:

$$\text{coker}_1 \xrightarrow{g_1'} \text{coker}_2 \xrightarrow{g_2'} \text{coker}_3 \longrightarrow 0.$$

Since g_2 surjects onto N_3, we have that $g_2(N_2 + \varphi_2(M_2)) = N_3 + \varphi_3(M_3) = \text{coker}_3$, hence g_2' is surjective as well and we have exactness on the right. For $n_1 \in N_1$ we have that

$$\begin{aligned}(g_2' \circ g_1')(n_1 + \varphi_1(M_1)) &= g_2'(g_1(n_1) + \varphi_2(M_2)) \\ &= (g_2 \circ g_1)(n_1) + \varphi_2(M_2) \\ &= 0 + \varphi_2(M_2)\end{aligned}$$

since already $g_2 \circ g_1 = 0$. Hence $g_2' \circ g_1' = 0$ and we have exactness on the left.

Finally, we want to prove there is a homomorphism $\delta : \text{ker}_3 \to \text{coker}_1$ such that the following sequence is exact:

$$\text{ker}_2 \xrightarrow{f_2'} \text{ker}_3 \xrightarrow{\delta} \text{coker}_1 \xrightarrow{g_1'} \text{coker}_2 .$$

Let $m_3 \in \text{ker}_3$. Since f_2 is surjective, $m_2 \in M_2$ exists such that $f_2(m_2) = m_3$. Now $(\varphi_3 \circ f_2)(m_2) = 0 = (g_2 \circ \varphi_2)(m_2)$ because of commutativity, so $\varphi_2(m_2) \in \ker g_2 = \text{im}\, g_1$. Since g_1 is injective, a unique $n_1 \in N_1$ exists such that $g_1(n_1) = \varphi_2(m_2)$. Define $\delta(m_3) = n_1 + \varphi_1(M_1)$. This is well-defined provided the definition does not depend on the choice of $m_2 \in M_2$.

Let $m_2' \in M_2$ be such that $f_2(m_2') = m_3$ and $m_2' \neq m_2$. Then (in the same manner as above) a unique $n_1' \in N_1$ exists such that $g_1(n_1') = \varphi_2(m_2')$. The homomorphism is well-defined for m_3 if $n_1' - n_1 \in \varphi_1(M_1)$. Since $f_2(m_2') = f_2(m_2) \Leftrightarrow f_2(m_2' - m_2) = 0 \Leftrightarrow m_2' - m_2 \in \ker f_2 = \text{im}\, f_1$, a $m_1 \in M_1$ exists such that $f_1(m_1) = m_2' - m_2$.

Note that since g_1 is injective, the following holds true: if $x, y \in N_1$ for which $g_1(x) = g_1(y)$, then $x = y$. We claim that $n_1' - n_1 = \varphi_1(m_1)$. For this:

$$\begin{aligned}g_1(n_1' - n_1) = g_1(n_1') - g_1(n_1) = \varphi_2(m_2') - \varphi_2(m_2) = \varphi_2(m_2' - m_2) \\ = \varphi_2(f_1(m_1)) = (g_1 \circ \varphi_1)(m_1) = g_1(\varphi_1(m_1)).\end{aligned}$$

We still have to prove exactness at ker_3 and coker_1.

Let $m_2 \in \text{ker}_2$. By going through the steps defining δ, we see we have to find an $n_1 \in N_1$ such that $g_1(n_1) = \varphi_2(m_2)$. But since $m_2 \in \text{ker}_2$ and g_1 is injective:

$$g_1(n_1) = \varphi_2(m_2) = 0 \Longrightarrow n_1 = 0.$$

Therefore $\delta \circ f_2 = 0$ and we have exactness at ker_3.

Let $m_3 \in \text{ker}_3$. Then $\delta(m_3) = n_1 + \varphi_1(M_1)$ where $m_2 \in M_2$ such that $f_2(m_2) = m_3$ and $n_1 \in N_1$ such that $g_1(n_1) = \varphi_2(m_2)$. But then:

$$(g_1' \circ \delta)(m_3) = g_1(n_1) + \varphi_2(M_2) = \varphi_2(m_2) + \varphi_2(M_2) = 0 + \varphi_2(M_2).$$

Hence $g_1' \circ \delta = 0$ and we have exactness at coker_1.

All in all, combining the various exact sequences, we extended the diagram as follows, in which all (extended) horizontal and vertical sequences are exact:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \ker_1 & \longrightarrow & \ker_2 & \longrightarrow & \ker_3 & \xrightarrow{\delta} & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & \xrightarrow{\delta} & \mathrm{coker}_1 & \longrightarrow & \mathrm{coker}_2 & \longrightarrow & \mathrm{coker}_3 & \longrightarrow & 0.
\end{array}$$

⊠

The map $\widetilde{\varphi}$

By simply reducing the coefficients of the rational functions defining φ, we obtain a morphism $\widetilde{\varphi}$ from $\widetilde{E}(\overline{\mathbb{F}_p})$ to $\widetilde{E'}(\overline{\mathbb{F}_p})$. This morphism can be constant, see e.g. [14, Example 4.5, p. 74] where $\widehat{\phi}$ mod 2 is the zero map. If we suppose that $\widetilde{\varphi}$ is non-constant (which is equivalent to the constant denominator of ψ having non-zero reduction), then it follows from algebraic geometry that it is an epimorphism.

Fact 4.1.4 Non-singular points of $\widetilde{E}$ are mapped to non-singular points of $\widetilde{E'}$.

PROOF (SKETCH). We will present a sketch of this fact using the theory of Néron minimal models, cf. [14, §15].

Let $\mathcal{E}$, $\mathcal{E}'$ be the Néron minimal models for E, E', respectively. These are group schemes over $\mathrm{Spec}(R)$ whose generic fiber $\mathcal{E} \times_{\mathrm{Spec}(R)} \mathrm{Spec}(K)$ is isomorphic to E/K (as a group variety). They also come with natural isomorphisms $\mathcal{E}(R) \to E(K)$ and $\mathcal{E}'(R) \to E'(K)$. Let $\widetilde{\mathcal{E}} = \mathcal{E} \times_{\mathrm{Spec}(R)} \mathrm{Spec}(k)$ be the special fiber of $\mathcal{E}$ and likewise but with primes added for $\mathcal{E}'$. Then $\widetilde{\mathcal{E}}$ and $\widetilde{\mathcal{E}'}$ are both algebraic groups over k. Let $\widetilde{\mathcal{E}}^0/k$, $\widetilde{\mathcal{E}'}^0/k$ be the identity component of $\widetilde{\mathcal{E}}$, $\widetilde{\mathcal{E}'}$, respectively. We then have (with the identification $\mathcal{E}(R) \cong E(K)$) that:

$$\widetilde{\mathcal{E}}^0(k) \cong \widetilde{E}_{\mathrm{ns}}(k), \qquad \widetilde{\mathcal{E}'}^0(k) \cong \widetilde{E}'_{\mathrm{ns}}(k). \tag{4.1}$$

The morphism $\varphi : E \longrightarrow E'$ extends to a flat morphism of schemes $\varphi' : \mathcal{E} \longrightarrow \mathcal{E}'$ over $\mathrm{Spec}(R)$. Reducing we obtain a morphism of algebraic groups (over k):

$$\widetilde{\varphi}' : \widetilde{\mathcal{E}} \longrightarrow \widetilde{\mathcal{E}'}.$$

Naturally, φ' is continuous for the Zariski-topology, hence $\widetilde{\varphi}'$ is continuous as well and the identity component is mapped to the identity component:

$$\widetilde{\varphi}'(\widetilde{\mathcal{E}}^0(k)) \subset \widetilde{\mathcal{E}'}^0(k).$$

Together with the identifications (4.1) this gives the desired result. ⊠

Hence, we obtain a map $\widetilde{E}_{\mathrm{ns}} \longrightarrow \widetilde{E}'_{\mathrm{ns}}$. This map is surjective as well. For let R be a non-singular point of $\widetilde{E'}(\overline{\mathbb{F}_p})$. Since $\widetilde{\varphi}$ is an epimorphism, there is a point $\widetilde{P}$ on $\widetilde{E}(\overline{\mathbb{F}_p})$ which is mapped to R. This point $\widetilde{P}$ cannot be singular, since then R would be singular as well.

