A. M. Viergever

Two cases of Fermat's Last Theorem using descent on elliptic curves

Bachelor thesis

22 June 2018

Thesis supervisor: dr. R.M. van Luijk

Leiden University
Mathematical Institute

Contents

Introduction

In this thesis, we will consider two special cases of a very famous theorem which has a long history, and analyze them geometrically using elliptic curves. Let $n \in \mathbb{Z}_{\geq 1}$ and consider the equation

$$x^n + y^n = z^n \tag{1}$$

of which we are looking for integer solutions. For $n = 1$, this is trivial, and for $n = 2$, it turns out that there are infinitely many solutions.

The case $n = 2$

An integer solution $(x, y, z) \in \mathbb{Z}^3$ to the equation $x^2 + y^2 = z^2$ is called a *Pythagorean triple*. We say that it is *primitive* if $\gcd(x, y, z) = 1$. Note that if $(x, y, z) \in \mathbb{Z}^3$ is a Pythagorean triple, we have for all $\lambda \in \mathbb{Z}$ that $(\lambda x, \lambda y, \lambda z)$ is also a Pythagorean triple. So once we know that, for example, $(3, 4, 5)$ is an integer solution to equation (1), we have immediately proved that there are infinitely many Pythagorean triples.
However, there is also a more geometric way to show this, and actually even more: we will show that there exist infinitely many *primitive* Pythagorean triples. Note that finding a solution in co-prime integers to the equation $x^2 + y^2 = z^2$ is, since we can assume that $z \neq 0$ (for $(0, 0, 0)$ is not primitive), equivalent to finding a rational solution to the equation

$$x^2 + y^2 = 1 \tag{2}$$

i.e. to finding a rational point on the unit circle in $\mathbb{R}^2$. Now, let $t \in \mathbb{Q}$ be a rational number and consider the line given by $y = tx + t$, which intersects the unit circle in $(-1, 0)$ and exactly one other point. This point is of the form $(x, tx + t)$, for some $x \in \mathbb{Q}$ which we can find by solving the equation

$$x^2 + (tx + t)^2 = 1 \text{ so } (1 + t^2)x^2 + 2t^2x + t^2 - 1 = 0.$$

As we already knew, $x = -1$ is a solution, and we find that the x-coordinate of the other point where the line intersects the unit circle is $x = \frac{1-t^2}{1+t^2}$.
This defines a map ϕ from $\mathbb{Q}$ to set of the rational solutions of (2), given by

$$\phi \colon \mathbb{Q} \to \{(x, y) \in \mathbb{Q}^2 : x^2 + y^2 = 1\} \setminus \{(-1, 0)\}, t \mapsto \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right).$$

On the other hand, if we have a rational solution (x_0, y_0) to (2), we take the line L from $(-1, 0)$ to (x_0, y_0), which is given by $y = \frac{y_0}{x_0+1}x + \frac{y_0}{x_0+1}$ and intersects the y-axis in the point $(0, \frac{y_0}{x_0+1})$. This gives a map

$$\psi \colon \{(x, y) \in \mathbb{Q}^2 : x^2 + y^2 = 1\} \setminus \{(-1, 0)\} \to \mathbb{Q}, (x, y) \mapsto \frac{y}{x + 1}$$

and it can easily be checked that ψ provides an inverse for ϕ, which shows that ϕ is a bijection. We find that the set of rational solutions of equation (2) can be parametrized by $\mathbb{Q}$.

The case $n \geq 3$

For $n \geq 3$, we can still find some "trivial solutions" to equation (1), for example $(1, 0, 1)$ and $(0, 1, 1)$. However, it is a very famous result that there are no nontrivial solutions.

Theorem 0.0.1 (Fermat's Last Theorem)**.** *For $n \geq 3$, equation (1) has no integer solutions $(x, y, z) \in \mathbb{Z}^3$ satisfying $xyz \neq 0$.*

This theorem has been named after Pierre de Fermat, a French nobleman born in 1601 with a lifelong interest in mathematics. He read a version of Diophantus's "Arithmetica", and wrote down some of his own conjectures in the margins of the book, including Theorem 0.0.1. Fermat claimed that he had a proof, but that the margins were, unfortunately, too small to write it down. Later on, all margin-conjectures of Fermat had been proven, but even after 350 years, nobody had managed to prove Theorem 0.0.1. It therefore became known as "Fermat's Last Theorem".
Finally, in 1994, Theorem 0.0.1 has been proven by the British mathematician Andrew Wiles [Wil95], who — after working in isolation for seven years — found a brilliant proof which has been called "the proof of the century"[1].

Structure and goal of this thesis

Wiles' proof is far too difficult to treat in this thesis, but for many special cases of Theorem 0.0.1, easier proofs had already been discovered before the general case had been established. The case $n = 4$, for example, is the only one of which we know a proof by Fermat himself, and the case $n = 3$ has been proven by Euler in 1770 (we will give versions of those proofs in Section 2.1 and Section 3.1, respectively). Both of those proofs come down to the principle of infinite descent. The key idea of this method is that whenever we have a solution $(x, y, z) \in \mathbb{Z}^3$ to equation (1) (for $n = 3$ or $n = 4$) satisfying $xyz \neq 0$, we can find another solution $(u, v, w) \in \mathbb{Z}^3$ satisfying $uvw \neq 0$ with $|u| < |x|, |v| < |y|$ and $|w| < |z|$. Since this can never be the case when working with positive integers, we have a contradiction, so we conclude that there are no nontrivial solutions at all. This method has been the inspiration for the method of descent by an isogeny for elliptic curves, which can be used to prove special cases of the Weak Mordell–Weil Theorem.
In this thesis, we will relate the classical proofs for the cases $n = 3$ and $n = 4$ of Fermat's Last Theorem to a descent by 2- and 3-isogeny on elliptic curves. This will provide a geometric explanation for the fact that there are no nontrivial solutions. Chapter 1 will summarize some of the definitions and theorems which will be used. In Chapter 2, the case $n = 4$ is analyzed, whereas Chapter 3 is devoted to the case $n = 3$.

[1] By John Conway, who was interviewed about Wiles' achievement in the documentary "The proof" produced by BBC in 1997.

Chapter 1

Some important theorems and definitions

This chapter will introduce some of the notation, definitions and theorems which will be used in the rest of this thesis. We will need some background knowledge about elliptic curves, which can be found in Chapter 1 till 3 from [Sil09] (of which we also adopt most of our notation). In Section 1.1, we will highlight some theorems, notations and definitions which we will use very often. Section 1.2 will introduce the method descent by 2-isogeny on elliptic curves, and Section 1.3 is devoted to the method of descent by 3-isogeny.

1.1 Often used notation, definitions and theorems

Let $n \in \mathbb{Z}_{\geq 1}$ and choose an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. We will denote $\mathbb{A}^n$ for the affine n-space over $\overline{\mathbb{Q}}$ and $\mathbb{P}^n$ for the n-dimensional projective space over $\overline{\mathbb{Q}}$. Furthermore, we will need the following definition in Chapter 2.

Definition 1.1.1. Let $w_0, ..., w_n \in \mathbb{Z}_{\geq 1}$ be integers. We define the *weighted projective space* $\mathbb{P}(w_0, ..., w_n)$ over $\overline{\mathbb{Q}}$ to be the set of equivalence classes of $\mathbb{A}^{n+1} \setminus \{(0, 0, ..., 0)\}$ under the relation $\sim$ defined by $(a_0, ..., a_n) \sim (a'_0, ..., a'_n)$ if and only if there exists some $\lambda \in \overline{\mathbb{Q}}^*$ such that $\lambda^{w_i} a_i = a'_i$ for all $i \in \{0, ..., n\}$.

The notions of torsion points and dual isogenies will be of great interest to us, so we will briefly recall them. Let $(E_1, \mathcal{O})$ and $(E_2, \mathcal{O}')$ be elliptic curves over $\mathbb{Q}$. Then for $m \in \mathbb{Z}$, we have the *multiplication by m map* $[m] \colon E_1 \to E_1$ defined by

$$[m] \colon E_1 \to E_1, P \mapsto \begin{cases} \overbrace{P + P + \cdots + P}^{m \text{ times}} & \text{if } m \geq 1 \\ -\underbrace{(P + P + \cdots + P)}_{-m \text{ times}} & \text{if } m \leq -1 \\ \mathcal{O} & \text{otherwise} \end{cases}.$$

Since $[m](\mathcal{O}) = \mathcal{O}$, we have that $[m]$ is an endomorphism of E_1. Identifying E_1 with its set of points over $\overline{\mathbb{Q}}$, we denote the set of *m-torsion points of* E_1 by $E_1[m] = \{P \in E_1 : [m]P = \mathcal{O}\}$

and its *torsion subgroup* by $(E_1)_{\text{tors}} = \bigcup_{m\geq 1} E_1[m]$. By Corollary 6.4 of [Sil09], if $m \neq 0$, we have that $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$ (we use here that we will only work over $\mathbb{Q}$, which is of characteristic zero). In particular, the number of m-torsion points of E_1 over $\overline{\mathbb{Q}}$ is equal to m^2.
Now, let $\phi\colon E_1 \to E_2$ be a non-constant isogeny, then by Theorem 6.1 of [Sil09], there is a unique isogeny $\hat{\phi}\colon E_2 \to E_1$ such that $\hat{\phi}\circ\phi = [\deg(\phi)]$. This isogeny $\hat{\phi}$ is called the *dual* of ϕ. By Theorem 6.2 of [Sil09], we have that

$$\phi \circ \hat{\phi} = [\deg(\phi)], \deg(\hat{\phi}) = \deg(\phi) \text{ and } \hat{\hat{\phi}} = \phi.$$

Further, denote the automorphism group of E_1 over $\overline{\mathbb{Q}}$ by $\mathrm{Aut}(E_1)$. In Sections 2.2 and 3.2, we will need the following result, which is Corollary 10.2 of [Sil09].

Proposition 1.1.2. *The automorphism group of E_1 is a finite group, which has order 4 if the j-invariant of E_1 equals 1728, order 6 if the j-invariant of E_1 equals 0, and order 2 otherwise.*

In order to state another important result which we will use, we first need the following definition.

Definition 1.1.3. Let C and C' be curves. A *birational map* is a rational map $C \to C'$ admitting an inverse which is also a rational map. If there exists a birational map $C \to C'$, we say that C and C' are *birationally equivalent*.

In the final sections of both Chapter 2 and 3, we will need some advanced result, which is, for algebraically closed fields, Corollary I.6.11 of [Har77] (proof of which follows from Propositions I.6.7–I.6.9). The fact that this theorem is also true for general fields, follows from Proposition 2.6 of [Sta18, Algebraic Curves].

Theorem 1.1.4. *Let C be a curve over $\mathbb{Q}$, then there exists a smooth projective curve $\overline{C}$ over $\mathbb{Q}$ such that C and $\overline{C}$ are birationally equivalent, and $\overline{C}$ is unique up to isomorphism over $\overline{\mathbb{Q}}$. Furthermore, let D be a projective variety, and let $\phi\colon C \to D$ be a rational map. Then ϕ induces a morphism $\overline{\phi}\colon \overline{C} \to D$.*

1.2 Descent by 2-isogeny

We will now describe the procedure of descent by 2-isogeny on an elliptic curve, which will be one of the main subjects of this thesis. In our description of it, we will be following [Bri15], which is, in turn, following [Cas91]. We will not prove the lemmas stated in this section, but they can be found in those sources.
The statement that for an elliptic curve E over a number field K we have that $E(K)/2E(K)$ is finite is called the *Weak Mordell–Weil Theorem*, and descent by 2-isogeny is a way to prove it over $\mathbb{Q}$, in case that the elliptic curve has a nontrivial rational 2-torsion point. So let $(E, \mathcal{O})$ be an elliptic curve over $\mathbb{Q}$ which has a rational 2-torsion point other than $\mathcal{O}$. Then, by making some translations over $\mathbb{Q}$, we find that E can be given by a Weierstrass equation

$$E : y^2 = x(x^2 + ax + b)$$

with $a, b \in \mathbb{Z}$, which has the rational 2-torsion point $(0,0)$. Since E is smooth, the polynomial on the left hand side is separable, so we have that $b \neq 0$ and $a^2 - 4b \neq 0$.

Lemma 1.2.1. *Consider the second elliptic curve $(E', \mathcal{O}')$ over $\mathbb{Q}$ given by the equation $E' : v^2 = u(u^2 + a'u + b')$, where $a' = -2a$ and $b' = a^2 - 4b$, and the isogeny*

$$\phi\colon E \to E', (x,y) \mapsto \begin{cases} (x + a + \frac{b}{x}, y - \frac{by}{x^2}) & \text{if } x \neq 0 \\ \mathcal{O}' & \text{otherwise} \end{cases}$$

then $\ker(\phi) = \{\mathcal{O}, (0,0)\}$.

Note that E' is indeed an elliptic curve, since we have that $b' = a^2 - 4b \neq 0$ and also that $a'^2 - 4b' = 4a^2 - 4a^2 + 16b = 16b \neq 0$, which implies that it is smooth. Lemma 1.2.1 also tells us that ϕ is of degree two.
Using Lemma 1.2.1 again on E' yields an elliptic curve $E'' : y^2 = x(x^2 + 4ax + 16b)$ which is isomorphic to E (by $E \to E'', (x,y) \to (4x, 8y)$), and an isogeny

$$\hat{\phi}\colon E' \to E, (u,v) \mapsto \begin{cases} (\frac{1}{4}(u + a' + \frac{b'}{u}), \frac{1}{8}(y - \frac{b'y}{x^2})) & \text{if } u \neq 0 \\ \mathcal{O} & \text{otherwise} \end{cases}$$

satisfying $\ker(\hat{\phi}) = \{\mathcal{O}', (0,0)\}$. The slight abuse of notation already hints towards the following lemma.

Lemma 1.2.2. *The isogeny $\hat{\phi}$ is the dual of ϕ.*

In other words, $\hat{\phi} \circ \phi = [2]$ on E.

Lemma 1.2.3. *Define the map*

$$q\colon E'(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2, (u,v) \mapsto \begin{cases} [u] & \text{if } u \neq 0 \\ [b'] & \text{if } u = 0 \end{cases}$$

and $q(\mathcal{O}) = [1]$. Then q is a homomorphism of groups and the sequence

$$E(\mathbb{Q}) \xrightarrow{\phi} E'(\mathbb{Q}) \xrightarrow{q} \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

is exact. Furthermore, let $r \in \mathbb{Z}$ be square-free, then we have that $[r] \in \mathrm{im}(q)$ if and only if the equation $r^2l^4 + a'rl^2m^2 + b'm^4 = rn^2$ has a solution $(l,m,n) \in \mathbb{Z}^3 \setminus \{(0,0,0)\}$. This can only happen if r divides b'.

It follows that $\mathrm{im}(q)$ is finite, since there are only finitely many $r \in \mathbb{Z}$ dividing b'. Furthermore, by the Isomorphism Theorem we have that $\mathrm{im}(q) \cong E'(\mathbb{Q})/\ker(q) = E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ is finite. Repeating the procedure on E' yields that $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$ is also finite.
We will now, and also often later, need the following tool from homological algebra.

Lemma 1.2.4 (Kernel-cokernel sequence)**.** *Let A, B and C be abelian groups and $f\colon A \to B$ and $g\colon B \to C$ group homomorphisms. Let $i_1 : \ker(f) \to \ker(g \circ f)$ be the natural inclusion map, let $i_2 : \ker(g) \to coker(f)$ be the restriction of the natural quotient map $B \to coker(f)$ and let $i_3 : coker(g \circ f) \to coker(g)$ be the natural quotient map. Then the sequence*

$$0 \to \ker(f) \xrightarrow{i_1} \ker(g \circ f) \xrightarrow{f} \ker(g) \xrightarrow{i_2} \operatorname{coker}(f) \xrightarrow{g} \operatorname{coker}(g \circ f) \xrightarrow{i_3} \operatorname{coker}(g) \to 0$$

is exact.

So if we denote $E(\mathbb{Q})[2]$ for the rational 2-torsion points of E, the sequence

$$0 \to \ker(\phi) \to E(\mathbb{Q})[2] \to \ker(\hat{\phi}) \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to E(\mathbb{Q})/2E(\mathbb{Q}) \to E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \to 0$$

is exact, from which it follows that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. This proves the Weak Mordell–Weil Theorem, which can be used to prove the "strong" Mordell–Weil Theorem.