The objects $\widetilde{E}_{\mathrm{ns}}$ and $\widetilde{E}'_{\mathrm{ns}}$ are commutative groups, with the group laws given by the usual group law on an elliptic curve. We will shortly show that $\widetilde{\varphi} : \widetilde{E}_{\mathrm{ns}} \longrightarrow \widetilde{E}'_{\mathrm{ns}}$ is a group homomorphism, but for now we only need that it is well-defined and surjective.

The left side of the diagram

Since φ is a homomorphism taking $E(L_v)$ to $E'(L_v)$, we automatically have a homomorphism from $E_1(L_v)$ to $E'(L_v)$. However, even more is true: the image of $E_1(L_v)$ under φ is contained in $E'_1(L_v)$.

PROOF. Consider the following commutative diagram (in which not all maps have to be homomorphisms):

$$\begin{array}{ccc} E_1(L_v) & \longrightarrow & \widetilde{E}_{\mathrm{ns}}(\overline{\mathbb{F}_p}) \\ \downarrow{\scriptstyle \varphi} & & \downarrow \\ E'_1(L_v) & \longrightarrow & \widetilde{E'}(\overline{\mathbb{F}_p}) \end{array}$$

We know (see e.g. the proof of [14, Prop. 1.4 (a), p. 50]) that $\widetilde{O} \in \widetilde{E}$, $\widetilde{O'} \in \widetilde{E'}$ are non-singular. Let $P \in E_1(L_v)$, i.e. $\widetilde{P} = \widetilde{O}$. Then $\widetilde{\varphi}(\widetilde{P}) = \widetilde{O'}$, therefore $\widetilde{\varphi(P)} = \widetilde{O'}$. Conclusion: $\varphi(P) \in E'_1(L_v)$. ⊠

We can even say a little more. Suppose that $p \neq \ell$. We have that $E_1(L_v)$ is isomorphic to the group $\widehat{E}(\mathfrak{M})$ coming from the formal group of E, where $\mathfrak{M}$ is the maximal ideal of $\mathcal{O}_{L_v}$, the ring of integers of $L_v = K_v^{\mathrm{unr}}$. Likewise: $E'_1(L_v) \cong \widehat{E'}(\mathfrak{M})$. Now, consider the multiplication-by-ℓ-map $[\ell]$ on $\widehat{E}$. Since $\mathrm{char}(\mathcal{O}_{L_v}/\mathfrak{M}) = p$ and ℓ are relatively prime, $\ell \in \mathcal{O}^*_{L_v}$, so $[\ell] : \widehat{E} \longrightarrow \widehat{E}$ is an isomorphism. Hence $[\ell] : \widehat{E}(\mathfrak{M}) \longrightarrow \widehat{E}(\mathfrak{M})$ is an isomorphism as well and thus:

$$[\ell] : E_1(L_v) \xrightarrow{\sim} E_1(L_v).$$

But $[\ell]$ on $E_1(L_v)$ factors through $\varphi_{|E_1(L_v)}$ and the restriction $\widehat{\varphi}_{|E'_1(L_v)}$ of the dual isogeny from E' to E (which is also defined over $\mathbb{Q}$ since φ is) restricted to $E'_1(L_v)$. Hence: $E_1(L_v) \cong E'_1(L_v)$ in case $p \neq \ell$.

The center part of the diagram

Consider the following commutative diagram:

$$\begin{array}{ccc} E_0(L_v) & \longrightarrow & \widetilde{E}_{\mathrm{ns}}(\overline{\mathbb{F}_p}) \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \widetilde{\varphi}} \\ E'(L_v) & \longrightarrow & \widetilde{E'}(\overline{\mathbb{F}_p}) \end{array}$$

Let $P \in E_0(L_v)$. Then $\widetilde{\varphi}(\widetilde{P})$ is a non-singular point of $\widetilde{E'}$. Hence $\varphi(P)$, which is a priori an element of $E'(L_v)$, reduces to a non-singular point of $\widetilde{E'}$, so: $\varphi(E_0(L_v)) \subset E'_0(L_v)$.

The right side of the diagram

Now, it is easy to show that the map

$$\widetilde{\varphi} : \widetilde{E}_{\mathrm{ns}}(\overline{\mathbb{F}_p}) \longrightarrow \widetilde{E}'_{\mathrm{ns}}(\overline{\mathbb{F}_p})$$

is a group homomorphism by simple considering the following commutative diagram, in which all arrows except the one labeled $\widetilde{\varphi}$ are *a priori* group homomorphisms and $\widetilde{\varphi}$ is a well-defined map:

$$\begin{array}{ccc} E_0(L_v) & \xrightarrow{\text{surj.}} & \widetilde{E}_{\mathrm{ns}}(\overline{\mathbb{F}_p}) \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \widetilde{\varphi}} \\ E'_0(L_v) & \longrightarrow & \widetilde{E}'_{\mathrm{ns}}(\overline{\mathbb{F}_p}). \end{array}$$

The kernels and cokernels

Next, we want to be able to say something about the various kernels and cokernels which will appear in the long exact sequence produced by Lemma 4.1.3.

Note that in the situation we will apply the results of this Chapter to, the degree of φ is $\ell \geq 3$ so that by Proposition 3.2.4 the kernel of φ is integral, i.e.: $\Phi \subset E(\mathbb{Z})$. In particular: $\Phi \subset E(\mathcal{O}_{L_v})$ for each place v.

We henceforth assume that the kernel of φ is integral: $\Phi \subset E(\mathbb{Z}) \subset E(\mathcal{O}_{L_v})$. Since E is given by a minimal Weierstraß equation, $E_1(L_v)$ is simply given by:

$$\{O\} \cup \{(x,y) \in E(L_v) \mid v(x), v(y) < 0\}.$$

Then $\ker_1 = \ker(\varphi : E_1(L_v) \longrightarrow E'_1(L_v))$ is trivial.

We also have that $\ker_2 = \ker(\varphi : E_0(L_v) \longrightarrow E'_0(L_v))$ is a subgroup of Φ so that either $\ker_2$ is trivial (in which case all points $O \neq P \in \Phi$ have singular reduction) or Φ itself.

Furthermore, since $\ker_1 = \ker(\varphi : E_1(L_v) \longrightarrow E'_1(L_v))$ is trivial, $\ker_2$ injects into $\ker_3 = \ker(\widetilde{\varphi} : \widetilde{E}_{\mathrm{ns}}(\overline{\mathbb{F}_p}) \longrightarrow \widetilde{E}'_{\mathrm{ns}}(\overline{\mathbb{F}_p}))$. Also, $\ker_3$ corresponds to the poles of the rational functions $\widetilde{\psi}(x,y)$, $\widetilde{\xi}(x,y)$ on $\widetilde{E}$. But since we assumed that the kernel was integral, all of the poles of the rational functions $\psi(x,y)$, $\xi(x,y)$ on E already had integral coordinates, hence $\ker_2$ surjects onto $\ker_3$. So: $\ker_2 \cong \ker_3$.

The snake lemma now asserts the existence of a map δ such that the following is a long exact sequence (of $\mathbb{Z}$-modules):

$$0 \longrightarrow \ker \varphi_{|E_0(L_v)} \xrightarrow{\sim} \ker \widetilde{\varphi}_{|\widetilde{E}_{\mathrm{ns}}(\overline{\mathbb{F}_p})} \xrightarrow{\delta} \mathrm{coker}_1 \longrightarrow \mathrm{coker}_2 \longrightarrow \mathrm{coker}_3 \longrightarrow 0.$$

Since the second map is an isomorphism, δ has to be the zero map. Because $\widetilde{\varphi} : \widetilde{E}_{\mathrm{ns}}(\overline{\mathbb{F}_p}) \longrightarrow \widetilde{E}'_{\mathrm{ns}}(\overline{\mathbb{F}_p})$ is surjective, coker_3 is trivial. From these two facts it follows that $\mathrm{coker}_1 \cong \mathrm{coker}_2$.

All in all, we can now easily prove the following:

Theorem 4.1.5 *Let $E/\mathbb{Q}$, $E'/\mathbb{Q}$ be elliptic curves given by globally minimal Weierstraß equations. Assume that an isogeny $\varphi : E \longrightarrow E'$ of prime degree ℓ exists such that the kernel is integral (i.e.: $\ker\varphi \subset E(\mathbb{Z})$). Suppose $\widetilde{\varphi}$ isn't the zero map.*

Let $P = (t, s) \in E$ be such that $t \in \mathbb{Q}$ and s is a quadratic number and set $K = \mathbb{Q}(P)$. Let p be a rational prime and let v be a place of $\mathbb{Q}(P)$ lying over p. Set $L_v := K_v^{unr}$ be the maximal unramified extension of the completion K_v of K at v.

Then:

(a) if $v \nmid \ell$, then

$$E_0'(L_v)/\varphi(E_0(L_v)) = (0),$$

so $\mathbb{Q}(\varphi^{-1}(P))/\mathbb{Q}(P)$ is unramified at v;

(b) if $v \mid \ell$, then:

$$E_0'(L_v)/\varphi(E_0(L_v)) \cong E_1'(L_v)/\varphi(E_1(L_v)).$$

PROOF. In the previous pages, we have built up the following commutative diagram and which all vertical and (extended) horizontal sequences are exact:

$$\begin{array}{ccccccccc}
 & & 0 & \longrightarrow & \ker_2 & \xrightarrow{\sim} & \ker_3 & \xrightarrow{\delta=0} & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E_1(L_v) & \longrightarrow & E_0(L_v) & \longrightarrow & \widetilde{E}_{\mathrm{ns}}(\overline{\mathbb{F}_p}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \widetilde{\varphi}} & & \\
0 & \longrightarrow & E_1'(L_v) & \longrightarrow & E_0'(L_v) & \longrightarrow & \widetilde{E}'_{\mathrm{ns}}(\overline{\mathbb{F}_p}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \xrightarrow{\delta=0} & \mathrm{coker}_1 & \xrightarrow{\sim} & \mathrm{coker}_2 & \longrightarrow & 0. &
\end{array}$$

If $v \nmid \ell$, then coker_1 is trivial, so $\mathrm{coker}_2 = E_0'(L_v)/\varphi(E_0(L_v)) \cong \mathrm{coker}_1$ is trivial as well. Hence $Q \in K_w \subset L_v$ and $\mathbb{Q}(Q)/\mathbb{Q}(P)$ is unramified at v, which accounts for *(a)*.

If $v \mid \ell$, then all we have is the isomorphism of groups in *(b)*. ⊠

For practical purposes we also have the following elementary:

Lemma 4.1.6 *Let E be an elliptic curve defined over $\mathbb{Q}$, given by a globally minimal Weierstraß equation and let Δ be its discriminant. Then for each rational prime p dividing Δ, there is an element $t_p \in \mathbb{F}_p$, such that:*

$$t \equiv t_p \pmod{p} \Longleftrightarrow P = (t, s) \in E' \text{ reduces singularly modulo } p.$$

PROOF. Let p be a rational prime dividing Δ. It is sufficient to prove that the singular curve $E \bmod p$ has precisely one singular point, that it is $\mathbb{F}_p$-rational and that there are no other points with the same $\widetilde{x}$-coordinate.

(i) Suppose $E \bmod p$ has more than one singular point. Consider a line through two singular points. This line intersects the projective *cubic* curve at least four times (counted with multiplicity), which is impossible.

(ii) Suppose the singular point is not $\mathbb{F}_p$-rational. By definition it is a zero of the three polynomials

$$F, \quad \frac{\partial F}{\partial x}, \quad \frac{\partial F}{\partial y} \in \mathbb{F}_p[x, y]$$

where $F(x, y) = y^2 + \widetilde{a_1}xy + \widetilde{a_3}y - (x^3 + \widetilde{a_2}x^2 + \widetilde{a_4}x + \widetilde{a_6})$ has all coefficients in $\mathbb{F}_p$. Suppose the singular point has coordinates in some extension $K/\mathbb{F}_p$. Letting $\mathrm{Gal}(K/\mathbb{F}_p)$ act on the singular point gives at least one other point. This point also satisfies the three polynomials, so the other point must be singular point. But that contradicts (i), hence $K = \mathbb{F}_p$.

(iii) Let the $\widetilde{x}$-coordinate of the singular point be $t_p \in \mathbb{F}_p$. Consider the line $\widetilde{x} = t_p$ which by assumption intersects E mod p at least two-fold in the singular point. It also intersects E mod p in $\widetilde{O}$. Hence the line intersects E mod p exactly twice in the singular point, exactly once in $\widetilde{O}$ and in no other points. This proves E mod p has no other points with $\widetilde{x} = t_p$.

⊠

Remark 4.1.7 If for all places v dividing Δ, P reduces non-singularly (i.e. $P \in E_0(K_v)$, then the condition in the Theorem is trivially satisfied. The groups $E'(L_v)/E'_0(L_v)$, $E(L_v)/E_0(L_v)$ (and thus the quotient), are only simple to compute explicitly if E and E' have split multiplicative reduction at v, since then $E(L_v)/E_0(L_v) \cong E(K_v)/E_0(K_v)$ and likewise with primes added.

4.2 Ramification at infinite places

We utilize Lemma 2.2.2 to prove no ramification at infinite places will occur.

Lemma 4.2.1 *Let notation and hypotheses be as in Theorem 4.1.5. Then $\mathbb{Q}(\varphi^{-1}(P))/\mathbb{Q}(P)$ is unramified at all infinite places.*

PROOF. From Lemma 3.1.7 we know that the extension under consideration is Galois. In view of Corollary 2.2.2 it suffices to show that if $P \in E'(\mathbb{R})$ then $\varphi^{-1}(P) \subset E(\mathbb{R})$ and if $P \notin E'(\mathbb{R})$, then $\varphi^{-1}(P) \subsetneq E(\mathbb{R})$.