Theorem 1.2.5 (Mordell–Weil)**.** *Let E be an elliptic curve over a number field K. Then $E(K)$ is a finitely generated abelian group.*

By the Structure Theorem of abelian groups, we have that $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$ for some $r \in \mathbb{Z}_{\geq 0}$, which is called the *rank* of E. We will now show how the method of descent by 2-isogeny can be used to find this rank. We need the following two lemmas.

Lemma 1.2.6. *Let A be a finite abelian group and denote $A[2]$ for its 2-torsion subgroup, then $\#(A/2A) = \#A[2]$.*

Proof. We have that $A \to A, x \mapsto 2x$ is a group homomorphism with image $2A$ and kernel $A[2]$, so by the Isomorphism Theorem, $2A \cong A/A[2]$, which implies that

$$\#(2A) = \#(A/A[2]) = \frac{\#A}{\#A[2]}$$

so $\#(A/2A) = \#A[2]$. □

Lemma 1.2.7. *The cardinality of $E(\mathbb{Q})/2E(\mathbb{Q})$ equals $\#coker(\phi) \cdot \#coker(\hat{\phi})$ if and only if b' is a square, and $\frac{1}{2} \cdot \#coker(\phi) \cdot \#coker(\hat{\phi})$ otherwise.*

Proof. From the kernel-cokernel sequence in Lemma 1.2.4, we see that the sequence

$$0 \to \ker(\hat{\phi})/\phi(E(\mathbb{Q})[2]) \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to E(\mathbb{Q})/2E(\mathbb{Q}) \to E(\mathbb{Q})/\hat{\phi}(E(\mathbb{Q})) \to 0$$

is also exact.This implies that

$$\#\left(E(\mathbb{Q})/2E(\mathbb{Q})\right) = \frac{\#(E'(\mathbb{Q})/\phi(E(\mathbb{Q}))) \cdot \#(E(\mathbb{Q})/\hat{\phi}(E(\mathbb{Q})))}{\#(\ker(\hat{\phi})/\phi(E(\mathbb{Q})[2]))}.$$

We know that E has four 2-torsion points over $\overline{\mathbb{Q}}$. The isogeny ϕ maps $(0,0)$ and $\mathcal{O}$ to $\mathcal{O}'$, so it sends the two remaining 2-torsion points to $(0,0)$ (by the kernel of $\hat{\phi}$). So $\#(\ker(\hat{\phi})/\phi(E(\mathbb{Q}))[2])$ equals 2 if E has no other rational 2-torsion points than $(0,0)$ and $\mathcal{O}$, and 1 otherwise. Therefore, $\#\left(E(\mathbb{Q})/2E(\mathbb{Q})\right)$ equals $\#\text{coker}(\phi) \cdot \#\text{coker}(\hat{\phi})$ if and only if $(0,0) \in \phi(E(\mathbb{Q}))$, so if and only if E has four rational 2-torsion points, which is the case if and only if b' is a square. In the same way, $\#\left(E(\mathbb{Q})/2E(\mathbb{Q})\right)$ equals $\frac{1}{2} \cdot \#\text{coker}(\phi) \cdot \#\text{coker}(\hat{\phi})$ if and only if $(0,0) \notin \phi(E(\mathbb{Q}))$, so if and only if E has precisely two rational 2-torsion points, which is the case if and only if b' is not a square. □

The method of descent by 2-isogeny can be used to find $\#\text{coker}(\phi)$ and $\#\text{coker}(\hat{\phi})$, from which we can compute the cardinality of $E(\mathbb{Q})/2E(\mathbb{Q})$ using Lemma 1.2.7. Note that

$$E(\mathbb{Q})/2E(\mathbb{Q}) = (E(\mathbb{Q})_{\text{tors}}/2E(\mathbb{Q})_{\text{tors}}) \oplus (\mathbb{Z}/2\mathbb{Z})^r .$$

Since the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is finite, we can apply Lemma 1.2.6 to it, then we have that $\#\left(E(\mathbb{Q})_{\text{tors}}/2E(\mathbb{Q})_{\text{tors}}\right) = \#E(\mathbb{Q})[2]$. We can therefore compute the rank r of $E(\mathbb{Q})$ if we know the cardinality of the 2-torsion subgroup. This can be retrieved by observing that E has four rational 2-torsion points if and only if b' is a square, and two otherwise.

1.3 Descent by 3-isogeny

Analogous to descent by 2-isogeny, there is also a method of descent by 3-isogeny, which we will summarize following [Coh07], to which we also redirect for proofs of the stated lemmas. Let E be an elliptic curve over $\mathbb{Q}$ given by the equation

$$E : y^2 = x^3 + d(ax + b)^2$$

where $a, b, d \in \mathbb{Q}$ are such that $b \neq 0, d \neq 0$ and $27b - 4a^3d \neq 0$ (this will ensure that E is smooth again, since the discriminant of E equals $16d^2b^3(27b - 4a^3d)$). Let $\delta \in \overline{\mathbb{Q}}^*$ be such that $\delta^2 = d$. Then one can check that $(0, b\delta)$ is a 3-torsion point, so it generates a subgroup of E of order 3 which is stable under $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (note that this need not be a group generated by a rational 3-torsion point).

Lemma 1.3.1. *Consider the second elliptic curve E' given by*

$$v^2 = u^3 + d'(a'u + b')^2$$

where $a' = a$, $b' = \frac{27b-4a^3d}{9}$ and $d' = -3d$. Then the isogeny $\phi\colon E \to E'$ given by

$$(x, y) \mapsto \begin{cases} \left(\frac{x^3+4d((a^2/3)x^2+abx+b^2)}{x^2}, \frac{y(x^3-4bd(ax+2b))}{x^3}\right) & \text{if } x \neq 0 \\ \mathcal{O}' & \text{otherwise} \end{cases}$$

satisfies $\ker(\phi) = \{\mathcal{O}, (0, b\delta), (0, -b\delta)\}$.

It follows that $\deg(\phi) = 3$. Let $\delta' \in \overline{\mathbb{Q}}^*$ be such that $\delta'^2 = d'$. Using Lemma 1.3.1 again on E', we get a third elliptic curve E'' with $a'' = a, b'' = 3(27b - 4a^3d) + 12a^3d = 9b$ and $d'' = 9d$, which is isomorphic to E (by $E \to E'', (x, y) \mapsto (9x, 27y)$). Furthermore, we get a second isogeny $\hat{\phi}\colon E \to E'$ given by

$$(u, v) \mapsto \begin{cases} \left(\frac{u^3+4d'((a'^2/3)u^2+a'b'u+b'^2)}{9u^2}, \frac{v(u^3-4b'd'(a'u+2b'))}{27u^3}\right) & \text{if } u \neq 0 \\ \mathcal{O} & \text{otherwise} \end{cases}$$

and $\hat{\phi}(\mathcal{O}') = \mathcal{O}$ satisfying $\ker(\hat{\phi}) = \{\mathcal{O}', (0, b'\delta'), (0, -b'\delta')\}$. As the slight abuse of notation already indicates, these isogenies are dual.

Lemma 1.3.2. *The isogeny $\hat{\phi} \circ \phi$ is multiplication by 3 on E.*

We now set $K_{d'} = \mathbb{Q}(\delta')$ and define the 3-descent map $q\colon E'(\mathbb{Q}) \to K_{d'}^*/(K_{d'}^*)^3$ by

$$(u, v) \mapsto \begin{cases} [v - (a'u + b')\delta'] & \text{if } u \neq 0 \\ [2b'\delta'] & \text{otherwise} \end{cases}$$

and $q(\mathcal{O}') = [1]$.

Lemma 1.3.3. *The map q is a homomorphism of groups, and the sequence*

$$E(\mathbb{Q}) \xrightarrow{\phi} E'(\mathbb{Q}) \xrightarrow{q} K_{d'}^*/(K_{d'}^*)^3$$

is exact.

A proof that the image of q is finite is given in [vB10]. One can then use the kernel-cokernel sequence again to deduce that $E(\mathbb{Q})/3E(\mathbb{Q})$ is finite.
If $d' \notin (\mathbb{Q}^*)^2$, an extra complexity arises in working with the field $K_{d'}$ instead of $\mathbb{Q}$. The following proposition proved by Cohen will turn out to be useful.

Proposition 1.3.4. *If $d' \notin \mathbb{Q}^2$, the image of q is contained in the subset of $K_{d'}^*/(K_{d'}^*)^3$ consisting of all elements of which the norm is trivial in $\mathbb{Q}^*/(\mathbb{Q}^*)^3$.*

In Chapter 3, we will need a bit of algebraic number theory. In particular, we will use the notion of the *ring of integers* $\mathcal{O}(K_{d'})$ of $K_{d'}$, which is defined as

$$\mathcal{O}(K_{d'}) = \{x \in K_{d'} : \text{ the minimum polynomial of } x \text{ over } \mathbb{Q} \text{ has coefficients in } \mathbb{Z}\}.$$

By Exercise 1.15 of [Ste17], if d' is square-free, we have that $\mathcal{O}(K_{d'}) = \mathbb{Z}[\frac{1+\delta'}{2}]$ if $d' \equiv 1$ modulo 4, and $\mathcal{O}(K_{d'}) = \mathbb{Z}[\delta']$ otherwise. By Exercise 1.23, the ring $\mathcal{O}(K_{-3})$ is a principal ideal domain, as we will need in Section 3.2.

Chapter 2

The case $n = 4$

For $n = 4$, a proof of Fermat's Last Theorem was given by Fermat himself [Fer91]. We will give a version of it in Section 2.1. In Section 2.2, we will relate the standard proof to a descent by 2-isogeny. Then in Section 2.3, we will work out a version of the descent by 2-isogeny method on elliptic curves of a certain form, which "look like the Fermat curve". Finally, in Section 2.4, we will view the method of descent by 2-isogeny from a different perspective.

2.1 The standard proof

In giving this proof, we will follow [Bri15].

Theorem 2.1.1 (Fermat, $n = 4$)**.** *The equation $x^4 + y^4 = z^4$ has no solutions $(x, y, z) \in \mathbb{Z}^3$ with $xyz \neq 0$.*

Proof. Suppose that $(x, y, z) \in \mathbb{Z}^3$ is a solution satisfying $xyz \neq 0$, then $x^4 + y^4 = (z^2)^2$ so (x, y, z^2) is a nontrivial solution to the equation

$$x^4 + y^4 = z^2 \tag{2.1}$$

which implies that it suffices to prove that (2.1) has no nontrivial solutions.
Suppose that $(x, y, z) \in \mathbb{Z}^3$ is a solution to (2.1) with $xyz \neq 0$ and $\max\{|x|, |y|\}$ minimal, then x, y, z may be assumed to be co-prime (for if a prime p would divide x, y and z, we can see from equation (2.1) that p^2 divides z and then $(\frac{x}{p}, \frac{y}{p}, \frac{z}{p^2})$ is also a solution, contradicting the minimality of $\max\{|x|, |y|\}$), and even pairwise co-prime (looking at (2.1), every prime dividing two of the variables must also divide the third). Considering the equation modulo 4 (where every square is equal to either 0 or 1) we see that x and y cannot both be odd, so without loss of generality, we may assume that x is even and y is odd, so z is also odd.
We now factor the equation as $x^4 = (z + y^2)(z - y^2)$. Note that if a prime p divides both factors on the right hand side, it also divides $(z + y^2) + (z - y^2) = 2z$, and since it cannot divide z (then it would also divide $(z + y^2) - z = y^2$ and therefore z and y would not be co-prime, producing a contradiction) we have $p = 2$. So $\gcd(z + y^2, z - y^2) \in \{1, 2\}$. Now, note that since y^2 and z are both odd, we have that either $z + y^2$ or $z - y^2$ is a multiple of 4 and the other one is not (otherwise, we arrive at a contradiction modulo 4). Since x^4 is a multiple of 16, there are two possibilities:

- There are positive integers u and v such that $z + y^2 = 8u^4$ and $z - y^2 = 2v^4$, where v is odd.
- There are positive integers u and v such that $z + y^2 = 2u^4$ and $z - y^2 = 8v^4$, where u is odd.

However, if we look at the first option and eliminate z we get $y^2 = 4u^4 - v^4$, so $y^2 \equiv -1$ modulo 4, which is impossible. So the second possibility holds. We can eliminate z again to get $y^2 = u^4 - 4v^4$. We can factorize this equation as $4v^4 = (u^2 + y)(u^2 - y)$, then since y and u are odd, we have again that both $u^2 + y$ and $u^2 - y$ are even. Since at least one of $u^2 + y$ and $u^2 - y$ is positive, this yields that there are positive integers s and r such that $u^2 + y = 2r^4$ and $u^2 - y = 2s^4$, so $r^4 + s^4 = u^2$. Thus, we have found a new solution $(r, s, u) \in \mathbb{Z}^3$ to (2.1), where

$$x^4 = (z - y^2)(z + y^2) = 16u^4v^4 = 4u^4(u^2 + y)(u^2 - y) = 16u^4r^4s^4$$

which implies that r and s are nonzero and furthermore, that $|r| < |x|$, which is a contradiction. So (2.1) has no nontrivial solutions in integers, which implies that neither has the equation $x^4 + y^4 = z^4$. □

2.2 Descent by 2-isogeny

Looking more closely at the proof given above, we have two curves:

$$C : X^4 + Y^4 = Z^2 \text{ and } C' : U^4 - 4V^4 = W^2$$

over $\mathbb{Q}$, in the weighted projective plane $\mathbb{P}(1, 1, 2)$ over $\overline{\mathbb{Q}}$, together with two rational maps:

$$\psi \colon C \to C', [X : Y : Z] \mapsto [Z : -XY : X^4 - Y^4]$$

and

$$\hat{\psi} \colon C' \to C, [U : V : W] \mapsto [2UV : W : U^4 + 4V^4].$$

In Section 2.2.1, we will show that C and C' are elliptic curves, and that ψ and $\hat{\psi}$ are isogenies. (Note that apparently, we slightly abuse the notation for the dual, but later on, we will show that $\hat{\psi}$ is really the dual of ψ.) Then in Section 2.2.2, we can apply the method of descent by 2-isogeny described in Section 1.2 to C and C'. In Section 2.2.3, we will relate this to the classical proof in Section 2.1, to show that the infinite descent in this proof actually comes down to a descent on elliptic curves. Finally in Section 2.2.4, we will say some words on the automorphisms of C.

2.2.1 C and C' are elliptic curves

We will show now that C and C' are elliptic curves.