Suppose $Q \in \varphi^{-1}(P)$. For $\varphi(Q) = P$ to hold, it is necessary that $\psi(x(Q)) = t$. By clearing the denominator of the left hand side, we see that $x(Q)$ must be a root of the polynomial λ_t from Lemma 3.1.7. Since λ_t is a polynomial of odd degree with real coefficients, it has at least one real root. So there is at least one Q such that $x(Q) \in \mathbb{R}$.

If $P \in E'(\mathbb{R})$ then $\mathbb{Q}(P) \subset \mathbb{R}$. From Proposition 3.1.5 and the fact that $\varphi(E(\mathbb{R})) \subset E'(\mathbb{R})$ since φ is defined over $\mathbb{Q} \subset \mathbb{R}$, it now follows that $\mathbb{Q}(\varphi^{-1}(P)) = (\mathbb{Q}(P))(x(Q)) \subset \mathbb{R}$. If, on the other hand, $P \notin E'(\mathbb{R})$, then $\mathbb{Q}(P)$ is totally complex hence $\mathbb{Q}(\varphi^{-1}(P)) \supset \mathbb{Q}(P)$ is complex as well.

Hence $\mathbb{Q}(P)$ and $\mathbb{Q}(\varphi^{-1}(P))$ are simultaneously totally real or complex, so from Lemma 2.2.2 it follows that the extension is unramified at all infinite places. ⊠

4.3 Local to global

Theorem 4.3.1 *Let notation and hypotheses be as in Theorem 4.1.5. If for all places v dividing Δ but not dividing ℓ, $\widetilde{\varphi}$ is not the zero map and the image of P in the finite group*

$$\big(E'(L_v)/E'_0(L_v)\big) \Big/ \varphi\big(E(L_v)/E_0(L_v)\big) \tag{4.2}$$

is trivial, then $\mathbb{Q}(\varphi^{-1}(P))/\mathbb{Q}(P)$ is unramified at all infinite places and at all finite places of $\mathbb{Q}(P)$ not dividing ℓ.

PROOF. Lemma 4.2.1 takes care of the ramification at infinite places. Let v be a finite place not dividing ℓ. From Theorem 4.1.5 we know that the cokernel $E'_0(L_v)/\varphi(E_0(L_v))$ is trivial. Recall the following two (canonical) exact sequences:

$$0 \longrightarrow E_0(L_v) \longrightarrow E(L_v) \longrightarrow E(L_v)/E_0(L_v) \longrightarrow 0$$

$$0 \longrightarrow E'_0(L_v) \longrightarrow E'(L_v) \longrightarrow E'(L_v)/E'_0(L_v) \longrightarrow 0.$$

From these two sequences and the snake lemma we build up the following commutative diagram of Abelian groups in which all vertical and (extended) horizontal are exact:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E_0(L_v)\cap\Phi & \longrightarrow & \Phi & \longrightarrow & \ker_3 & \xrightarrow{\delta} & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E_0(L_v) & \longrightarrow & E(L_v) & \longrightarrow & E(L_v)/E_0(L_v) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\varphi} & & \downarrow & & \\
0 & \longrightarrow & E'_0(L_v) & \longrightarrow & E'(L_v) & \longrightarrow & E'(L_v)/E'_0(L_v) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & \xrightarrow{\delta} & \mathrm{coker}_1 & \longrightarrow & \mathrm{coker}_2 & \longrightarrow & \mathrm{coker}_3 & \longrightarrow & 0.
\end{array}$$

For $\mathbb{Q}(\varphi^{-1}(P))/\mathbb{Q}$ to be unramified at v is equivalent to $Q \in L_v$ which in turn is equivalent to the image of P in the cokernel $\mathrm{coker}_2 = E(L_v)/\varphi(E'(L_v))$ being trivial.

From Theorem 4.1.5 we know that $\mathrm{coker}_1 = E_0(L_v)/E'_0(L_v)$ is trivial. If $v \nmid \Delta$, then $E_0(L_v) = E(L_v)$ and $E'_0(L_v) = E(L_v)$, which implies that all groups in the right most vertical exact sequence are trivial. In particular we have the exact sequence

$$0 \longrightarrow \mathrm{coker}_2 \longrightarrow 0\,(\longrightarrow 0)$$

from which it follows that coker_2 is trivial. Hence P has trivial image in it as well.

If $v \mid \Delta$ but doesn't divide ℓ, then the bottom horizontal exact sequence of the diagram reads:

$$0 \longrightarrow \mathrm{coker}_2 \longrightarrow \mathrm{coker}_3 \longrightarrow 0.$$

In particular: coker_2 is isomorphic to coker_3 which is the group (4.2). So, if P has trivial image in coker_3, then it has trivial image in coker_2 as well. ⊠

Chapter 5

Families

In this chapter we are going to use the results from the previous chapter to explicitly realize families of quadratic number fields with class number divisible by ℓ.

5.1 The main theorem

Theorem 5.1.1 *Let $\ell = 3$, 5 or 7. Let $E = E_\ell$ and $E' = E'_\ell$ be given by Table 3.1 with* integral *parameters such that $\Delta(E) \neq 0$ and the Weierstraß equations are globally minimal. Let $\Delta(t) = \Delta_\ell(t)$ be given by Table 5.1. Then:*

(a) There are infinitely many $t \in \mathbb{Q}$ such that $\mathbb{Q}(\sqrt{\Delta(t)})$ is a quadratic number field with class number divisible by ℓ.

(b) (a) even holds for t ranging over rationals with fixed denominator.

(c) More explicitly, the conditions (all of which are necessary and sufficient except for conditions (iii) and (iv) which are merely sufficient) on t are:

(i) $t \notin \pi(E'(\mathbb{Q}))$ where $\pi : E' \longrightarrow \mathbb{P}^1$ is the morphism defined by $(x, y) \longmapsto x$;
(ii) λ_t is irreducible in $\mathbb{Q}[x]$;
(iii) for each prime p dividing $\Delta(E)$: either p divides the denominator of t or $t \not\equiv t_p \pmod{p}$, where the t_p come from Lemma 4.1.6;
(iv) further conditions on t (explicitly dependent of the choice of parameters) are:

$\ell = 3$) if $3 \mid vw$, then 3 does not divide the numerator of t;

$\ell = 5$) if $d \equiv 0$ or $2 \pmod 5$, then either 5 divides the denominator of t or

$$t \not\equiv \begin{cases} 0, & \text{if } d \equiv 0 \pmod 5 \\ -1, & \text{if } d \equiv 2 \pmod 5 \end{cases} \pmod 5;$$

$\ell = 7$) if $d \equiv 0$, 1 or $5 \pmod 7$, then either 7 divides the denominator of t or

$$t \not\equiv \begin{cases} 0, & \text{if } d \equiv 0 \text{ or } 1 \pmod 7 \\ 5, & \text{if } d \equiv 5 \pmod 7 \end{cases} \pmod 7.$$

PROOF. *(a)* follows trivially from *(b)*. We first prove *(c)*.

Note that $\Delta(E) \neq 0$ implies that $\Delta(E') \neq 0$. One possible way to see this is to inspect Table 3.2.

Let $t \in \mathbb{Q}$ and let $P = (t, s) \in E'$ be a point of E'. From Theorem 3.1.1 *(b)* we know that P generates a quadratic number field if and only if $P \notin E'(\mathbb{Q})$ which is equivalent to $t \notin \pi(E'(\mathbb{Q}))$. This accounts for condition *(i)*. From now on, we assume $P \notin E'(\mathbb{Q})$ and set $k = \mathbb{Q}(P)$. The $\Delta_\ell(t)$ in Table 5.1 were computed as the right hand side of (3.3) with the b_i''s as in (3.4). Hence: $k = \mathbb{Q}(\sqrt{\Delta(t)})$.

From Lemma 3.1.7 and Remark 3.1.6 we see that $K := \mathbb{Q}(\varphi^{-1}(P))$ is a cyclic extension of order ℓ of k, provided that the polynomial λ_t is irreducible over $\mathbb{Q}$ which accounts for condition *(ii)*. From now on, we assume that λ_t is irreducible over $\mathbb{Q}$.

Next we have to see to it that the extension K/k is unramified in the sense of Theorem 2.1.1 *(ii)* and *(iii)*. For that we first use Theorem 4.3.1 which we can use since the kernel Φ of φ is integral by Proposition 3.2.4 and, by inspection, the constant denominator of both ψ, ξ is 1.

Condition *(iii)* is equivalent to $\forall v \mid \Delta(E) : P \in E_0(K_v)$ with notation as in Theorem 4.3.1, hence the image of P in the group denoted is trivial. This takes care of ramification at all infinite places of k and at all finite places of k not dividing ℓ. To deal with ramification at places lying over ℓ we use the results in §2.3.

Let L be a subfield of K such as in the statement of Lemma 2.3.2. Write $t = \xi/n$ with n a positive integer and ξ an integer coprime to n. Since λ_t is monic and irreducible over $\mathbb{Q}$ for the present choice of t, the polynomial

$$\phi(X) := n^\ell \lambda_{\xi/n}(X/n)$$

is monic and irreducible over $\mathbb{Q}$ as well. Furthermore, it has coefficients in $\mathbb{Z}[\xi]$ because of Fact 3.2.3 and the way we defined λ_t and subsequently $\phi(X)$. Now we can take L to be isomorphic to $\mathbb{Q}[X]/(\phi(X))$ and use Proposition 2.3.4. A sufficient condition for K/k to be unramified at places lying over ℓ is that $\phi(X)$ doesn't reduce modulo ℓ to:

$$\phi(X) \equiv (X + c)^\ell \equiv X^\ell + c \bmod \ell$$

for some $c \in \mathbb{F}_\ell$. This will give the conditions in *(iii)*.

The coefficient of $X^{\ell-1}$ in $\phi(X)$ is $-\xi + n(...)$. The coefficient of X^i is divisible by $n^{\ell-i}$ for $i = 1, 2, \ldots, \ell - 2$. For all cases: if $n \equiv 0\ (\ell)$, then $\xi \not\equiv 0\ (\ell)$ since we assumed that $\gcd(\xi, n) = 1$. Hence the coefficient of $X^{\ell-1}$ in $\phi(X)$ will be non-zero (but the coefficients of X^i for $i \leq \ell - 2$ will all be zero), so that in this case there is no ramification over ℓ. Hence we only have to consider $t \in \mathbb{Q}$ such that $\ell \nmid \mathrm{denom}(t)$, i.e.: $\ell \nmid n$. In all cases, this will give a congruence condition on t modulo ℓ.

Next, we are going to treat the three cases separately. In each case, we are going to look at the zeroes of the coefficient of X in $\phi(X)$.

$\boxed{\ell = 3}$

$$\phi(X) = X^3 - \xi X^2 + vwn^2 X + v^2 n^3.$$

The coefficient of X is zero mod 3 precisely if $3 \mid vw$ or $n \equiv 0\ (3)$, of which we only have to consider the first. If $3 \mid vw$, then $\phi(X) \mod 3 = X^3 - \xi X^2 \mod 3$, so $\xi = \mathrm{numer}(t) \not\equiv 0 \pmod 3$ is *required*.

$\boxed{\ell = 5}$

$$\phi(X) = X^5 + (2nd - \xi)X^4 + dn(n(1 + 3d - d^2) - 2\xi)X^3 + (dn)^2(3n(d+1) - \xi)X^2 + d^3n^4(d+3)X + d^4n^5.$$

The coefficient of X is zero mod 5 precisely if $n \equiv 0$ (5) or $d \equiv 0$ or 2 (5). If $d \equiv 0$ (5), then $\phi(X) \mod 5 = X^5 - \xi X^4 \mod 5$, so $\xi \not\equiv 0 \pmod 5 \Leftrightarrow t \not\equiv 0 \pmod 5$ is *required.* If $d \equiv 2$ (5), then the coefficient of $\phi(X) \mod 5$ equals $-(n+\xi) \mod 5$, hence we consider $\xi \equiv -n$ (5). The polynomial then reduces to $X^5 + n \pmod 5$. So, if $d \equiv 2 \pmod 5$, then $\xi \not\equiv -n \pmod 5 \Leftrightarrow t \not\equiv -1 \pmod 5$ is *required.*

$\boxed{\ell = 7}$

$$\phi(X) = X^7 - (2nd(d^2-1) + \xi)X^6 + \ldots + d^8n^6(d^7 - 8d^6 + 22d^5 - 25d^4 + 5d^3 + 14d^2 - 12d + 3)X + d^{10}n^7(d^6 - 6d^5 + 15d^4 - 20d^3 + 15d^2 - 6d + 1).$$

The coefficient of X is zero mod 7 precisely if $n \equiv 0$ (7) or $d \equiv 0,\ 1$ or 5 (7). If $d \equiv 0$ or 1 (7), then $\phi(X) \mod 7 = X^7 - \xi X^6 \mod 7$, so $\xi \not\equiv 0 \pmod 7 \Leftrightarrow t \not\equiv 0$ is *required.* If $d \equiv 5$ (7), then the coefficient of X^6 equals $5n - \xi \mod 7$, so we let $\xi \equiv 5n$ (7). The polynomial then reduces to $X^7 + 5 \mod 7$. So, if $d \equiv 5 \pmod 7$, then $\xi \not\equiv 5n \pmod 7 \Leftrightarrow t \not\equiv 5 \pmod 7$ is *required.*

We next prove *(b).* Fix an integer $n \geq 1$ and again write $t = \xi/n$ where ξ is an integer coprime to n. Note that conditions *(iii)* and *(iv)* can be rephrased in the following manner. For each choice of parameters and denominator there is a finite number of pairs (p_i, r_i) of (not necessarily distinct) primes p_i and $r_i \in \mathbb{F}_{p_i}$ such that conditions *(iii)* and *(iv)* are (for the fixed denominator n) equivalent to:

$$\forall i : \xi \not\equiv r_i \pmod{p_i}$$

Explicitly, all pairs are given by:

- each prime p dividing $\Delta(E)$ but not dividing n gives the pair $(n \cdot t_p, p)$;
- each prime p dividing n gives the pair $(0 \mod p, p)$;
- depending on ℓ and the parameter(s):
  - $\ell = 3$, $3 \nmid n$ and $3 \mid vw$, gives the pair $(0 \mod p, 3)$;
  - $\ell = 5$, $5 \nmid n$ and $d \equiv 0$ or 2 (mod 5), gives the pair $(0 \mod 5, 5)$ or $(-n \mod 5, 5)$, respectively;
  - $\ell = 7$, $7 \nmid n$ and $d \equiv 0, 1$ or 5 (mod 7), gives the pair $(0 \mod 7, 7)$ if $d \equiv 0$ or 1 (mod 7) and the pair $(5n \mod 7, 7)$ if $d \equiv 5$ (mod 7).