Proposition 2.2.1. *Let $t \in \mathbb{Z} \setminus \{0\}$ be a nonzero integer and let C_t be the curve over $\mathbb{Q}$ in the weighted projective plane $\mathbb{P}(1, 1, 2)$ given by the equation $Z^2 = X^4 + tY^4$, together with the rational point $\mathcal{O} = [1 : 0 : 1]$. Then $(C_t, \mathcal{O})$ is an elliptic curve.*

Proof. First, we show that C_t is smooth. Let $P = [a : b : c] \in C_t$ and suppose $a \neq 0$. Then we consider the affine patch $1 + ty^4 = z^2$, where $y = \frac{Y}{X}$ and $z = \frac{Z}{X^2}$. Defining $g(x, y) = 1 + ty^4 - z^2$, we have that $\frac{\partial g}{\partial y}(P) = \frac{4tb^3}{a^3}$ and $\frac{\partial g}{\partial z}(P) = -\frac{2c}{a}$ so C_t can only be singular at P if $b = c = 0$, but the equation of C_t shows that such points are not on the curve. Now, suppose $a = 0$, then $b \neq 0$, so we consider the affine part $u^4 + t = w^2$, where $u = \frac{X}{Y}$ and $w = \frac{Z}{Y^2}$. Denote $h(u, w) = u^4 + t - w^2$ then $\frac{\partial h}{\partial u}(P) = \frac{4a^3}{b^3} = 0$ and $\frac{\partial h}{\partial w}(P) = -\frac{2c}{b}$, and since the equation of C_t shows that $c \neq 0$, we conclude that C_t is smooth.
It remains to show that C_t has genus 1. Therefore, we go to the affine patch $1 + ty^4 = z^2$ with coordinates $y = \frac{Y}{X}$ and $z = \frac{Z}{X^2}$ again and consider the maximal ideal

$$\mathcal{M} = \{f \in \overline{\mathbb{Q}}[C_t] : f(0, 1) = 0\} \subset \overline{\mathbb{Q}}[C_t]$$

for the point $(0, 1)$, which is generated by y and $z - 1$. Localizing in this ideal, we find the local ring

$$\mathcal{R}_{\mathcal{O}} = \left\{ \frac{f}{g} \in \overline{\mathbb{Q}}(C_t) : f, g \in \overline{\mathbb{Q}}[C_t], g \notin \mathcal{M} \right\}$$

which has a unique maximal ideal $\mathcal{M}_{\mathcal{O}}$ generated by $\mathcal{M}$. Note that in $\mathcal{R}_{\mathcal{O}}$, we have that $z - 1 = \frac{z^2-1}{z+1} = \frac{ty^4}{z+1}$, so $\mathcal{M}_{\mathcal{O}}$ is generated by y alone. Similarly, we find that the maximal ideal for the point $(0, -1)$ is generated by y. So y is a uniformizer in both of those points.
Now, consider the projection map $\alpha \colon C_t \to \mathbb{P}^1, [X : Y : Z] \mapsto [X : Y]$ and for $P \in C_t$, denote $e_\alpha(P)$ for the ramification index of α at P, then

$$\deg(\alpha) = \sum_{P \in \alpha^{-1}([1:0])} e_\alpha(P) = e_\alpha([1 : 0 : 1]) + e_\alpha([1 : 0 : -1]) = \operatorname{ord}_{[1:0:1]}(y) + \operatorname{ord}_{[1:0:-1]}(y) = 2.$$

It is clear that the ramification points of α are the four points on C_t satisfying $Z = 0$, and by the degree of ϕ, the ramification index in those points must be equal to 2. Since ϕ is non-constant and separable (since every field of characteristic 0 is perfect) we have by the Riemann–Hurwitz Theorem that the genus g of C_t satisfies

$$(2g - 2) = \deg(\phi)(2 \cdot 0 - 2) + \sum_{P \in C_t} (e_\phi(P) - 1) = -4 + 4 = 0$$

so $g = 1$. We conclude that $(C_t, \mathcal{O})$ is an elliptic curve. □

The elliptic curve $(C_t, [0 : 1 : 0])$ is isomorphic to the elliptic curve in Weierstrass form $E_t : v^2 = u^3 - 4tu$, an isomorphism[1] given by

$$\tau_t \colon C_t \to E_t, [X : Y : Z] \mapsto \left[2Y(Z + X^2) : 4(ZX + X^3) : Y^3\right].$$

In particular, we have shown that $(C, [1 : 0 : 1])$ and $(C', [1 : 0 : 1])$ are both elliptic curves over $\mathbb{Q}$ (take $t = 1$ and $t = -4$). Now let $\mathcal{O} = [0 : 1 : 1]$ and $\mathcal{O}' = [1 : 0 : -1]$, then we also have that $(C, \mathcal{O})$ and $(C', \mathcal{O}')$ are elliptic curves, and it is easy to check that with those chosen points, ψ and $\hat{\psi}$ are isogenies. Therefore, in the remainder of this section we will use those chosen points, and denote C for the elliptic curve $(C, \mathcal{O})$ and C' for the elliptic

[1] See Appendix A.1 for a proof that τ_t is indeed an isomorphism

curve $(C', \mathcal{O}')$. We have that C is isomorphic to the elliptic curve $E : y^2 = x^3 - 4x$ in Weierstrass form, and that C' is isomorphic to the elliptic curve $E' : v^2 = u^3 + 16u$ in Weierstrass form (these are precisely the elliptic curves E_1 and E_{-4}). By composing τ_1 with the curve automorphism of C which switches X and Y and composing τ_{-4} with the curve automorphism of C' taking V to $-V$ and W to $-W$, we find isomorphisms

$$\tau\colon C \to E, [X : Y : Z] \mapsto \left[2(ZX + XY^2) : 4(ZY + Y^3) : X^3\right]$$

and

$$\tau'\colon C' \to E', [U : V : W] \mapsto \left[-2(WV - VU^2) : 4(WU - U^3) : V^3\right].$$

2.2.2 The descent-method applied to E

We will now apply the descent by 2-isogeny method in Section 1.2 to the elliptic curve E in Weierstrass form. This yields a second elliptic curve given by $v^2 = u(u^2 + 16)$, which turns out to coincide with the curve E' isomorphic to C', and isogenies

$$\phi\colon E \to E', (x, y) \mapsto \begin{cases} (x - \frac{4}{x}, y + \frac{4y}{x^2}) & \text{if } x \neq 0 \\ \mathcal{O}' & \text{otherwise} \end{cases}$$

and

$$\hat{\phi}\colon E' \to E, (u, v) \mapsto \begin{cases} \left(\frac{1}{4}\left(u + \frac{16}{u}\right), \frac{1}{8}\left(v - \frac{16v}{u^2}\right)\right) & \text{if } u \neq 0 \\ \mathcal{O} & \text{otherwise} \end{cases}$$

and by Lemma 1.2.2, we have that $\phi \circ \hat{\phi} = [2]$.
Furthermore, by Lemma 1.2.3 the maps

$$q\colon E'(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2, (u, v) \mapsto \begin{cases} [u] & \text{if } u \neq 0 \\ [1] & \text{otherwise} \end{cases}$$

(and $q(\mathcal{O}') = [1]$) and

$$q'\colon E(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2, (x, y) \mapsto \begin{cases} [x] & \text{if } x \neq 0 \\ [-1] & \text{otherwise} \end{cases}$$

(and $q'(\mathcal{O}) = [1]$) are group homomorphisms and we have that $\mathrm{im}(q) \cong E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ and $\mathrm{im}(q') \cong E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$.
To find $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$, we need to check whether the equation $r^2\ell^4 + 16m^4 = rn^2$ has a nonzero solution $(l, m, n) \in \mathbb{Z}^3$ for all square-free $r \in \mathbb{Z}$ such that r divides 16, so we need to check $r \in \{\pm 1, \pm 2\}$. Trivially, we have that $[1] \in \mathrm{im}(q)$. Furthermore, it is clear from the equation that a negative r is never going to work. Thus, we need only to check whether the equation

$$2l^4 + 8m^4 = n^2 \tag{2.2}$$

has a nonzero integer solution. Suppose that $(l, m, n) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$ is a solution, then we can assume that l, m and n are co-prime (if they had a common divisor a, equation (2.2)

shows that a^2 would divide n, so we would obtain another solution $(\ell/a, m/a, n/a^2))$. Note that n must be even, since the left hand side of equation (2.2) is even, which implies that all terms except possibly for $2l^4$ are divisible by 4, so l is also even. But then all terms on the left hand side are divisible by 8, so 4 divides n, which implies that $8m^4$ must be divisible by 16, so m is also even. This is a contradiction, so equation (2.2) has no nonzero integer solutions, which implies that $\mathrm{im}(q) = \{[1]\}$, so $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ is trivial.
We will now repeat this procedure with q' to find $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$. We need to check whether the equation $r^2l^4 - 4m^4 = rn^2$ has a nonzero integer solution for all square-free integers $r \in \mathbb{Z}$ dividing -4, i.e. $r \in \{\pm 1, \pm 2\}$. Note that $[1]$ is always in $\mathrm{im}(q')$, and that for $r = 2$, the equation $4(l^4 - m^4) = 2n^2$ has the solution $(1, 1, 0)$, so $[2] \in \mathrm{im}(q')$. Furthermore, we have that $[-1] \in \mathrm{im}(q')$ since it is the image of the rational 2-torsion point $(0, 0)$, so $\mathrm{im}(q') = \{\pm[1], \pm[2]\}$, so $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \cong (\mathbb{Z}/2\mathbb{Z})^2$.
From the kernel-corkernel sequence (Lemma 1.2.4), we have that

$$E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to E(\mathbb{Q})/2E(\mathbb{Q}) \to E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \to 0$$

is exact, from which we deduce that $E(\mathbb{Q})/2E(\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. Note that E has four rational 2-torsion points, which are (2,0), (-2,0), (0,0) and $\mathcal{O}$ (corresponding to $[1 : 0 : 1], [1 : 0 : -1], [0 : 1 : 1]$ and $[0 : 1 : -1]$ on C). By the Mordell–Weil Theorem (Theorem 1.2.5) we have that $E(\mathbb{Q})$ and $C(\mathbb{Q})$ are finitely generated, so we have that $E(\mathbb{Q})$ is of rank zero, which implies that $C(\mathbb{Q})$ is of rank zero. Let T denote the torsion subgroup of $C(\mathbb{Q})$, then $C(\mathbb{Q}) \cong T$ so $\#(T/2T) = \#(C(\mathbb{Q})/2C(\mathbb{Q})) = 4$. This is actually a special case of Lemma 1.2.6.
By Lemma 1.2.4 (but now with ϕ and $\hat{\phi}$ switched), we also have that the sequence

$$E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \to E'(\mathbb{Q})/2E'(\mathbb{Q}) \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to 0$$

is exact, so $E'(\mathbb{Q})/2E'(\mathbb{Q})$ is generated by $\phi(0, 0) = \mathcal{O}'$ (which does not contribute anything) and $\phi(2, 0) = (0, 0)$ and therefore isomorphic to $\mathbb{Z}/2\mathbb{Z}$. By the Mordell–Weil Theorem again, $E'(\mathbb{Q})$ and $C'(\mathbb{Q})$ are finitely generated, so since we know that E' has the rational 2-torsion points $(0, 0)$ and $\mathcal{O}'$ (corresponding to $[1 : 0 : 1]$ and $[1 : 0 : -1]$ on C'), $E'(\mathbb{Q})$ is of rank zero, and therefore $C'(\mathbb{Q})$ is of rank zero[2].

2.2.3 Relating the descent method and the classical proof

The relation between the descent method in Section 2.2 and the classical proof in Section 2.1 will become more clear now.

Proposition 2.2.2. *The diagram*

$$\begin{array}{ccccc} C & \xrightarrow{\psi} & C' & \xrightarrow{\hat{\psi}} & C \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau'} & & \downarrow{\scriptstyle \tau} \\ E & \xrightarrow{\phi} & E' & \xrightarrow{\hat{\phi}} & E \end{array}$$

[2]In fact, one can prove that the two elliptic curves used in a descent by 2-isogeny always have the same rank.

commutes.

Proof. Let $P = [X : Y : Z] \in C$, then we have that

$$\begin{aligned}(\tau' \circ \psi)(P) &= \tau'([Z : -XY : X^4 - Y^4]) \\ &= \left[2((X^4 - Y^4)XY - XYZ^2) : 4((X^4 - Y^4)Z - Z^3) : -X^3Y^3\right] \\ &= [-4XY^5 : -8ZY^4 : -X^3Y^3] = \left[4XY^2 : 8ZY : X^3\right]\end{aligned}$$

and if $X \neq 0$ (note that since $X^4 = (Z - Y^2)(Z + Y^2)$ we have that $Z + Y^2 \neq 0$ too in that case), we have that

$$\begin{aligned}(\phi \circ \tau)(P) &= \phi\left(\left[2(ZX + XY^2) : 4(ZY + Y^3) : X^3\right]\right) = \phi\left(2\frac{Z + Y^2}{X^2}, 4\frac{ZY + Y^3}{X^3}\right) \\ &= \left(2\left(\frac{Z + Y^2}{X^2} - \frac{X^2}{Z + Y^2}\right), 4\left(\frac{ZY + Y^3}{X^3} + \frac{YX}{Z + Y^2}\right)\right) \\ &= \left(2\frac{Z^2 + 2ZY^2 + Y^4 - X^4}{X^2(Z + Y^2)}, 4\frac{Y(Z^2 + 2Y^2Z + Y^4 + X^4)}{X^3(Z + Y^2)}\right) \\ &= \left(2\frac{2ZY^2 + 2Y^4}{X^2(Z + Y^2)}, 4\frac{2YZ(Z + Y^2)}{X^3(Z + Y^2)}\right) = \left(4\frac{Y^2}{X^2}, 8\frac{ZY}{X^3}\right) = [4XY^2 : 8ZY : X^3]\end{aligned}$$

and if $X = 0$, it is easy to check that $(\phi \circ \tau)(\mathcal{O}) = [0 : 1 : 0] = (\phi \circ \tau)([0 : 1 : -1])$. So the first block of the diagram commutes. Furthermore, we have for all $Q = [U : V : W] \in C'$ that:

$$\begin{aligned}(\tau \circ \hat{\psi})(Q) &= \tau([2UV : W : U^4 + 4V^4]) \\ &= \left[2(2(U^4 + 4V^4)UV + 2UVW^2) : 4((U^4 + 4V^4)W + W^3) : 8U^3V^3\right] \\ &= \left[8VU^5 : 8WU^4 : 8U^3V^3\right] = [VU^2 : WU : V^3]\end{aligned}$$

and if $V \neq 0$ (which also implies that $W - U^2 \neq 0$), we have that

$$\begin{aligned}(\hat{\phi} \circ \tau')(Q) &= \hat{\phi}\left(\left[-2(WV - VU^2) : 4(WU - U^3) : V^3\right]\right) = \hat{\phi}\left(-2\frac{W - U^2}{V^2}, 4\frac{WU - U^3}{V^3}\right) \\ &= \left(\frac{1}{4}\left(-2\frac{W - U^2}{V^2} - 8\frac{V^2}{W - U^2}\right), \frac{1}{8}\left(4\frac{WU - U^3}{V^3} - 16\frac{UV}{W - U^2}\right)\right) \\ &= \left(\frac{1}{4}\left(\frac{-2(W^2 - 2WU^2 + U^4) - 8V^4}{V^2(W - U^2)}\right), \frac{1}{8}\left(\frac{4U(W^2 - 2WU^2 + U^4) - 16UV^4}{V^3(W - U^2)}\right)\right) \\ &= \left(\frac{1}{4}\left(\frac{-4U^4 + 4U^2W}{V^2(W - U^2)}\right), \frac{1}{8}\left(\frac{8UW(W - U^2)}{V^3(W - U^2)}\right)\right) = \left(\frac{U^2}{V^2}, \frac{WU}{V^3}\right) \\ &= [VU^2 : WU : V^3]\end{aligned}$$

and for $V = 0$, we have that either $Q = \mathcal{O}$, which implies that $(\hat{\phi} \circ \tau')(Q) = [0 : 1 : 0]$, or $Q = [1 : 0 : -1]$, which implies $(\hat{\phi} \circ \tau')(Q) = \hat{\psi}([0 : 1 : 0]) = [0 : 1 : 0]$, so the other half of the diagram also commutes. □

2.2.4 A note on the automorphisms of C

As we have seen in Section 2.2.2, ψ is surjective if we restrict it to rational points, however, $\hat{\psi}$ is not (of course, both maps are surjective if we do not restrict to rational points). One can, in fact, already see this at the beginning the standard proof of the case $n = 4$ of Fermat's Last Theorem in Section 2.1, since two assumptions are made: we can choose Z to be positive, and we can assume that X is even and Y is odd. This corresponds to applying two curve automorphisms of C to our point: the one which sends $[X : Y : Z]$ to $[-X : Y : -Z]$ and the one which sends $[X : Y : Z]$ to $[Y : -X : Z]$. Note that C has j-invariant 1728 (which we can see from the equation of E), and therefore, it has complex multiplication by Proposition 1.1.2: the map $C \to C, [X : Y : Z] \to [iX : Y : Z]$ is an elliptic curve automorphism, which generates $\mathrm{Aut}(C)$. The automorphism $[X : Y : Z] \mapsto [-X : Y : Z]$ is therefore the only nontrivial elliptic curve automorphism of C which is defined over $\mathbb{Q}$, so it must be the negation in the group law of C. Hence, every curve automorphism of C which is defined over $\mathbb{Q}$ is either the translation map by a point in $C(\mathbb{Q})$, or such a translation map composed with $[X : Y : Z] \mapsto [-X : Y : Z]$.