The second condition comes from $\gcd(\xi, n) = 1 \Leftrightarrow \forall p \mid n : \xi \not\equiv 0 \pmod p$. Note that all primes except ℓ occur at most once as p_i and that ℓ can occur at most twice. Hence the set of congruences is not degenerate.

The set

$$\{\xi \in \mathbb{Z} \mid \forall i : \xi \not\equiv r_i \pmod{p_i}\} \tag{5.1}$$

is a finite, non-empty union of arithmetic progressions. To see that, choose $s_i \in \mathbb{F}_{p_i}$ such that $s_i \not\equiv r_i \pmod{p_i}$ and if $p_i = p_j$ then $s_i \equiv s_j \pmod{p_i}$ (for compatibility). Let m be the product of distinct p_i. By the Chinese Remainder Theorem a unique $s \in \mathbb{Z}/m\mathbb{Z}$ exists such that:

$$\forall i : \xi \equiv s_i \pmod{p_i} \iff \xi \equiv s \pmod{m}.$$

If we let the s_i vary over all $\mathbb{F}_{p_i} \setminus \{r_i\}$, then we have written (5.1) as a finite and non-empty union of arithmetic progressions of the form $\hat{s} + m\mathbb{Z}$ where $\hat{s}$ is an arbitrary lift of s from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}$.

Write $\mathbb{Q}_{(n)}$ for the set of all rationals with denominator n. Then (with a slight abuse of notation) the subset of all $\xi\mathbb{Z}$ such that ξ satisfies all the necessary conditions can be written as:

$$\Big(\{\xi \in \mathbb{Z} \mid \forall i : \xi \not\equiv r_i \pmod{p_i}\} \cap \{\xi \in \mathbb{Z} \mid \phi(X) \text{ is irreducible}\}\Big) \setminus n\pi(E'(\mathbb{Q}_{(n)}))$$

To see that $n\pi(E'(\mathbb{Q}_{(n)}))$ is finite, substitute $x = t = \xi/n$ in the Weierstraß equation (3.2) and multiply by n^6 to obtain:

$$(n^3y)^2 + (a_1'n^2)(n^2y)\xi + (a_3'n^5)\xi = \xi^3 + (a_2'n^2)\xi^2 + (a_4'n^4)\xi + (a_6'n^6).$$

This is again a Weierstraß equation (with coordinates $y' = n^3y$ and $x' = \xi$) for an elliptic curve and as such it has only finitely many integral points by Siegel's theorem ([14, Cor. 3.2.1, p. 248] with $S = M_{\mathbb{Q}}^{\infty}$). Hence there are only finitely many $\xi \in \mathbb{Z}$ such that $\xi/n \in \pi(E'(\mathbb{Q}))$, so certainly $n\pi(E'(\mathbb{Q}_{(n)}))$ is finite.

Since $n\pi(E'(\mathbb{Q}_{(n)}))$ is finite, we are done if we can prove that

$$\{\xi \in \mathbb{Z} \mid \forall i : \xi \not\equiv r_i \pmod{p_i}\} \cap \{\xi \in \mathbb{Z} \mid \phi(X) \text{ is irreducible}\}$$

is infinite. But from the discussion above, the left hand set is a finite, non-empty union of arithmetic progressions of the form $\xi = \hat{s} + m\zeta$. Recall that $\phi(X) \in \mathbb{Z}[\xi][X]$. But for any of these arithmetic progressions it is already true that there are infinitely many $\zeta \in \mathbb{Z}$ such that the evaluation of $\phi(X)$ at $\xi = \hat{s} + m\zeta$ is irreducible, by Hilbert's Irreducibility Theorem (cf. [7, Chapter 9, p. 225–]). ⊠

The condition that the equations for E and E' from Table 3.1 be globally minimal might seem a little restrictive, but is satisfied for "most" choices of parameters. More precisely:

Corollary 5.1.2 *Theorem 5.1.1 gives infinitely many families for each ℓ.*

PROOF. From [14, Remark 1.1, p. 172] we know that a Weierstraß equation with integral coefficients is globally minimal (over $\mathbb{Z}$) if and only if $v_p(\Delta) < 12$ or $v_p(c_4) < 4$ for all primes p. So, if Δ and c_4 are coprime, then the equation is globally minimal.

Table 5.2 contains the discriminants and c_4's for the Weierstraß equations of E_ℓ, E'_ℓ. Clearly it suffices to prove the Corollary for $\ell = 3$ with one of the two parameters taken constant, say $w = 1$.

Any common divisor of Δ and c_4 must also divide the resultant $\mathrm{Res}(\Delta, c_4)$, where Δ and c_4 are considered as as polynomials in the (remaining) parameter. We compute the resultants

and find that they are non-zero and only divisible by ℓ in each case. We also compute the roots in $\mathbb{F}_\ell$ of Δ in each case to find that the number of those is less than ℓ.

We can prohibit Δ being divisible by ℓ in the following manner. Let each root $x \in \mathbb{F}_p$ of Δ give a pair (x, p) and let $\{(x_i, p_i)\}$ be all such pairs. We are then looking at the following set (where $d = v$ is understood in case $\ell = 3$):

$$\{d \in \mathbb{Z} \mid d \not\equiv x_i \pmod{p_i}\}.$$

Note that the set of congruences is not degenerate because of the number of roots of $\Delta \mod \ell$. As in the proof of Theorem 5.1.1, this set is then a finite, non-empty union of arithmetic progressions. In particular: it is infinitely large, hence the number of families is infinite. ⊠

Remark 5.1.3 The condition that λ_t must be irreducible is computationally the hardest. It can be seen that there is a finite number of algebraic curves such that the rational points of those curves correspond to $t \in \mathbb{Q}$ for which λ_t becomes reducible. Thus, in general, we need to compute all the rational points on several algebraic curves, which is not always practical. Even when it is, it is not always possible to explicitly give all resulting t, e.g., when one of the curves is an elliptic curve with positive Mordell-Weil-rank. Restricting attention to integral t often makes things much easier.

Remark 5.1.4 Theorem 5.1.1 leaves some space for improvement, since it just relies on the quadratic point $P \in E'$ reducing nowhere singularly instead of the slightly more general condition *(ii)* of Theorem 4.1.5.