Note that if a curve automorphism which is defined over $\mathbb{Q}$ is of order 2, it is either the translation map by a rational 2-torsion point, or the map $C(\mathbb{Q}) \to C(\mathbb{Q}), R \mapsto P - R$ for a point $P \in C(\mathbb{Q})$ (so a translation composed with negation). If in the latter case, the automorphism commutes with negation, we have that $-P + R = P + R$ for all $R \in C(\mathbb{Q})$, so P is a rational 2-torsion point. Therefore, since the curve automorphisms described above commute with negation, we have that they must correspond to the translation maps by points of order two, possibly composed with the negation map.

We will now try to find out which points belong to which curve automorphisms. We have that $[X : Y : Z] \mapsto [-X : Y : -Z]$ is translation by a point, since it has no fixed points: suppose that there exists a point $P = [X : Y : Z] \in C$ such that there exists some $\lambda \in \mathbb{Q}^*$ such that $[-X : Y : -Z] = [\lambda X : \lambda Y : \lambda^2 Z]$. Then we have that either $\lambda^2 = -1$ or $Z = 0$. If $\lambda^2 = -1$, we have that either $-X \neq \lambda X$ or $\lambda Y \neq Y$ (since at least one of X and Y must be nonzero), so the first case is not possible. If $Z = 0$, we have that $X, Y \neq 0$, and since $-X = \lambda X$ implies that $\lambda = -1$ and $Y = \lambda Y$ implies $\lambda = 1$, we also get a contradiction in this case. So $[X : Y : Z] \mapsto [-X : Y : -Z]$ is indeed translation by some point, which must be $[0 : 1 : -1]$ (by the image of $\mathcal{O}$). In a similar way, we have that the curve automorphism $[X : Y : Z] \mapsto [Y : -X : Z]$ is translation by $[1 : 0 : 1]$. It follows that the translation by $[1 : 0 : -1]$ map must be the composition of the other two, and therefore, it corresponds to the automorphism $[X : Y : Z] \mapsto [Y : X : -Z]$.

So apparently, in the classical proof given in Section 2.1 it may be necessary to add something from the kernel of the multiplication by 2 map, i.e. translate by a rational 2-torsion point, in order to make sure that our point is in the right co-set (since we see that we do not need the negation map).

2.3 The method of descent by 2-isogeny for a special class of elliptic curves

Let $t \in \mathbb{Z} \setminus \{0\}$ be a nonzero integer and let C_t be the curve over $\mathbb{Q}$ given by $X^4 + tY^4 = Z^2$ in the weighted projective plane $\mathbb{P}(1,1,2)$. In Section 2.2.1, we have shown that, together with the chosen point $\mathcal{O} = [1:0:1]$, $(C_t, \mathcal{O})$ is an elliptic curve. We used this on C_1 and C_{-4}, and had to choose different points on them, in order to make ψ and $\hat{\psi}$ into isogenies, which enabled us to compare the classical proof in Section 2.1 with a descent by 2-isogeny on elliptic curves in Weierstrass form. However, we can also develop a version of the method of descent by 2-isogeny for the elliptic curve $(C_t, \mathcal{O})$, so that we do not need go to a Weierstrass curve first. In this section, we will derive computational formulas for the addition on such elliptic curves, which will allow us to reformulate the lemmas in Section 1.2 for $(C_t, \mathcal{O})$. Then, instead of using the isomorphism to a Weierstrass curve, we can also apply the descent by 2-isogeny method directly.

2.3.1 Addition formulas

Note that C_t has j-invariant 1728 (since we noted in section 2.2.1 that it is isomorphic to the elliptic curve in Weierstrass form E_t), so by Proposition 1.1.2, it has complex multiplication: the map

$$C_t \to C_t, [X:Y:Z] \mapsto [X:iY:Z]$$

is an elliptic curve automorphism of order four, which generates the automorphism group of C_t. Therefore, we have that $[X:Y:Z] \mapsto [X:-Y:Z]$ must be the negation map (it is the only elliptic curve automorphism of C_t which is defined over $\mathbb{Q}$). So we get the following proposition.

Proposition 2.3.1 (Negation)**.** *Let $P = [X:Y:Z] \in C_t$ then $-P = [X:-Y:Z]$.*

It follows that, if we let $\sqrt{t} \in \overline{\mathbb{Q}}^*$ be such that $(\sqrt{t})^2 = t$, the 2-torsion points of C_t are $[1:0:1], [1:0:-1], [0:1:\sqrt{t}]$ and $[0:1:-\sqrt{t}]$. So C_t always has the rational 2-torsion point[3] $T = [1:0:-1]$. More geometrically, one can see that in the affine patch $z^2 = 1 + ty^2$ (with coordinates $z = \frac{Z}{X^2}$ and $y = \frac{Y}{X}$), negation is just mirroring in the z-axis.
Similar to Section 2.2.4, we have that the translation by T map is the curve automorphism $C_t \to C_t, [X:Y:Z] \mapsto [X:-Y:-Z]$, whereas the translation by $[0:1:\sqrt{t}]$ map is the curve automorphism $[X:Y:Z] \mapsto [\sqrt{t}Y:-X:\sqrt{t}Z]$ and the 2-torsion point $[0:1:-\sqrt{t}]$ corresponds to the curve automorphism $[X:Y:Z] \mapsto [\sqrt{t}Y:X:-\sqrt{t}Z]$.
We will now compute addition formulas for all other points of C_t. Considering the affine patch $z^2 = 1 + ty^4$, where $z = \frac{Z}{X^2}$ and $y = \frac{Y}{X}$, we have shown in the proof of Proposition 2.2.1 that the maximal ideal of the local ring in $\mathcal{O}$ is generated by y. Therefore, $\frac{z+1}{y^3}$ has a pole of order 3 at $\mathcal{O}$, and since the other zero of y is the point $[1:0:-1]$ and $z+1$ has a zero of order 4 in this point, it has no other poles. So if we denote $\mathcal{L}(3\mathcal{O})$ for the Riemann-Roch space associated to $3\mathcal{O}$, we have that $\mathcal{L}(3\mathcal{O})$ is generated by $1, \frac{z+1}{y^2}$ and $\frac{z+1}{y^3}$.

[3] One can check that the isomorphism τ_t which maps C_t to an elliptic curve in Weierstrass form sends T to $(0,0)$.

Proposition 2.3.2 (Addition)**.** *Let $P = (a, b), Q = (c, d)$ be two points in the affine patch $z^2 = 1 + ty^4$ such that $a \neq 0$ and $c \neq 0$.*

- *If $P \neq Q$, define*

$$\alpha = -\frac{b+1}{a^2}\left(\frac{(b+1)c^3 - a^3(d+1)}{(b+1)ac^3 - a^3c(d+1)} + \frac{1}{a}\right) \text{ and } \beta = -\left(\frac{(b+1)c^3 - a^3(d+1)}{(b+1)ac^3 - a^3c(d+1)}\right)$$

- *If $P = Q$, define*

$$\alpha = \frac{b(b+1)}{2a^3(3b-1)} \text{ and } \beta = -\frac{2ta^4 + 3b(b+1)}{2ta^5 + 2b(b+1)a}$$

Let $y_1 = -\frac{2t\beta}{t\beta^2 - \alpha^2} - a - c$ and $z_1 = -1 - \frac{\alpha y_1^3}{1+\beta y_1}$. Then $P + Q = (-y_1, z_1)$.

Proof. By the Riemann-Roch Theorem, $\mathcal{L}(3\mathcal{O} - P - Q)$ is a vector space of dimension 1 over $\overline{\mathbb{Q}}$, so there exist $\alpha, \beta, \gamma \in \overline{\mathbb{Q}}$ such that $\mathcal{L}(3\mathcal{O} - P - Q)$ is generated by the function $g = \alpha + \beta\frac{z+1}{y^2} + \gamma\frac{z+1}{y^3}$. Since P and Q are both not equal to $\mathcal{O}$, we have that $\gamma \neq 0$. We will consider two cases:

- If $P \neq Q$, we have – since g must have zero's in P and Q – that

$$\alpha + \beta\frac{b+1}{a^2} + \gamma\frac{b+1}{a^3} = 0 \text{ and } \alpha + \beta\frac{d+1}{c^2} + \gamma\frac{d+1}{c^3} = 0$$

  so

$$\beta\left(\frac{b+1}{a^2} - \frac{d+1}{c^2}\right) + \gamma\left(\frac{b+1}{a^3} - \frac{d+1}{c^3}\right) = 0$$

  from which we – scaling $\gamma = 1$ and denoting that since $P \neq Q$, we have that $\frac{b+1}{a^2} \neq \frac{d+1}{c^2}$ and $\frac{b+1}{a^3} \neq \frac{d+1}{c^3}$ – deduce that

$$\beta = -\left(\frac{(b+1)c^3 - a^3(d+1)}{(b+1)ac^3 - a^3c(d+1)}\right) \text{ so } \alpha = -\frac{b+1}{a^2}\left(\frac{(b+1)c^3 - a^3(d+1)}{(b+1)ac^3 - a^3c(d+1)} + \frac{1}{a}\right)$$

  which gives us a generator for the Riemann-Roch space.

- If $P = Q$, we still have that

$$\alpha + \beta\frac{b+1}{a^2} + \gamma\frac{b+1}{a^3} = 0$$

  Furthermore, in order for P to be a double zero of g, we get the extra condition that the tangent spaces need to be equal at P. We scale $\gamma = 1$ again, then for $z^2 - ty^4 - 1$, we have that $\frac{dz}{dy} = \frac{4ty^3}{2z}$ and for $\alpha + \beta\frac{z+1}{y^2} + \frac{z+1}{y^3} = \alpha + \frac{(z+)(\beta y+1)}{y^3}$, we get that $\frac{dz}{dy} = -\frac{(z+1)(2\beta y+3)}{y(\beta y+1)}$. So we have the following:

$$\frac{4ta^3}{2b} = -\frac{(b+1)(2\beta a+3)}{a(\beta a+1)} \text{ so } \beta = -\frac{2ta^4 + 3b(b+1)}{2ta^5 + 2b(b+1)a}$$

  from which we deduce that

$$\alpha = -\frac{b+1}{a^2}\left(\beta + \frac{1}{a}\right) = \frac{b(b+1)^2}{2ta^7 + 2b(b+1)a^3} = \frac{b(b+1)}{2a^3(3b-1)}$$

  which gives a generator for the Riemann-Roch space again.

We can find the third zero of g, by observing that for $R = (y, z) \in C_t$, we have that $g(R) = \alpha + \beta\frac{z+1}{y^2} + \frac{z+1}{y^3} = 0$ if and only if $z = -1 - \frac{\alpha y^3}{1+\beta y}$. Substituting this in the equation of C_t yields

$$0 = ty^4 + 1 = z^2 = 1 + \frac{2\alpha y^3}{1+\beta y} + \frac{\alpha^2 y^6}{1 + 2\beta y + \beta^2 y^2}$$

so

$$ty(1+\beta y)^2 - 2\alpha(1+\beta y) - \alpha^2 y^3 = (t\beta^2 - \alpha^2)y^3 + 2t\beta y^2 + (t - 2\alpha\beta)y - 2\alpha.$$

We already know that a and c are roots of this polynomial, so looking at the quadratic term, the third zero must be $y = -\frac{2t\beta}{t\beta^2-\alpha^2} - a - c$. Now if we define $y_1 = -\frac{2t\beta}{t\beta^2-\alpha^2} - a - c$ and $z_1 = -1 - \frac{\alpha y_1^3}{1+\beta y_1}$ and the point $S = (y_1, z_1) \in C_t$, we have in the zero part of the Piccard group $\mathrm{Pic}^0(C_t)$ of C_t that

$$[0] = [\mathrm{div}(g)] = [3\mathcal{O} - P - Q - S] \text{ so } -[S - \mathcal{O}] = [P - \mathcal{O}] + [Q - \mathcal{O}].$$

By Proposition 2.3.1, we conclude that $P + Q = -S = (-y_1, z_1)$. □

2.3.2 The method of 2-descent on $(C_t, \mathcal{O})$

We will now derive the descent by 2-isogeny procedure directly on C_t. To make the link with the original method clearer, we will refer to the corresponding lemmas in Section 1.2.

Lemma 2.3.3 (Lemma 1.2.1)**.** *Consider the second elliptic curve C_t' over $\mathbb{Q}$ which is given by $U^4 - 4tV^4 = W^2$ and the isogeny*

$$\psi_t \colon C_t \to C_t', [X : Y : Z] \mapsto [Z : XY : X^4 - tY^4]$$

then $\ker(\psi_t) = \{\mathcal{O}, T\}$.

We will denote $\mathcal{O}' = [1 : 0 : 1]$ for the chosen point of $C_t' = C_{-4t}$ and $T' = [1 : 0 : -1]$ for its rational 2-torsion point.

Proof. First, note that C_t' is indeed an elliptic curve over $\mathbb{Q}$, as we already checked in Section 2.2.1. Furthermore, ψ_t is a rational map of smooth projective curves, and therefore a morphism, and since it sends $\mathcal{O}$ to $\mathcal{O}'$, it is indeed an isogeny. What remains to check is that the kernel of ψ_t is indeed $\{\mathcal{O}, T\}$. Therefore, note that $\psi_t(T) = \mathcal{O}$, so $\{\mathcal{O}, T\} \subset \ker(\psi_t)$. On the other hand, if $[X : Y : Z] \in \ker(\psi_t)$, there exists some $\lambda \in \overline{\mathbb{Q}}^*$ such that $\lambda Z = 1, -\lambda XY = 0$ and $\lambda^2(X^4 - tY^4) = 1$. It follows from the second equation that either $Y = 0$ or $X = 0$. In the latter case, we have that either $[X : Y : Z] = [0 : 1 : \sqrt{t}]$ or $[X : Y : Z] = [0 : 1 : -\sqrt{t}]$. The first equation then implies that $\lambda = \pm\frac{1}{\sqrt{t}}$, however, the third one gives that $-t\lambda^2 = 1$, so $\lambda^2 = -\frac{1}{t}$. This is a contradiction, so we have that $Y = 0$, and therefore, $[X : Y : Z] \in \{\mathcal{O}, T\}$. We conclude that $\ker(\psi_t) = \{\mathcal{O}, T\}$. □

We can use Lemma 2.3.3 again to find a third elliptic curve $C_t'' \colon X^4 + 16tY^4 = Z^2$, which is isomorphic to C_t (an isomorphism given by $C_t'' \to C_t, [X : Y : Z] \mapsto [X : 2Y : Z]$). So we get a second isogeny

$$\hat{\psi}_t \colon C_t' \to C_t, [U : V : W] \mapsto [W : 2UV : U^4 + 64tV^4]$$

with $\ker(\hat{\psi}_t) = \{\mathcal{O}', T'\}$. This turns out to be the dual of ψ_t (which can be checked with the addition formulas in the previous sections), similar to Lemma 1.2.2.

Lemma 2.3.4 (First half of Lemma 1.2.3)**.** *Define the map*

$$q\colon C_t'(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2, [U:V:W] \mapsto \begin{cases} [2\frac{W+U^2}{V^2}] & \text{if } V \neq 0 \\ [t] & \text{if } [U:V:W] = T' \\ [1] & \text{if } [U:V:W] = \mathcal{O}' \end{cases}.$$

Then q is a homomorphism of groups, and the sequence $C_t(\mathbb{Q}) \xrightarrow{\psi_t} C_t'(\mathbb{Q}) \xrightarrow{q} \mathbb{Q}^*/(\mathbb{Q}^*)^2$ is exact.

Proof. One can check that q is a homomorphism of groups using the formulas in the previous section[4].
To check that the sequence is exact, suppose that $[U:V:W] \in \ker(q)$. If $[U:V:W] = \mathcal{O}'$, it is clearly in the image of ψ, and if $[U:V:W] = T'$, we have that t is a square, which implies that $[0:1:\sqrt{t}] \in C_t(\mathbb{Q})$ and $\psi_t([0:1:\sqrt{t}]) = [\sqrt{t}:0:-t] = T$. Otherwise, we have that $2\frac{W+U^2}{V^2}$ is a nonzero square in $\mathbb{Q}^*$, so

$$\frac{4V^4}{2V^2(W+U^2)} = \frac{-W^2+U^4}{2tV^2(W+U^2)} = -\frac{(W-U^2)(W+U^2)}{2tV^2(W+U^2)} = -\frac{W-U^2}{2tV^2}$$

is also a square. Let $\alpha \in \overline{\mathbb{Q}}$ be a root of $-\frac{W-U^2}{2tV^2}$, and define $P = [V : V\alpha : UV\alpha]$, then we have that

$$\begin{aligned} V^4 + tV^4\alpha^4 &= V^4 + t\left(\frac{W^2 - 2WU^2 + U^4}{4t^2}\right) = V^4 + t\left(\frac{2U^4 - 2U^2W - 4tV^4}{4t^2}\right) \\ &= U^2\left(-\frac{W-U^2}{2t}\right) = (UV\alpha)^2 \end{aligned}$$

so $P \in C_t(\mathbb{Q})$, and note that

$$\begin{aligned} \psi_t(P) &= \left[UV\alpha : V^2\alpha : V^4 - tV^4\alpha^4\right] = \left[U : V : -\frac{2tV^4}{W-U^2} + \frac{W-U^2}{2}\right] \\ &= \left[U : V : \frac{-4tV^4 + W^2 - 2WU^2 + U^4}{2(W-U^2)}\right] = \left[U : V : \frac{2W^2 - 2WU^2}{2(W-U^2)}\right] = [U:V:W]. \end{aligned}$$

So $\ker(q) \subset \psi_t(C_t(\mathbb{Q}))$. On the other hand, let $[X:Y:Z] \in C_t(\mathbb{Q})$. If $[X:Y:Z] \in \{\mathcal{O}, T\}$, it is in the kernel of q. Otherwise, we have that

$$(q \circ \psi_t)([X:Y:Z]) = q([Z : XY : X^4 - tY^4]) = \left[2\frac{X^4 - tY^4 + Z^2}{X^2Y^2}\right] = \left[4\frac{X^2}{Y^2}\right] = [1]$$

so $[X:Y:Z] \in \ker(q)$, which implies that $\psi_t(C_t(\mathbb{Q})) \subset \ker(q)$, so $\psi_t(C_t(\mathbb{Q})) = \ker(q)$, which completes the proof. □

[4]However, the easiest way to prove this is to use the isomorphism to a Weierstrass equation

Lemma 2.3.5 (Remainder of Lemma 1.2.3)**.** *Let $r \in \mathbb{Z}$ be a square-free integer, then we have that $[r] \in \mathrm{im}(q)$ if and only if the equation*

$$r^2l^4 + tm^4 = rn^2$$

has a solution $(l, m, n) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$. Furthermore, this can only happen if r divides t.

Proof. The element $[1]$ always lies in the image of q, and the corresponding equation also always has the solution $(1, 0, 1)$. Also, $[t]$ always lies in the image of q, and the equation $t^2l^4 + tm^4 = tn^2$ always has the solution $(0, 1, 1)$. So now, suppose that $[r] \notin \{[1], [t]\}$ and $[r] \in \mathrm{im}(q)$. Then there exists a point $[U : V : W] \in C'_t(\mathbb{Q})\setminus\{\mathcal{O}', T'\}$ such that $\left[2\frac{W+U^2}{V^2}\right] = [r]$, so there is some $a \in \mathbb{Q}^*$ such that $2\frac{W+U^2}{V^2} = ra^2$, which implies that $W = \frac{ra^2V^2}{2} - U^2$, so

$$U^4 - 4tV^4 = W^2 = \frac{r^2a^4V^4}{4} - ra^2V^2U^2 + U^4 \text{ which implies that } r^2\frac{(aV)^4}{4} + 4tV^4 = r(aVU)^2.$$

Writing $V = \frac{v}{w}$ and $U = \frac{u}{w}$ where $u, v, w \in \mathbb{Z}$, this becomes $r^2(av)^4 + t(2v)^4 = r(2auvw)^2$. Substituting $l = av, m = 2v$ and $n = 2auvw$, we obtain an equation of the desired form. On the other hand, substituting back we find that any nonzero solution to this equation gives rise to a point in $P \in C'_t(\mathbb{Q})$ such that $q(P) = [r]$.
It remains to show that this can only happen if r divides t. Therefore, assume that there is a nonzero solution $(l, m, n) \in \mathbb{Z}^3$ to the equation $r^2l^4 + tm^4 = rn^2$, from which we may assume without loss of generality that l, m and n are co-prime, and that there exists a prime number p which divides r but does not divide t. Then p divides m (all terms except for tm^4 are divisible by p and since t is not, m must be divisible by p), and therefore it also divides n (since r is square-free and the left hand side of the equation is divisible by p^2). This implies that p also divides l (we have $r^2l^4 = rn^2 - tm^4$, where the right hand side is divisible by p^3), which is a contradiction. □

As a corollary, we have that the image of q must be finite (there are only finitely many integers dividing t), so since

$$C'_t(\mathbb{Q})/\psi_t(C_t(\mathbb{Q})) = C'_t(\mathbb{Q})/\ker(q) \cong \mathrm{im}(q)$$

we have shown that $C'_t(\mathbb{Q})/\psi_t(C_t(\mathbb{Q}))$ is finite. In the same way, we can find that $C_t(\mathbb{Q})/\hat{\psi}_t(C'_t(\mathbb{Q}))$ is finite. One can now use the kernel-cokernel sequence (Lemma 1.2.4) to prove that $C_t(\mathbb{Q})/2C_t(\mathbb{Q})$ is also finite. Furthermore, we can use the isomorphism to $\mathrm{im}(q)$ to find generators for $C_t(\mathbb{Q})/2C_t(\mathbb{Q})$.
To illustrate this method, we go back to the original elliptic curve $C : X^4 + Y^4 = Z^2$ (so $t = 1$) and apply Lemma 2.3.1 to obtain the second elliptic curve $C' : U^4 - 4V^4 = W^2$. Now let $r \in \mathbb{Z}$ be a square-free integer, then by Lemma 2.3.3, we have that $[r]$ can only be in $\mathrm{im}(q)$ if r divides 1, i.e. $r \in \{-1, 1\}$. The class $[1]$ is always in $\mathrm{im}(q)$ and it is clear that $r = -1$ is not going to work, so $C'(\mathbb{Q})/\psi_1(C(\mathbb{Q}))$ is trivial.
In order to find the image of $q' \colon C(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$, we need to check for all square-free integers r dividing -4, so $r \in \{\pm1, \pm2\}$, whether the equation $r^2\ell^4 - 4m^4 = rn^2$ has solutions $(l, m, n) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$. For $r = 1$, we know that this is always the case. For $r = 2$, the

equation becomes $4(\ell^4 - m^4) = 2n^2$ which has $(1, 1, 0)$ as a solution, and for $r = -2$, we have that $4(\ell^4 - m^4) = -2n^2$ has the solution $(1, 1, 0)$. So $C(\mathbb{Q})/\hat{\psi}_1(C'(\mathbb{Q})) \cong (\mathbb{Z}/2\mathbb{Z})^2$, which implies that $C(\mathbb{Q})/2C(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Note that this is the same result as we obtained in Section 2.2.

2.4 Twists and ϕ-coverings

A way to clarify the method of descent by 2-isogeny, is to view it from the perspective of twists and ϕ-coverings, which we will investigate in this section.

2.4.1 Twists

Let $E : y^2 = x(x^2 + ax + b)$ be an elliptic curve over $\mathbb{Q}$ as in Section 1.2, so with $a, b \in \mathbb{Z}$, where $b \neq 0$ and $a^2 - 4b \neq 0$, and rational 2-torsion point $(0, 0)$. Let $r \in \mathbb{Q}^*$, then if $[r] \notin \{[1], [b]\}$, we have that $[r]$ is in the image of the two descent map $q' \colon E(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ if and only if there exists some $s \in \mathbb{Q}^*$ and a point $(x, y) \in E(\mathbb{Q})$ such that $x = rs^2$.
This motivates the definition of an algebraic set in $\mathbb{P}^2 \times \mathbb{A}^1$ (where we take coordinates X, Y, Z in $\mathbb{P}^2$ and s in $\mathbb{A}^1$) defined by the equations

$$\begin{cases} ZY^2 &= X(X^2 + aXZ + bZ^2) \\ X &= Zrs^2 \end{cases}.$$

Proposition 2.4.1. *This set is the union of the line $\{[0 : 1 : 0]\} \times \mathbb{A}^1$ and some algebraic curve F_r which has $([0 : 0 : 1], 0)$ as its only singular point.*

Proof. The subset of all elements satisfying $Z = 0$ is precisely the line $\{[0 : 1 : 0]\} \times \mathbb{A}^1$. The complement F_r is, by taking coordinates $y = \frac{Y}{Z}$ and $x = \frac{X}{Z}$, isomorphic to the algebraic set in $\mathbb{A}^2 \times \mathbb{A}^1$ given by the equations

$$\begin{cases} y^2 &= x(x^2 + ax + b) \\ x &= rs^2 \end{cases}$$

which, eliminating x, is the affine algebraic set in $\mathbb{A}^2$ defined as the zero set of the polynomial

$$F = y^2 - rs^2(r^2s^4 + ars^2 + b) \in \mathbb{Q}[y, s]$$

Note that $r^2s^4 + ars^2 + b$ has, by the quadratic formula, the zero's $\frac{-a \pm \sqrt{a^2 - 4b}}{2r}$. Since $a^2 \neq a^2 - 4b$ (for $b \neq 0$), those roots are distinct, so in particular, $r^2s^4 + ars^2 + b$ is not a square in $\overline{\mathbb{Q}}[s]$. Since F is monic and of degree two, this implies that F is irreducible in $(\overline{\mathbb{Q}}[s])[y]$. Therefore, F_r is an algebraic curve. Since $rs^2(r^2s^4 + ars^2 + b)$ only has a double root at zero, it has only one singular point, which corresponds to $([0 : 0 : 1], 0)$. □

By construction, F_r has a rational point precisely if $[r] \in \mathrm{im}(q')$. By Theorem 1.1.4, we have that there exists a smooth projective curve $\overline{F_r}$ over $\mathbb{Q}$ (which is unique up to isomorphism over $\overline{\mathbb{Q}}$) such that $F_r \setminus \{([0 : 0 : 1], 0)\}$ is birationally equivalent to $\overline{F_r}$. Furthermore, we get the following.

Proposition 2.4.2. *$\overline{F_r}$ is isomorphic to the smooth projective curve $E_r \subset \mathbb{P}(1,1,2)$ given by the equation $r^2X^4 + arX^2Y^2 + bY^4 = rZ^2$.*

Proof. Consider the map

$$\sigma\colon F_r \to E_r, ([X:Y:Z], s) \mapsto \left[sZ : Z : \frac{ZY}{rs}\right].$$

Then this is a well defined rational map, since for all $([X:Y:Z], s) \in F_r$ we have that

$$Y^2Z = X(X^2 + aXZ + bZ^2) = rs^2Z\left(r^2s^4Z^2 + ars^2Z^2 + bZ^2\right)$$

so

$$r\left(\frac{ZY}{sr}\right)^2 = r^2(sZ)^4 + ar(sZ)^2Z^2 + bZ^4.$$

Note that σ is regular everywhere, except for the singular point. Now we define the map

$$\sigma'\colon E_r \to F_r, [X:Y:Z] \mapsto \left(\left[\frac{rX^2}{Y} : \frac{ZrX}{Y^2} : Y\right], \frac{X}{Y}\right)$$

then σ' is a well defined rational map, since for all $[X:Y:Z] \in E_r$ satisfying $Y \neq 0$, we have that

$$r\frac{Z^2}{Y^2} = r^2\frac{X^4}{Y^2} + arX^2 + bY^2 \text{ so } Y\left(\frac{rZX}{Y^2}\right)^2 = \frac{rX^2}{Y}\left(\frac{r^2X^4}{Y^2} + arX^2 + bY^2\right).$$

We have that σ' is also regular everywhere, except for the points satisfying $Y = 0$. Furthermore, it is easy to check that σ' provides a birational inverse for σ. By Theorem 1.1.4, σ determines an isomorphism $\overline{F_r} \to E_r$. □

Now, we consider for the affine part $Z \neq 0$ of F_r, with coordinates $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, the projection map $\pi_r\colon F_r \to E, (s,(x,y)) \mapsto (x,y)$ which determines a unique map $\overline{\pi}_r\colon \overline{F_r} \to E$, and make the following observations:

1. First, note that over $\overline{\mathbb{Q}}$, we have that $(F_r)_{\overline{\mathbb{Q}}} \cong (F_1)_{\overline{\mathbb{Q}}}$ for all $r \in \mathbb{Q}^*$, an isomorphism given by $(F_r)_{\overline{\mathbb{Q}}} \to (F_1)_{\overline{\mathbb{Q}}}, (s,(x,y)) \mapsto (s\rho,(x,y))$, where $\rho \in \overline{\mathbb{Q}}^*$ is such that $\rho^2 = r$. These isomorphisms determine isomorphisms $(\overline{F_r})_{\overline{\mathbb{Q}}} \to (\overline{F_1})_{\overline{\mathbb{Q}}}$. So we actually only need to consider $\overline{F_1}$ and the family of curves which are isomorphic to it over $\overline{\mathbb{Q}}$. Those are called the *twists* of $\overline{F_1}$.

2. Furthermore, if $r' = r\gamma^2$ for some $\gamma \in \mathbb{Q}^*$, we can define the map

   $$f\colon F_r \to F_{r'}, (s,(x,y)) \mapsto \left(\frac{s}{\gamma},(x,y)\right)$$

   which is an isomorphism over $\mathbb{Q}$. Then we have that $\pi_r = \pi_{r'} \circ f$. So $\overline{F_r}$ and $\overline{F_{r'}}$ are isomorphic over $\mathbb{Q}$.

3. Also, note that, up to isomorphism over $\mathbb{Q}$, there are only finitely many $r \in \mathbb{Q}^*$ for which F_r has rational points, since we know that $\mathrm{im}(q')$ is finite by Lemma 1.2.3. If $\overline{F_r}$ has got rational points which do not correspond to rational points of F_r, then either they correspond to the singular point with $s = 0$ or they are "at infinity". In the first case, by the proof of Proposition 2.4.2, we have that those points correspond to the points $[X : Y : Z] \in E_r(\mathbb{Q})$ satisfying $X = 0$, so $bY^4 = rZ^2$. If this is a rational point, it follows that $[r] = [b]$, so $[r] \in \mathrm{im}(q')$. In the second case, we have that those points correspond to the points $[X : Y : Z] \in E_r(\mathbb{Q})$ satisfying $Y = 0$, so they satisfy $rX^4 = Z^2$, which implies that $[r] = [1]$, so $[r] \in \mathrm{im}(q')$. Therefore, $\overline{F_r}$ can only have a rational point if $[r] \in \mathrm{im}(q')$. This implies that, up to isomorphism over $\mathbb{Q}$, there are also only finitely many $r \in \mathbb{Q}^*$ for which $\overline{F_r}$ has rational points.

4. And finally, note that every point in $E(\mathbb{Q})$ is the image under $\overline{\pi}_r$ for precisely one of the curves $\overline{F_r}$, up to isomorphism over $\mathbb{Q}$.

Equivalently, we have that

$$E(\mathbb{Q}) = \bigcup_{[r] \in \mathbb{Q}^*/(\mathbb{Q}^*)^2} \overline{\pi}_r(\overline{F_r}(\mathbb{Q}))$$

and this union is disjoint and contains only finitely many points.
Applying the method of descent by 2-isogeny, we get a second elliptic curve given by $E' : v^2 = u(u^2 + a'u + b')$ where $a' = -2a$ and $b' = a^2 - 4b$, for which we can consider the algebraic set in $\mathbb{P}^2 \times \mathbb{A}^1$ (with coordinates U, V, W in $\mathbb{P}^2$ and s in $\mathbb{A}^1$) given by

$$\begin{cases} WV^2 &= U(U^2 + a'UW + b'W^2) \\ U &= Wrs^2 \end{cases} \text{ or the affine equations } \begin{cases} v^2 &= u(u^2 + a'u + b') \\ u &= rs^2 \end{cases}$$

(where $u = \frac{U}{W}$ and $v = \frac{V}{W}$). Then by the results above, this is the union of a line and an algebraic curve F_r' which has $([0 : 1 : 0], 0)$ as its only singular point. By Theorem 1.1.4 again, there exists a smooth projective curve $\overline{F_r'}$ which is birationally equivalent to F_r' and unique up to isomorphism over $\overline{\mathbb{Q}}$.