ℓ	$\Delta_\ell(t)$
3	$4t^3 + w^2t^2 - 18vwt - v(4w^3 + 27v)$
5	$4t^3 + (d^2 + 6d + 1)t^2 + 2d(10d^2 - 19d - 9)t +$
	$d(4d^4 - 40d^3 - 20d^2 - 59d - 4)$
7	$4t^3 + (d^4 - 6d^3 + 3d^2 + 2d + 1)t^2$
	$-2d(d-1)(10d^5 + 10d^4 - 61d^3 + 81d^2 - 59d + 10)t$
	$-d(d-1)(4d^9 + 36d^8 - 148d^7 + 280d^6 - 528d^5 + 843d^4 - 727d^3 + 304d^2 - 72d + 4)$

Table 5.1: Discriminant formulas coming from elliptic construction

	Δ	c_4
E_3	$v^3(w^3 - 27v)$	$w(w^3 - 24v)$
E_3'	$v(w^3 - 27v)^3$	$w(w^3 + 216v)$
E_5	$-d^5(d^2 + 11d - 1)$	$d^4 + 12d^3 + 14d^2 - 12d + 1$
E_5'	$-d(d^2 + 11d - 1)^5$	$d^4 - 228d^3 + 494d^2 + 228d + 1$
E_7	$d^7(d-1)^7(d^3 - 8d^2 + 5d + 1)$	$(d^2-d+1)(d^6-11d^5+30d^4-15d^3-10d^2+5d+1)$
E_7'	$d(d-1)(d^3 - 8d^2 + 5d + 1)^7$	$(d^2-d+1)(d^6+229d^5+270d^4-1695d^3+1430d^2-235d+1)$

Table 5.2: Discriminants and c_4's of the elliptic curves in Table 3.1

5.2 The infinitude of isomorphism classes within a family

It remains to show that, given a family of quadratic fields by means of a polynomial $F \in \mathbb{Z}[X]$ and a $S \subset \mathbb{Q}$, this family actually contains infinitely many isomorphism classes. We do this (in a general setting) by looking at the image of the discriminant polynomial $\Delta(t)$ in $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

The following result is adapted from [16].

Lemma 5.2.1 *Let $F \in \mathbb{Z}[X]$ be a non-constant, separable polynomial. Let S be an infinitely large set of integers. Then infinitely many prime numbers p exist for which there is an $n \in \mathbb{Z}$ such that p divides $F(n)$ exactly once.*

PROOF. First, discard the finitely many integral zeroes of $F(X)$ from S (if necessary). Then, note that

$$\{p \in \mathbb{Z} \text{ prime} \mid p \text{ divides } F(n) \text{ for some } n \in S\}$$

is an infinite set. For suppose it were finite and equal to, say, $\{p_1, \ldots, p_k\}$. Then for $N \gg 0$:

$$\begin{aligned} \#\{F(n) \mid |F(n)| \leq N, n \in S\} &\leq 1 + 2\#\{m = p_1^{e_1} \ldots p_k^{e_k} \mid m \leq N\} \\ &= 1 + 2\#\{e_i \in \mathbb{Z}_{\geq 0} \mid \sum e_i \log p_i \leq \log N\} \\ &\leq c_1 \cdot (\log N)^k, \end{aligned}$$

for some positive constant c_1, independent of N. But since F is a polynomial of degree $d = \deg F > 0$:

$$\#\{F(n) \mid |F(n)| \leq N\} \geq c_2 \cdot N^{1/d}$$

for some positive constant c_2, only depending on F and S. This yields a contradiction.

Now, let $\Delta \in \mathbb{Z}$ be the discriminant of F, which is non-zero by assumption. Suppose $p > 2$ is a prime such that $p \nmid \Delta$ and $p \mid F(n)$ for some $n \in S$. Taylor's theorem says that

$$F(n+p) = F(n) + pF'(n) + \frac{p^2}{2}F''(n) + p^3(\ldots)$$

so $F(n+p) \equiv pF'(n) \not\equiv 0 \bmod p^2$ by the choice of p and n. Hence $p \| F(n+p)$. ⊠

Corollary 5.2.2 *Let $F \in \mathbb{Z}[X]$ be a non-constant, separable polynomial. Let S be an infinitely large set of integers. Then the image of $F(S)$ in $\mathbb{Q}^*/\mathbb{Q}^{*2}$ is infinitely large.*

PROOF. Suppose that $F(S) \bmod \mathbb{Q}^{*2}$ is finite. Then there is a finite set N of square free integers such that $F(S) \bmod \mathbb{Q}^{*2} = N \bmod \mathbb{Q}^{*2}$. But then there are only a *finite* number of primes p such that for some integer $n \in S$ the prime p divides $F(n)$ an odd number of times. Lemma 5.2.1 now yields the desired contradiction. ⊠

Remark 5.2.3 It is possible to make this more quantitative, see e.g. [6].

Corollary 5.2.4 *The infinite family whose existence is ascertained by Theorem 5.1.1, contains infinitely many isomorphism classes.*

PROOF. We prove that this is already true for a family with t ranging over rationals with fixed denominator. Let $n \geq 1$ be an integer and let be S be a set of rationals with denominator n, such that $\mathbb{Q}(\sqrt{\Delta_\ell(t)})$, $t \in S$ gives an infinitude of quadratic number fields with class

number divisible by ℓ. Theorem 5.1.1 guarantees that S can be taken to be infinitely large. Now we would like to invoke Corollary 5.2.2 with $F(X) = n^3\Delta_\ell(X/n)$ which has integral coefficients. For this we need that $F(X)$ is separable and non-constant, which is equivalent to $\Delta_\ell(t)$ separable and non-constant.

It certainly is non-constant since $\Delta_\ell(t)$ is a polynomial of degree 3. If Δ_ℓ were inseparable, then it would follow from (3.3) that E' is singular, which it is not. ⊠

5.3 Some explicit families

We give a few explicit examples, one of which will be the family in §1.3.1.

Example 5.3.1 ($\ell = 3$) We choose $w = v = 1$.

$$\Delta = -26, \quad c_4 = -23;$$

$$\Delta' = -26^3, \quad c_4' = 7 \cdot 31.$$

Hence the equations for E and E' are globally minimal, since $\gcd(\Delta, c_4) = \gcd(\Delta', c_4') = 1$.

(i)
$$E' : \quad y^2 + xy + y = x^3 - 5x - 8.$$

This curve appears in the apecs-catalog and all rational points are known: $E'(\mathbb{Q}) = \{O, (4,4), (4,-9)\}$. So, we exclude $t = 4$.

(ii)
$$\lambda_t = x^3 - tx^2 + x + 1.$$

If we choose to have $T \subset \mathbb{Z}$, then we only have to check when λ_t has an integral root x. For that there are two possibilities, namely $x \mid 1$: $\lambda_t(1) = 3 - t$, $\lambda_t(-1) = -(1 + t)$. Hence we only have to exclude $t = -1$ and $t = 3$.

(iii) The singular point of E' mod 2 is $(1,0)$ and the singular point of E' mod 13 is $(4,4)$, thus:
$$t_2 \equiv 1 \pmod 2, \quad t_{13} \equiv 4 \pmod{13}.$$

If $t \in \mathbb{Z}$ such that $t \neq -1, 3, 4$ and

$$t \equiv 0, 2, 6, 8, 10, 12, 14, 16, 18, 20, 22 \text{ or } 24 \pmod{26},$$

then $\mathbb{Q}(\sqrt{\Delta(t)})$ has class number divisible by 3 where:

$$\Delta(t) = 4t^3 + t^2 - 18t - 31.$$

Example 5.3.2 ($\ell = 5$) We choose $d = 1$.

$$\Delta = -11, \quad c_4 = 2^4;$$

$$\Delta' = -11^5, \quad c_4' = 2^4 \cdot 31.$$

Thus the equations are globally minimal.

(i)

$$E' : \quad y^2 + 2xy + y = x^3 + x^2 - 10x - 30.$$

This is an aPecs-catalog curve as well and the Mordell-Weil-group (of rank 0) is known: $\pi(E'(\mathbb{Q})) = \{\infty, 4, 15\}$.