Proposition 2.4.3. *There exists an isomorphism $\overline{f}_r \colon (\overline{F_r'})_{\overline{\mathbb{Q}}} \to E_{\overline{\mathbb{Q}}}$ over $\overline{\mathbb{Q}}$.*

Proof. Consider the map

$$f \colon F_1' \to E, ((u, v), s) \mapsto \left(\frac{1}{2}\left(u - a + \frac{v}{s}\right), \frac{s}{2}\left(u - a + \frac{v}{s}\right)\right).$$

This is a well-defined rational map, since we have for all $((u, v), s) \in F_1'$ with $s \neq 0$ that the quadratic polynomial $x^2 + (a - u)x + b$ has zero's

$$x_\pm = \frac{1}{2}\left(u - a \pm \sqrt{u^2 - 2au + a^2 - 4b}\right) = \frac{1}{2}\left(u - a \pm \sqrt{\frac{v^2}{u}}\right) = \frac{1}{2}\left(u - a \pm \frac{v}{s}\right)$$

so $x_\pm + a + \frac{b}{x_\pm} = u$, from which it follows that $x_+(x_+^2 + ax_+ + b) = ux_+^2 = (sx_+)^2$, so $f((u, v), s) \in E$. Note that f is regular on all points except for the singular point. Furthermore, we define the map

$$E \to F_r', (x, y) \mapsto \left(\left(\frac{y^2}{x^2}, \left(2x + a - \frac{y^2}{x^2}\right)\frac{y}{x}\right), \frac{y}{x}\right)$$

then it is not difficult to check that it is a well defined rational map, which provides an inverse for f. It is regular for all $(x, y) \in E$ with $x \neq 0$. Therefore, f determines a unique rational map $\overline{f}\colon (\overline{F_1'})_{\overline{\mathbb{Q}}} \to E_{\overline{\mathbb{Q}}}$ which is an isomorphism. Since $\overline{F_r'}$ is isomorphic to $\overline{F_1'}$ for all $r \in \mathbb{Q}^*$, this implies that there exists an isomorphism $\overline{f}_r\colon (\overline{F_r'})_{\overline{\mathbb{Q}}} \to E_{\overline{\mathbb{Q}}}$ over $\overline{\mathbb{Q}}$. □

So in fact, the twists $\overline{F_r'}'$ are isomorphic to E over $\overline{\mathbb{Q}}$. Combining this with Proposition 2.4.2, we have that E_r is isomorphic to E' over $\overline{\mathbb{Q}}$ for all $r \in \mathbb{Q}^*$. So in fact, the method of descent by 2-isogeny is about replacing the original elliptic curve (of which rational points may be hard to find) by a set of twists of an isogenous curve, of which it may be easier to decide whether they have rational points. Moreover, it is already sufficient if we can decide whether a twist $\overline{F_r'}'$ does have *some* rational point, to obtain information about $E(\mathbb{Q})/2E(\mathbb{Q})$ and ultimately, about the rank of $E(\mathbb{Q})$.

2.4.2 A ϕ-covering

Let $\pi_r\colon F_r' \to E'$ denote the restriction of the natural projection map $\mathbb{P}^2 \times \mathbb{A}^1 \to \mathbb{P}^2$ as described in the previous section. Then π_r is a 2-to-1 map, since for almost all points in E', there are two choices for s. Let $\overline{\pi}_r\colon \overline{F_r'} \to E'$ denote the map determined by π_r. Then we get the following.

Proposition 2.4.4. *The diagram*

$$\begin{array}{ccc} \overline{F_r'} & \xrightarrow{\overline{f}_r} & E \\ & \searrow^{\overline{\pi}_r} & \downarrow \phi \\ & & E' \end{array}$$

commutes.

Proof. Let $f\colon F_1' \to E$ be the map we used to prove Proposition 2.4.3. Using the notation of that proof again, for all $((u, v), s) \in F_1' \setminus \{(0, 0), 0\}$, we define the zero $x_+ = \frac{1}{2}(u - a + \frac{v}{s})$ of the quadratic polynomial $x^2 + (a - u)x + b$ again, then we have that

$$\begin{aligned}(\phi \circ f)(s, (u, v)) = \phi(x_+, sx_+) &= \left(x_+ + a + \frac{b}{x_+}, sx_+ - \frac{bs}{x_+}\right) \\ &= \left(x_+ + a + \frac{b}{x_+}, s(2x_+ - u + a)\right) = (u, v)\end{aligned}$$

Therefore, after composing with the isomorphism $(\overline{F_1})_{\overline{\mathbb{Q}}} \to (\overline{F_r})_{\overline{\mathbb{Q}}}$ from the first remark of the previous section, the maps π_r and f determine maps which make diagram commute. □

Because of this interesting property, $\overline{\pi}_r$ is called a *ϕ-covering*.

Chapter 3

The case $n = 3$

The case $n = 3$ of Fermat's Last Theorem was first[1] proven by Euler [Eul70] in 1770 using the method of infinite descent. We will give a version of this proof in Section 3.1. In Section 3.2, we will show that one can find a similar link with a descent by 3-isogeny procedure of elliptic curves as in the case $n = 4$. Finally, in Section 3.3 we will investigate the descent by 3-isogeny procedure from the viewpoint of twists and ϕ-coverings.

3.1 The standard proof

In order to give the classical proof of Theorem 0.0.1 for $n = 3$, we will need the following lemma, a proof[2] of which can be found in, for example, [Rib99].

Lemma 3.1.1. *Let $s \in \mathbb{Z}$ be odd and suppose there exist $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$ such that $s^3 = a^2 + 3b^2$. Then there exist $u, v \in \mathbb{Z}$ such that $s = u^2 + 3v^2$, $a = u(u^2 - 9v^2)$ and $b = 3v(u^2 - v^2)$.*

Following Ribenboim, we will give the standard proof of the case $n = 3$ now.

Theorem 3.1.2 (Fermat $n = 3$)**.** *The equation $x^3 + y^3 = z^3$ has no solutions $(x, y, z) \in \mathbb{Z}^3$ satisfying $xyz \neq 0$.*

Proof. Suppose that we have a solution $(x, y, z) \in \mathbb{Z}^3$ with $xyz \neq 0$. Since 2 is not a cube, we have that x, y and z are distinct. Furthermore, we can assume without loss of generality that x, y and z are pairwise co-prime, since any prime dividing two of the three variables divides the third. It follows that exactly one of x, y, z is even, say that x and y are odd and z is even (if z is odd, we have that either x or y is even, so say x is even, then $(-x, z, y)$ is another solution).
We will now assume that $|z|$ is minimal under all solutions of which the last coordinate

[1] Actually, a full proof of Lemma 3.1.1 was missing, but Euler established this in an unpublished paper (of which an English translation and explanation can be found in [BL76]) which he wrote in 1760. However, there still turned out to be a missing link, which has been pointed out and solved by other mathematicians later.

[2] The elementary proof of Lemma 3.1.1 given by Ribenboim is quite long. However, with some more theory about unique factorization domains, there exist easier proofs.

is even, and derive a contradiction. Since x and y are odd, there are $a, b \in \mathbb{Z}$ such that $x + y = 2a$ and $x - y = 2b$, and we have that $a, b \neq 0$, $\gcd(a, b) = 1$ (for $x = a + b$ and $y = a - b$) and precisely one of them is odd (for modulo 4, we have that either $2a \equiv x + y \equiv 0$ or $2b \equiv x - y \equiv 0$). Since

$$z^3 = (a + b)^3 + (a - b)^3 = 2a(a^2 + 3b^2) \tag{3.1}$$

we have that b must be odd.
Now let p be a prime and $k \in \mathbb{Z}_{\geq 1}$ and suppose that p^k divides both $2a$ and $a^2 + 3b^2$, then since $p \neq 2$ (for $a^2 + 3b^2$ is odd) we have that p^k divides a, and therefore also $3b^2$, and since it cannot divide b, we have that $k = 1$ and $p = 3$. So we consider two cases:

1. $\gcd(2a, a^2 + 3b^2) = 1$. Then by equation (3.1), there exist $r, s \in \mathbb{Z}$ such that $2a = r^3$ and $a^2 + 3b^2 = s^3$. By Lemma 3.1.1, there are $u, v \in \mathbb{Z}$ such that $s = u^2 + 3v^2$, $a = u(u^2 - 9v^2)$ and $b = 3v(u^2 - v^2)$. Then we have that v is odd and u is even (for b is odd), $u, v \neq 0$ and $\gcd(u, v) = 1$ (any common divisor also divides a and b). Since u is not divisible by 3 (then a would also be divisible by 3), we have that $2u, u - 3v$ and $u + 3v$ are pairwise co-prime, so from

   $$r^3 = 2u(u - 3v)(u + 3v) \tag{3.2}$$

   it follows that there are $l, m, n \in \mathbb{Z} \setminus \{(0, 0, 0)\}$ such that $2u = n^3, u - 3v = l^3$ and $u + 3v = m^3$ and then we have that $l^3 + m^3 = n^3$, so (l, m, n) is another nontrivial solution of the equation, and we have that n is even and

   $$|z|^3 = |2a(a^2 + 3b^2)| = |n^3(u^2 - 9v^2)(a^2 + 3b^2)| > |n|^3$$

   so $|n| < |z|$, which contradicts the minimality of $|z|$.

2. $\gcd(2a, a^2 + 3b^2) = 3$. In this case, there is some $c \in \mathbb{Z}$ such that $a = 3c$, so from (3.1), we have that $z^3 = 18c(3c^2 + b^2)$. Since $\gcd(b, c) = 1$ (this follows from the fact that $\gcd(a, b) = 1$), $3c^2 + b^2$ is odd and 3 does not divide b, we have that $\gcd(18c, 3c^2 + b^2) = 1$. It follows that there exist $r, s \in \mathbb{Z}$ such that $18c = r^3$ and $3c^2 + b^2 = s^3$. By Lemma 3.1.1 again, there exist $u, v \in \mathbb{Z}$ such that $s = u^2 + 3v^2$, $b = u(u^2 - 9v^2)$ and $c = 3v(u^2 - v^2)$. Then we have that u is odd, v is even, $u, v \neq 0$ and $\gcd(u, v) = 1$, so $2v$, $u - v$ and $u + v$ are pairwise co-prime. Now from

   $$\left(\frac{r}{3}\right)^3 = 2v(u + v)(u - v) \tag{3.3}$$

   it follows that there are $l, m, n \in \mathbb{Z} \setminus \{(0, 0, 0)\}$ such that $2v = n^3, u + v = l^3$ and $u - v = -m^3$ and $l^3 + m^3 = n^3$. So (l, m, n) is another nontrivial solution and n is even, and since

   $$|z|^3 = 18|c(3c^2 + b^2)| = 27|n|^3|u^2 - v^2|(3c^2 + b^2) > |n|^3$$

   we have that $|n| < |z|$, which is again a contradiction.

We conclude that there are no nontrivial solutions to the equation $x^3 + y^3 = z^3$. □

3.2 Descent by 3-isogeny

Analyzing this proof, we start with the curve $C : X^3 + Y^3 = Z^3$ over $\mathbb{Q}$ in the projective plane $\mathbb{P}^2$. Together with the rational point $\mathcal{O} = [1 : -1 : 0]$, this is an elliptic curve, since C is smooth[3] and has genus 1 by the genus-degree formula. In the proof, two cases are considered. In the first one, we get the curve given by equation (3.2), and in the second one, we get the curve given by equation (3.3). Both of these are isomorphic to the curve $C' : W^3 = 2U^3 - 2UV^2$ over $\mathbb{Q}$, which, together with the point $\mathcal{O}' = [0 : 1 : 0]$, is also an elliptic curve (with similar reasoning). Furthermore, we find two rational maps (which are obtained from composing the rational maps we get in the first and the second case with isomorphisms to C and C'):

$$\psi\colon C \to C', [X : Y : Z] \mapsto [Z^3 : 2Y^3 - Z^3 : 2XYZ]$$

and $\hat{\psi}\colon C' \to C$ given by

$$[U : V : W] \mapsto \left[U^3 - UV^2 - VU^2 + \frac{V^3}{9} : U^3 - UV^2 + VU^2 - \frac{V^3}{9} : W\left(U^2 + \frac{V^2}{3}\right)\right]$$

which are morphisms since they are maps between smooth projective curves. Furthermore, it is easy to check that $\psi(\mathcal{O}) = \mathcal{O}'$ and $\hat{\psi}(\mathcal{O}') = \mathcal{O}$, so ψ and $\hat{\psi}$ are isogenies. (Note that we apparently abuse the notation of the dual again, but later on, we will show that $\hat{\psi}$ is indeed the dual of ψ.)
The curve C is isomorphic to the elliptic curve $E : y^2 = x^3 - 432$ in Weierstrass form. One isomorphism is given by $\tau\colon C \to E, [X : Y : Z] \mapsto [12Z : 36(Y - X) : X + Y]$. Similarly, C' is isomorphic to the elliptic curve in Weierstrass form $E' : v^2 = u^3 + 11664$, by the isomorphism $\tau'\colon C' \to E', [U : V : W] \mapsto [-18W : 108V : U]$. (These elliptic curves and isomorphisms have been obtained using SageMath [The18].)

3.2.1 The image of q

Let $a, b, d \in \mathbb{Z}$ be such that $b, d \neq 0$ and $27b - 4a^3d \neq 0$, then $E : y^2 = x^3 + d(ax + b)^2$ defines an elliptic curve over $\mathbb{Q}$, as in Section 1.3. Furthermore, assume that a^3d is divisible by 9, then the second elliptic curve $E' : v^2 = u^3 + d'(a'u + b')^2$ obtained from Lemma 1.3.1 satisfies $a', b', d' \in \mathbb{Z}$. Let $\delta' \in \overline{\mathbb{Q}}^*$ be such that $\delta'^2 = d'$. In order to perform a descent by 3-isogeny on E in the same way as we did it in the previous chapter, we need a way to explicitly construct the image of the three descent map defined by

$$q\colon E'(\mathbb{Q}) \to K_{d'}^*/(K_{d'})^3, (u, v) \mapsto \begin{cases} [v - \delta'(a'u + b')] & \text{if } u \neq 0 \\ [2b'\delta'] & \text{otherwise} \end{cases}$$

and $q(\mathcal{O}') = [1]$, as we will now do for the case that $K_{d'} = \mathbb{Q}$ (i.e. the 3-torsion point $(0, b'\delta')$ is rational). Note that $[r] \in \mathrm{im}(q)$ holds if and only if $[r^2] \in \mathrm{im}(q)$, which will be a helpful computational tool.

[3] See Appendix A.2

Proposition 3.2.1. *Suppose that $d' \in (\mathbb{Q}^*)^2$ and let r be a cube-free integer. Then $[r]$ lies in the image of q if and only if the equation*

$$2a'\delta' rlmn + 2b'\delta' n^3 + rm^3 = r^2 l^3$$

has a solution $(l, m, n) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$ Furthermore, this can only happen if all primes dividing r also divide $2b'\delta'$.

Proof. Note that every class in $\mathbb{Q}^*/(\mathbb{Q}^*)^3$ can be uniquely represented by a cube-free integer, and that if $r' = rs^3$ for some $s \in \mathbb{Q}^*$, the equation has a solution for r if and only if it has a solution for r': if $(l, m, n) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$ is a solution to the equation for r, we have that $(l, sm, s^2 n)$ is a solution to the equation for r' and the other way around.
For $r = 1$, the equation has the solution $(1, 1, 0)$, and $[1]$ also always lies in the image of q. Furthermore, if $[r] = [2b'\delta']$, we have that the equation for $2b'\delta'$ has the solution $(0, 1, -1)$, and also, $[2b'\delta']$ always lies in the image of q (it is the image of the rational 3-torsion point $(0, b'\delta')$). So we can assume without loss of generality that $[r] \notin \{[1], [2b'\delta'], [4b'^2 d']\}$.
Suppose that there exists some point $(u, v) \in E'(\mathbb{Q})$ such that

$$[r] = q(u, v) = [v - (a'u + b')\delta'].$$

Then there exists some $t \in \mathbb{Q}^*$ such that

$$v - (a'u + b')\delta' = rt^3. \tag{3.4}$$

Since

$$u^3 = (v - (a'u + b')\delta')(v + (a'u + b')\delta')$$

there also exists some $s \in \mathbb{Q}^*$ such that

$$v + (a'u + b')\delta' = r^2 s^3 \tag{3.5}$$

and $u = rst$. Subtracting equations (3.4) and (3.5) yields

$$2\delta'(a'u + b') + rt^3 = r^2 s^3 \text{ so } 2a'\delta' rst + 2b'\delta' + rt^3 = r^2 s^3.$$

Write $s = \frac{l}{n}$ and $t = \frac{m}{n}$, where $l, m, n \in \mathbb{Z}$, then it follows that

$$2a'\delta' rlmn + 2b'\delta' n^3 + rm^3 = r^2 l^3$$

as desired. On the other hand, going back through those substitutions, one can see that any nonzero solution to this equation gives rise to a rational point of E' which maps to $[r]$ under q.
It remains to show that this can only happen if r divides $2b'\delta'$. Therefore, suppose that $(l, m, n) \in \mathbb{Z} \setminus \{(0, 0, 0)\}$ is a solution to the equation, then we can assume without loss of generality that l, m and n are co-prime, and that there exists a prime number p dividing r but not dividing $2b'\delta'$. Looking at the equation, we then have that p must divide $2b'\delta' n^3$, and therefore, it must divide n. Now, there are two possible situations:

1. p^2 also divides r. In this case, p^3 must divide rm^3 (since it divides all other terms), so p divides m. Now, we have that all terms except possibly for $2b'\delta'n^3$ are divisible by p^4, so p^2 also divides n. But then all terms on the left hand side are divisible by p^5, so since r is cube-free, this implies that p also divides l.

2. If p^2 does not divide r, we have that p must divide m, from which it follows that all terms on the left hand side are divisible by p^3, so p also divides l.

In all cases, p divides l, m and n, which is a contradiction. We conclude that all primes dividing r must also divide $2b'\delta'$, which completes the proof. □

If the ring of integers of $K_{d'}$ is a principal ideal domain, which implies that it is also a unique factorization domain, one can also prove the following statement in a similar way.

Proposition 3.2.2. *Suppose that $\mathcal{O}(K_{d'})$ is a principal ideal domain and let $r \in \mathcal{O}(K_{d'})$ be cube-free. Then there exists a point $(u, v) \in E'(K_{d'})$ for which we have that*

$$[v - \delta'(a'u + b')] = [r]$$

in $K_{d'}^*/(K_{d'}^*)^3$ if and only if the equation $2a'\delta'rlmn + 2b'\delta'n^3 + rm^3 = r^2l^3$ has a solution $(l, m, n) \in \mathcal{O}(K_{d'}) \setminus \{(0, 0, 0)\}$. This can only happen if all primes dividing r also divide $2b'\delta'$.

3.2.2 The descent method applied to E

Applying the method of descent by 3-isogeny in Section 1.3 to the elliptic curve in Weierstrass form $E : y^2 = x^3 - 432$ which is isomorphic to C (so $a = 0, b = 12$ and $d = -3$), we obtain a second elliptic curve given by $y^2 = x^3 + 11664$, which turns out to be the Weierstrass curve E' isomorphic to C' again. Furthermore, we consider the isogenies

$$\phi\colon E \to E', (x, y) \mapsto \begin{cases} \left(\frac{x^3-12^3}{x^2}, \frac{y(x^3+2\cdot 12^3)}{x^3}\right) & \text{if } x \neq 0 \\ \mathcal{O}' & \text{otherwise} \end{cases}$$

satisfying $\ker(\phi) = \{\mathcal{O}, (0, 12\sqrt{-3}), (0, -12\sqrt{-3})\}$ and

$$\hat{\phi}\colon E' \to E, (u, v) \mapsto \begin{cases} \left(\frac{u^3+36^3}{9u^2}, \frac{v(u^3-2\cdot 36^3)}{27u^3}\right) & \text{if } u \neq 0 \\ \mathcal{O} & \text{otherwise} \end{cases}$$

with $\ker(\hat{\phi}) = \{\mathcal{O}', (0, 108), (0, -108\}$, which are dual (by Lemma 1.3.2). By Lemma 1.3.3, the maps $q\colon E'(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^3$ defined by

$$(u, v) \mapsto \begin{cases} [v - 108] & \text{if } u \neq 0 \\ [1] & \text{otherwise} \end{cases}$$

(and $q(\mathcal{O}') = [1]$) and $q'\colon E(\mathbb{Q}) \to \mathbb{Q}(\sqrt{-3})^*/(\mathbb{Q}(\sqrt{-3})^*)^3$ defined by

$$(x, y) \mapsto \begin{cases} [y - 12\sqrt{-3}] & \text{if } x \neq 0 \\ [1] & \text{otherwise} \end{cases}$$

(and $q(\mathcal{O}) = [1]$) are group homomorphisms and we have that $\mathrm{im}(q) \cong E'(\mathbb{Q})/\phi(E(\mathbb{Q})$ and $\mathrm{im}(q') \cong E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$. We will now analyze the images of both maps using Proposition 3.2.1 and Proposition 3.2.2.
Note that the 3-torsion point $(0, 108)$ of E' is rational, so in order to analyze the image of q, we need to check whether the equation

$$216n^3 + rm^3 = r^2l^3$$

has solutions in integers for all cube-free $r \in \mathbb{Z}$ dividing $2^3 \cdot 3^3$, i.e. for the following values of r:

- We know that $[1]$ is always in the image of q, as it is the image of the point at infinity.
- For $r = 2$, the equation becomes $2^2 \cdot 3^3n^3 + m^3 = 2l^3$. Suppose that we have a solution $(l, m, n) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$. Then we may assume that l, m and n are co-prime, since if a prime p divided all of them, we have that $(l/p, m/p, n/p)$ is again a solution. Since all terms except possibly for m^3 are even, we have that m must be even. But then 4 divides the left hand side of the equation, and therefore also the right hand side, so l must be even too. This, however, implies that all terms other than $2^2 \cdot 3^3n^3$ are divisible by 8, so n is also even, which is a contradiction. So the equation has no solutions, which implies that $[2] \notin \mathrm{im}(q)$, and hence $[4] \notin \mathrm{im}(q)$.
- For $r = 3$, we have to find out whether the equation $3l^3 = m^3 + 2^3 \cdot 3^2n^3$ has solutions $(l, m, n) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$. Suppose that (l, m, n) is such a solution and assume without loss of generality that l, m and n are co-prime. Then m must be divisible by 3. Similar to case $r = 2$, it follows that l is also divisible by 3, and therefore, 3 divides n too, which is a contradiction. We conclude that $[3], [9] \notin \mathrm{im}(q)$.
- For $r = 6$, the equation becomes $6l^3 = m^3 + 2^2 \cdot 3^2n^3$. If $(l, m, n) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$ were a solution with again, l, m and n co-prime, we have that m must be even, so similar to the previous cases, we also have that l, and therefore n is even, which is a contradiction. So $[6], [36] \notin \mathrm{im}(q)$.
- For $r = 12$, we have that the equation $12l^3 = m^3 + 2 \cdot 3^2n^3$ does not have solutions $(l, m, n) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$. After all, if (l, m, n) is a solution, we can assume that l, m and n are co-prime again, and then it follows from the equation that m is even, so also n is even, which implies that l is also even, which is a contradiction. Hence, $[12], [18] \notin \mathrm{im}(q)$.

We conclude that $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ is trivial.
Next, we analyze the image of q'. The 3-torsion point $(0, 12\sqrt{-3})$ of E is not rational, but we have that $\mathcal{O}(\mathbb{Q}(\sqrt{-3})) = \mathbb{Z}[\zeta]$, where $\zeta = \frac{-1+\sqrt{-3}}{2}$ is a primitive third root of unity, is a principal ideal domain. Note that $24\sqrt{-3} = 2^3(-\sqrt{-3})^3$ and that 2 and $\sqrt{-3}$ are prime elements of $\mathbb{Z}[\zeta]$. Therefore, by Proposition 3.2.2, if $r \in \mathbb{Z}[\zeta]$ is cube-free, we have that $[r]$ can only be in $\mathrm{im}(q')$ if r is of the form $r = \pm\zeta^k\sqrt{-3}^i2^j$, where $i, j, k \in \{0, 1, 2\}$. By

Proposition 1.3.4, we only need to check $r = \zeta$.
Note that $(12, 36) \in E(\mathbb{Q})$ and

$$q'(12, -36) = [-36 - 12\sqrt{-3}] = [-4 + 4\sqrt{-3}] = \left[\frac{-1 + \sqrt{-3}}{2}\right]$$

which implies that $[\zeta], [\zeta^2] \in \mathrm{im}(q')$. We conclude that $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \cong \mathbb{Z}/3\mathbb{Z}$.
We can use Lemma 1.2.4 to find that the sequence

$$E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to E(\mathbb{Q})/3E(\mathbb{Q}) \to E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \to 0$$

is exact, from which we deduce that $E(\mathbb{Q})/3E(\mathbb{Q})$ is generated by $(12, 36)$ (of which we also know now that it is a rational 3-torsion point[4]), and therefore, it is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. By the Mordell–Weil Theorem, $E(\mathbb{Q})$ and $C(\mathbb{Q})$ are finitely generated, so we have that $E(\mathbb{Q})$ is of rank zero, which implies that $C(\mathbb{Q})$ has rank zero too. Similarly, we find that $E'(\mathbb{Q})/3E'(\mathbb{Q})$ is generated by the rational 3-torsion point $(0, 108)$, so it is also isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Hence, $E'(\mathbb{Q})$ is also of rank zero, from which it follows that $C'(\mathbb{Q})$ has rank zero. We can also see from this that E and E', and therefore C and C', have precisely three rational 3-torsion points[5].

3.2.3 Relating the descent method and the classical proof

Similar to Section 2.2.3, we will now relate the classical proof in Section 3.1 and the method of descent by 3-isogeny in Section 3.2. Recall that we defined the isogenies $\psi\colon C \to C'$ and $\hat{\psi}\colon C' \to C$ in the introduction of this section, and also the isomorphisms $\tau\colon C \to E$ and $\tau'\colon C' \to E'$. Furthermore, in Section 3.2.2 we defined the isogenies $\phi\colon E \to E'$ and $\hat{\phi}\colon E' \to E$.

Proposition 3.2.3. *The diagram*

$$\begin{array}{ccccc} C & \xrightarrow{\psi} & C' & \xrightarrow{\hat{\psi}} & C \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau'} & & \downarrow{\scriptstyle \tau} \\ E & \xrightarrow{\phi} & E' & \xrightarrow{\hat{\phi}} & E \end{array}$$

commutes.

Proof. Let $P = [X : Y : Z] \in C$, then we have that

$$(\tau' \circ \psi)(P) = \tau'([Z^3 : 2Y^3 - Z^3 : 2XYZ]) = [-36XYZ : 216Y^3 - 108Z^3 : Z^3]$$

and

$$\begin{aligned}(\phi \circ \tau)(P) &= \phi([12Z : 36(Y_X) : X + Y]) \\ &= [12^4Z^4 - 12^4Z(X+Y)^3 : 36(Y - X)(12^3Z^3 + 2 \cdot 12^3(X+Y)^3) : 12^3Z^3(X+Y)] \\ &= [-12Z(3X^2Y + 3Y^2X) : 36(3Z^3(Y - X) + 6XY(Y+X)(Y-X)) : Z^3(X+Y)] \\ &= [-12XYZ \cdot 3(X+Y) : 36(X+Y)(-3Z^3 + 6Y^3) : Z^3(X+Y)] \\ &= [-36XYZ : 216Y^3 - 108Z^3 : Z^3]\end{aligned}$$

[4] One can check that $\tau([0 : 1 : 1]) = (12, 36)$, so this should not be too surprising

[5] In fact, it can be shown that an elliptic curve over $\mathbb{Q}$ can have at most three rational 3-torsion points, as is done in [vB10] (following a lecture of Jaap Top).

so the first half of the diagram commutes.
Now let $Q = [U : V : W] \in C'$, then

$$\begin{aligned}(\tau \circ \hat{\psi})(Q) &= \tau\left(\left[U^3 - UV^2 - VU^2 + \frac{V^3}{9} : U^3 - UV^2 + VU^2 - \frac{V^3}{9} : W\left(U^2 + \frac{V^2}{3}\right)\right]\right) \\ &= \left[12W\left(U^2 + \frac{V^2}{3}\right) : 72\left(VU^2 - \frac{V^3}{9}\right) : 2(U^3 - UV^2)\right]\end{aligned}$$

and

$$\begin{aligned}(\hat{\phi} \circ \tau')(Q) &= \hat{\phi}([-18W : 108V : U]) \\ &= [3 \cdot (9^4 \cdot 16W^4 - 2 \cdot 9 \cdot 36^3U^3W) : 108V(-8 \cdot 9^3W^3 - 2 \cdot 36^3U^3) : -8 \cdot 27 \cdot 9^3W^3U] \\ &= [54W(W^3 - 8U^3) : -108V(W^3 + 16U^3) : -27W^3U] \\ &= \left[-12 \cdot 27W\left(U^2 + \frac{V^2}{3}\right) : -72 \cdot 27U\left(VU^2 - \frac{V^3}{9}\right) : -27W^3U\right] \\ &= \left[12W\left(U^2 + \frac{V^2}{3}\right) : 72\left(VU^2 - \frac{V^3}{9}\right) : 2(U^3 - UV^2)\right]\end{aligned}$$

so the other half of the diagram also commutes. □

3.2.4 A note on the automorphisms of C

The descent by 3-isogeny in Section 3.2.2 shows that ϕ, and therefore ψ, is surjective if we restrict it to rational points. However, $\hat{\phi}$, so also $\hat{\psi}$, is not surjective when restricted to rational points.
Similar to Section 2.2.4, this can already be seen from the beginning of the classical proof in Section 3.1, since the assumption is made that for the nontrivial solution (x, y, z) of which we assume that it exists, we have that x and y are odd and z is even. This assumption comes down to applying the curve automorphisms $C \to C, [X : Y : Z] \mapsto [Y : Z : X]$ and $C \to C, [X : Y : Z] \mapsto [Z : X : Y]$ to the point $[x : y : z] \in C(\mathbb{Q})$.
Note that since the j-invariant of C equals 0 (which can be seen from the equation of E), we have by Proposition 1.1.2 that C has complex multiplication: let $\zeta_3 \in \overline{\mathbb{Q}}$ be a primitive third root of unity, then the automorphism group of C is of order 6, and it is generated by the automorphism $[X : Y : Z] \mapsto [Y : X : \zeta_3 Z]$. The automorphism $[X : Y : Z] \mapsto [Y : X : Z]$ is the only one which is defined over $\mathbb{Q}$, so this automorphism must be the negation[6] in the group law of C. Therefore, every curve automorphism of C which is defined over $\mathbb{Q}$ corresponds to translation by a rational point, possibly composed with this automorphism. So the curve automorphisms which are applied in the classical proof correspond to translations with rational 3-torsion points (since they are of order 3), possibly composed with the negation map.
We will now identify which rational points correspond to which curve automorphisms. The automorphism $C \to C, [X : Y : Z] \mapsto [Y : Z : X]$ is a translation by a rational point, since

[6] One can also compute the map $\tau^{-1} : E \to C, [U : V : W] \mapsto [V - 36W : V + 36W : 6U]$ and then check directly that $\tau^{-1}(-\tau([X : Y : Z])) = -[X : Y : Z]$.

otherwise, it would have fixed points, which it doesn't: if there exists some $[X:Y:Z] \in C$ such that $[X:Y:Z] = [Y:Z:X]$, there exists some $\lambda \in \overline{\mathbb{Q}}^*$ such that $\lambda X = Y, \lambda Y = Z$ and $\lambda Z = X$. It follows that $X, Y, Z \neq 0$ (if one of them is zero, also the other two are) and since $\lambda^3 X = \lambda^2 Y = \lambda Z = X$, we have that $\lambda^3 = 1$. But then, it follows that our point must be $[\lambda : \lambda^2 : 1]$. However, clearly such points do not lie on C, so the automorphism is a translation by the rational point $[1:0:1]$ (since it maps $\mathcal{O}$ to this point). Since $-[1:0:1] = [0:1:1]$, it follows that the inverse of the translation by $[1:0:1]$ map, i.e. the automorphism $C \to C, [X:Y:Z] \mapsto [Z:X:Y]$, is translation by $[0:1:1]$.
So, in the classical proof, one may have to translate the point $[x:y:z]$ by a rational 3-torsion point in order to get into the right co-set (for note that we do not need the negation map).