(ii)

$$\lambda_t = x^5 + (2-t)x^4 + (3-2t)x^3 + (6-t)x^2 + 4x + 1.$$

If we choose to have $T \subset \mathbb{Z}$ again, then we only have to exclude integers t for which *(1)* $\lambda_t(\pm 1) = 0$ or *(2)* (by Gauß' lemma) λ_t factors into a monic quadratic and monic cubic, both with integral coefficients. It turns out (see [2]) that no such t exist.

(iii) The singular point of E' mod 11 is $(4,1)$, so $t_{11} \equiv 4 \pmod{11}$.

If t is an integer such that $t \not\equiv 4 \pmod{11}$, then $\mathbb{Q}(\sqrt{\Delta(t)})$ has class number divisible by 5 where:

$$\Delta(t) = 4t^3 + 8t^2 - 36t - 119.$$

A minute computation shows that $\Delta(t+4) = 4t^3 + 56t^2 + 220t + 121$, which is formula (1.1) given by Granville (in the introduction).

Example 5.3.3 ($\ell = 7$) Choose $d = 2$.

$$\Delta = -2^7 \cdot 13, \quad c_4 = 3 \cdot 43,$$

$$\Delta' = -2 \cdot 13^7, \quad c_4' = 3 \cdot 41 \cdot 83.$$

Thus the Weierstraß equations are globally minimal.

(i)

$$E' : \quad y^2 - xy - 4y = x^3 - 4x^2 - 210x - 1050.$$

An aPecs-computation quickly reveals that $\pi(E'(\mathbb{Q})) = \{\infty\}$.

(ii)

$$\lambda_t = x^7 - (t+12)x^6 + 2(6t+47)x^5 - 4(13t+90)x^4 + 48(2t+11)x^3 + 64(3-t)x^2 - 1280x + 1024.$$

Some tedious but elementary calculations (see `family.7.2` on [2]) reveal that this polynomial is irreducible for every $t \in \mathbb{Z}$.

(iii) The singular point of E' mod 2 is $(0,0)$ and the singular point of E' mod 13 is $(9,0)$. Thus:

$$t_2 \equiv 0 \pmod{2}, \quad t_{13} \equiv 9 \pmod{13}.$$

If $t \in \mathbb{Z}$ such that

$$t \equiv 1, 3, 5, 7, 11, 13, 15, 17, 19, 21, 23 \text{ or } 25 \pmod{26},$$

then $\mathbb{Q}(\sqrt{\Delta(t)})$ has class number divisible by 7 where:

$$\Delta(t) = 4t^3 - 15t^2 - 832t - 4184.$$

5.4 Computations

Computations were done with the following mathematical software:

name	version	©	used for:
Maple	V release 5	Waterloo Inc.	factoring, solving Diophantine systems
aPecs	6	Ian Connell	computing with elliptic curves
Pari/GP	2.1.0	PARI Group	testing conjectures numerically

All necessary computations and data can be found at [2].

Chapter 6

Conclusions & remarks

6.1 The results

The main result is Theorem 5.1.1 where we prove that infinite families of quadratic number fields exist with class number divisible by $\ell = 3$, 5 or 7 such that all members are given as $\mathbb{Q}(\Delta(t))$ with $\Delta(t) \in \mathbb{Z}[t]$ a polynomial of degree 3 and $t \in T$, where T is a subset of the rational numbers which is often explicitly computable. In fact, in each case there is an infinite number of families (Corollary 5.1.2). It is also worth noting that the construction has no preference for either real or imaginary quadratic fields.

6.2 Further research

6.2.1 On the current result

One question immediately arises:

> Are all quadratic number fields with class number divisible by 3, 5 or 7 given by Theorem 5.1.1?

The answer is NO for several reasons:

1. We probably threw away many "good" quadratic fields because of the way ramification at finite places is avoided, cf. Remark 5.1.4 and §2.3 which provided only a necessary condition for ramification to occur.
2. The naive density of the family obtained is zero, while according to the Cohen-Lenstra heuristic (§1.1) the naive density of all quadratic fields with class number divisible by ℓ is positive.

6.2.2 On further results

It is natural to try and extend the results to other primes. Recall that the construction relied on the existence of elliptic curves defined over $\mathbb{Q}$ with a rational point of order $\ell = 3, 5$ or 7. We could try and achieve the same by considering an elliptic curve defined over $\mathbb{Q}$ with a rational (i.e. $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant) subgroup of prime order ℓ and dividing out by that subgroup. The facts from §3.2 describe precisely which ℓ are possible.

However, the resulting extensions of quadratic fields are not as simple as the extensions resulting from the current construction. In particular, the condition that the extensions be unramified will be harder to check and to satisfy.

Bibliography

[1] I. Connell, the Maple-package aPecs,
`http://www.math.mcgill.ca/connell/public/apecs/`.

[2] M. Boersma, electronic documents and files supporting this thesis,
`http://www.fmf.nl/~meinte/Thesis/`.

[3] J. Brinkhuis, *Normal integral bases and the Spiegelungssatz of Scholz*, Acta Arith. 69 (1995), p. 1–9.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM **138** (1993), Springer-Verlag.

[5] H. Cohen and H.W. Lenstra, *Heuristics on class groups of number fields*, Number Theory, Noordwijkerhout 1983, LN in Math. **1068**, Springer-Verlag (1984), p. 33–62.

[6] P. Cutter, A. Granville and Th.J. Tucker, *The number of fields generated by the square root of values of a given polynomial*, to appear in the Canadian Mathematical Bulletin.

[7] S. Lang, *Fundamentals of diophantine geometry*, Springer-Verlag (1983).

[8] R. Kloosterman, *Elliptic curves with large Selmer groups*, Master's Thesis in Mathematics, R*u*G (2001).

[9] D.S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, p. 193–237.

[10] B. Mazur, *Rational Isogenies of Prime Degree*, Inventiones Mathematica **44** (1978), p. 129–162.

[11] J.F. Mestre, *Courbes Elliptiques et Groupes de Classes d'Idéaux de Certains Corps Quadratiques*, Sém. de Théorie des Nombres, Bordeaux, Exp. **15** (1979/1980).

[12] R. Schoof, *Class groups of complex quadratic fields*, in *Elliptic curves and class groups*, Ph. D.-thesis (1985).

[13] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press (1986).

[14] J. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106** (1992), Springer-Verlag.

[15] H.P.F. Swinnerton-Dyer, *A Brief Guide to Algebraic Number Theory*, LMSST **50** (2001), Cambridge University Press.

[16] J. Top, *A remark on the rank of jacobians of hyperelliptic curves over $\mathbb{Q}$ over certain elementary Abelian 2-extensions*, Tôhoku Mathematical Journal, 2nd series, vol. **40**, no. 4 (1988), p. 613–616.

[17] J. Vélu, *Isogénies entre courbes elliptiques*, C.R. Académy Science Paris **273** (1971), p. 238–241.

Acknowledgements

First of all I'd like to thank Jaap Top: my (patient) teacher for many years and supervisor for many months.

I also want to thank Ineke Kruizinga-Huisman warmly for the years of mental support[1], gezelligheid and of course: coffee!

Thanks go to Gert-Jan van der Heiden for reviewing a draft version of this Thesis.

Last but certainly not least, I want to thank my parents Thijs en Margriet and my sister Atsje for all their support, both in the financial and mental coaching area.

[1] "Studeren?! Zit dat er in dan, jongen?" Blijkbaar wel! :-)