3.3 Twists and ϕ-coverings

Similarly to what we did in Section 2.4, we will now also investigate the method of descent by 3-isogeny from the viewpoint of twists and ϕ-coverings. Consider the elliptic curve $E : y^2 = x^3 + d(ax+b)^2$ over $\mathbb{Q}$, where $a, b, d \in \mathbb{Q}$ are such that $b, d \neq 0$ and $27b - 4a^3 d \neq 0$. Suppose that $\delta \in \overline{\mathbb{Q}}$ is such that $\delta^2 = d$, and denote $K_d = \mathbb{Q}(\delta)$. Applying the descent by 3-isogeny method in Section 1.3, we get a homomorphism of groups $q' \colon E(\mathbb{Q}) \to K_d^*/(K_d^*)^3$.

3.3.1 The case $d \in (\mathbb{Q}^*)^2$

Suppose that $d \in (\mathbb{Q}^*)^2$, i.e. $\delta \in \mathbb{Q}^*$, and let $r \in \mathbb{Q}^*$. If $[r] \notin \{[1], [2b\delta], [4b^2 d]\}$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^3$, we have that $[r] \in \mathrm{im}(q')$ if and only if there exists some $(x, y) \in E(\mathbb{Q})$ and $s \in \mathbb{Q}^*$ such that $y - \delta(ax+b) = rs^3$.

Proposition 3.3.1. *Consider the algebraic set $F_r \subset \mathbb{P}^2 \times \mathbb{A}^1$ (where we take coordinates X, Y, Z for $\mathbb{P}^2$ and s for $\mathbb{A}^1$) given by the equations:*

$$\begin{cases} Y^2 Z & = X^3 + dZ(aX + bZ)^2 \\ Y - \delta(aX + bZ) & = rs^3 Z \end{cases}.$$

Then this set is an algebraic curve, of which $([0 : b\delta : 1], 0)$ is the only singular point.

Proof. Consider the part of F_r where $Z \neq 0$, which can be given by the affine equations

$$\begin{cases} y^2 & = x^3 + d(ax+b)^2 \\ y - \delta(ax+b) & = rs^3 \end{cases}$$

where we take coordinates $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$. Eliminating y, this is isomorphic to the algebraic set in $\mathbb{A}^2$ which is the zero set of the polynomial $F \in \overline{\mathbb{Q}}[x, s]$ given by

$$F = x^3 - 2\delta a r s^3 x - r s^3 (r s^3 + 2\delta b).$$

Note that F is irreducible in $(\overline{\mathbb{Q}}[s])[x]$, since we have that if $f \in \overline{\mathbb{Q}}[s]$ is a zero, it needs to divide $rs^3(rs^3 + 2\delta b)$, but it is easy to check that for all possible degrees of f, some terms

remain which cannot vanish. Thus, F defines an algebraic curve, and since there are only finitely many points of F_r satisfying $Z = 0$, this implies that F_r is an algebraic curve.
Note that $\frac{\partial F}{\partial x} = 3x^2 - 2\delta ars^3$ and $\frac{\partial F}{\partial s} = -6\delta ars^2x - 6r^2s^5 - 6r^2\delta bs^2$. Clearly, both of those are zero if $x = s = 0$, which implies that F_r has a singular point at $([0 : b\delta : 1], 0)$. On the other hand, if we require $x \neq 0$ (which is only possible if $a \neq 0$), we have that $s \neq 0$. Then $\frac{\delta F}{\delta x} = \frac{\delta F}{\delta s} = 0$ can only hold if $x = -\frac{rs^3+r\delta b}{\delta a}$ and $x^2 = \frac{2\delta ars^3}{3}$, which is a contradiction. So F_r has no singular points except for $([0 : b\delta : 1], 0)$. □

By construction, we have that $[r] \in \mathrm{im}(q')$ if and only if F_r has a rational point $([X : Y : Z], s)$ such that $s \neq 0$. By Theorem 1.1.4, there exists a smooth projective curve $\overline{F_r}$ which is birationally equivalent to F_r, and $\overline{F_r}$ is unique up to isomorphism over $\overline{\mathbb{Q}}$. In Proposition 3.2.1, we also considered the curve $E_r \subset \mathbb{P}^2$ given by the equation

$$2ar\delta UVW + 2b\delta W^3 + rV^3 = r^2U^3.$$

One can check that this curve has singular points, but by Theorem 1.1.4 again, there exists some smooth projective curve $\overline{E_r}$ over $\mathbb{Q}$ which is birationally equivalent to E_r, and unique up to isomorphism over $\overline{\mathbb{Q}}$. Then we have the following.

Proposition 3.3.2. *The curves $\overline{F_r}$ and $\overline{E_r}$ are isomorphic over $\mathbb{Q}$.*

Proof. Consider the map $\sigma\colon F_r \to E_r, ([X : Y : Z], s) \mapsto [X : rZs^2 : rZs]$. Then this is a well defined rational map, since we have for all $([X : Y : Z], s) \in F_r$ that

$$\begin{aligned} r^2X^3 &= r^2Z(Y - \delta(aX + bZ))(Y + \delta(aX + bZ)) = r^3Z^2s^3(rs^3Z + 2\delta(aX + bZ)) \\ &= r(rs^2Z)^3 + 2a\delta r \cdot rZs^2 \cdot rsZ \cdot X + 2b\delta(rZs)^3. \end{aligned}$$

Note that σ is regular everywhere, except for the singular point. Furthermore, define the map $\sigma'\colon E_r \to F_r, [U : V : W] \mapsto \left(\left[U : \frac{rV^3}{W^3} + \delta\left(aU + \frac{bW^2}{rV}\right) : \frac{W^2}{rV}\right], \frac{V}{W}\right)$ then it is easy to check that σ' is a well defined rational map which provides an inverse for σ. It is regular everywhere, except for the points where $V = 0$ or $W = 0$. So σ admits a birational inverse, which implies that it determines a birational map $\overline{\sigma}\colon \overline{F_r} \to \overline{E_r}$ which, since both of those curves are smooth and projective, is an isomorphism. □

Note that for all $r \in \mathbb{Q}^*$, we have that $\overline{F_r}$ is isomorphic to $\overline{F_1}$ over $\overline{\mathbb{Q}}$, since if we let $\rho \in \overline{\mathbb{Q}}$ be such $r = \rho^3$, the map $(F_r)_{\overline{\mathbb{Q}}} \to (F_1)_{\overline{\mathbb{Q}}}, ([X : Y : Z], s) \mapsto ([X : Y : Z], \rho s)$ is clearly a bijective rational map, and therefore, it determines an isomorphism $(\overline{F_r})_{\overline{\mathbb{Q}}} \to (\overline{F_1})_{\overline{\mathbb{Q}}}$. Again, the $\overline{F_r}$ are called the *twists* of $\overline{F_1}$. Furthermore, suppose that $r' = r\gamma^3$ for some $\gamma \in \mathbb{Q}^*$. Then we have that the map

$$F_{r'} \to F_r, ([X : Y : Z], s) \mapsto ([X : Y : Z], \gamma s)$$

is clearly a bijective rational map, which determines an isomorphism $\overline{F_{r'}} \to \overline{F_r}$ over $\mathbb{Q}$. Since $\mathrm{im}(q')$ is finite by Proposition 3.2.1, this implies that up to isomorphism over $\mathbb{Q}$, there are only finitely many of the curves F_r which have got rational points. Note that if $\overline{F_r}$ has a rational point and F_r has not, we have that those points either correspond to the singular point, so $s = 0$, or are "at infinity". Using the proof of Proposition 3.3.2, we see that the rational points in the first case correspond to points $[U : V : W] \in \overline{E_r}(\mathbb{Q})$ satisfying $V = 0$,

so $2b\delta W^3 = r^2U^3$, which implies that $[r] = [2b\delta]$, and this class is always in $\mathrm{im}(q')$. In the second case, the rational points correspond to points $[U : V : W] \in \overline{E_r}(\mathbb{Q})$ satisfying $W = 0$, so $rV^3 = r^2U^3$, which implies that $[r] = [1]$, which is also always in $\mathrm{im}(q')$. So if $\overline{F_r}$ has a rational point, we always have that $[r] \in \mathrm{im}(q')$, which implies that there are, up to isomorphism over $\mathbb{Q}$, only finitely many twists of $\overline{F_1}$ which have rational points.
Now, consider the projection map $\pi_r \colon F_r \to \mathbb{P}^2, ([X : Y : Z], s) \mapsto [X : Y : Z]$, which determines a unique morphism $\overline{\pi}_r \colon \overline{F_r} \to \mathbb{P}^2$. Then up to isomorphism over $\mathbb{Q}$, every element in $E(\mathbb{Q})$ is the image under $\overline{\pi}_r$ for exactly one curve $\overline{F_r}$.
Summarizing the preceding discussion, we have that

$$E(\mathbb{Q}) = \bigcup_{[r] \in \mathbb{Q}^*/(\mathbb{Q}^*)^3} \overline{\pi}_r(\overline{F_r}(\mathbb{Q}))$$

where the union is disjoint and consists of finitely many points.
Similarly, we suppose that $d' \in (\mathbb{Q}^*)^2$, let δ' be such that $\delta'^2 = d'$ and consider the algebraic set $F_r' \subset \mathbb{P}^2 \times \mathbb{A}^1$ given by

$$\begin{cases} V^2W & = U^3 + d'W(a'U + b'W)^2 \\ V - \delta'(a'U + b'W) & = rs^3W \end{cases}$$

or, taking coordinates $u = \frac{U}{W}$ and $v = \frac{V}{W}$, the affine equations

$$\begin{cases} v^2 & = u^3 + d'(a'u + b')^2 \\ v - \delta'(a'u + b') & = rs^3 \end{cases}.$$

Then F_r' is a curve by Proposition 3.3.1. By Theorem 1.1.4, there exists some smooth projective curve $\overline{F_r}'$ such that F_r' is birationally equivalent to $\overline{F_r}'$. The proof of the following proposition is due to [Coh07] (more specifically, Proposition 8.4.4 of his book).

Proposition 3.3.3. *There exists an isomorphism $\overline{f}_r \colon (\overline{F_r}')_{\overline{\mathbb{Q}}} \to E_{\overline{\mathbb{Q}}}$ over $\overline{\mathbb{Q}}$.*

Proof. For $((u, v), s) \in F_1'$ with $s \neq 0$, define $u' = \frac{s + \frac{u}{s}}{2}$ and $v' = \frac{s - \frac{u}{s}}{2\delta'}$, let $x = \frac{-b}{v' + \frac{a}{3}}$ and consider the map

$$f \colon F_r \to E, ((u, v), s) \mapsto (x, u'x)$$

Note that since $s = u' + v'\delta'$ and $\frac{u}{s} = u' - v'\delta'$ we have that $u = u'^2 - d'v'^2 = u'^2 + 3dv'^2$, and

$$s^3 - \left(\frac{u}{s}\right)^3 = 2\delta'(3u'^2v' + v'^3d')$$

while on the other hand, it follows from

$$s^3 \cdot \left(\frac{u}{s}\right)^3 = u^3 = v^2 - d'(a'u + b')^2 = (v - \delta'(a'u + b'))(v + \delta'(a'u + b')) = s^3(v + \delta'(a'u + b'))$$

that $\left(\frac{u}{s}\right)^3 = v + \delta'(a'u + b')$, so we have that

$$\begin{aligned} s^3 - \left(\frac{u}{s}\right)^3 &= v - \delta'(a'u + b') - (v + \delta'(a'u + b')) = -2\delta'(a'u + b') \\ &= -2\delta'\left(a(u'^2 + 3dv'^2) + \frac{27b - 4a^3d}{9}\right) \end{aligned}$$

from which we see that

$$b = -u'^2\left(v' + \frac{a}{3}\right) + d\left(v'^3 - av'^2 + \frac{4a^3}{27}\right) = \left(v' + \frac{a}{3}\right)\left(d\left(v' - \frac{2a}{3}\right)^2 - u'^2\right).$$

It follows that

$$\begin{aligned}(x^3 + d(ax+b)^2)\left(v' + \frac{a}{3}\right)^3 &= -b^3 + db^2\left(v' + \frac{a}{3}\right)\left(-a + v' + \frac{a}{3}\right)^2 \\ &= b^2\left(v' + \frac{a}{3}\right)\left(-\left(d\left(v' - \frac{2a}{3}\right)^2 - u'^2\right) + d\left(v' - \frac{2a}{3}\right)^2\right) \\ &= b^2\left(v' + \frac{a}{3}\right)u'^2 = \left(v' + \frac{a}{3}\right)^3 u'^2x^2\end{aligned}$$

so $(x, u'x) \in E$. Therefore, f is a well defined rational map. Furthermore, f has a birational inverse, since for $(x, y) \in E$, we can define $u' = \frac{y}{x}$ and $v' = -\left(\frac{b}{x} + \frac{a}{3}\right)$, then it is not difficult to check that the point $((u, v), s)$ with coordinates defined by $u = u'^2 - d'v^2$, $s = u' + v'\delta'$ and $v = s^3 + \delta'(a'u + b')$ is in F'_r, which defines an inverse for f.
Therefore, f determines an isomorphism $\overline{f}\colon \overline{F_1}' \to E$ over $\overline{\mathbb{Q}}$. Since we already know that $\overline{F_1}'$ is isomorphic to $\overline{F_r}'$ over $\overline{\mathbb{Q}}$, this implies that there is an isomorphism $\overline{f}_r\colon (\overline{F_r}')_{\overline{\mathbb{Q}}} \to E_{\overline{\mathbb{Q}}}$ over $\overline{\mathbb{Q}}$, as desired. □

It follows that there also exists an isomorphism $(\overline{F_r})_{\overline{\mathbb{Q}}} \to (E')_{\overline{\mathbb{Q}}}$. So actually, in the method of descent by 3-isogeny, we replace the problem of finding the rational points of E by checking whether another set of curves has a rational point, which may be less difficult. Furthermore, in order to obtain useful information about $E(\mathbb{Q})/3E(\mathbb{Q})$ and ultimately, the rank of $E(\mathbb{Q})$, it suffices to decide whether the twists do have rational points or not.
The proof of the following is also due to [Coh07] (same proposition).

Proposition 3.3.4. *The following diagram commutes:*

$$\begin{array}{ccc} \overline{F_r}' & \xrightarrow{\overline{f}_r} & E \\ & \searrow^{\overline{\pi}_r} & \downarrow \phi \\ & & E' \end{array}$$

Proof. Let $((u, v), s) \in F'_1$ be such that $s \neq 0$, then we have that $\pi_1((u, v), s) = (u, v)$. On the other hand - using the notation of the previous proof again - we have that

$$(\phi \circ f)(u, v) = \phi(x, y) = \left(x + 4d\left(\frac{a^2}{3} + \frac{ab}{x} + \left(\frac{b}{x}\right)^2\right), u'\left(x - 4d\left(\frac{ab}{x} + 2\left(\frac{b}{x}\right)^2\right)\right)\right)$$

and note that $x = \frac{-b}{v' + \frac{a}{3}} = u'^2 - d\left(v' - \frac{2a}{3}\right)^2$ so

$$\begin{aligned}x + 4d\left(\frac{a^2}{3} + \frac{ab}{x} + \left(\frac{b}{x}\right)^2\right) &= u'^2 - d\left(v' - \frac{2a}{3}\right)^2 + d\left(\frac{4a^2}{3} - 4a\left(v' + \frac{a}{3}\right) + 4\left(v' + \frac{a}{3}\right)^2\right) \\ &= u'^2 + 3dv'^2 = u.\end{aligned}$$

We also have that $v = \frac{1}{2}\left(s^3 + \left(\frac{u}{s}\right)^3\right) = u'^3 - 9u'v'^2d$ which implies that

$$u'\left(x - 4d\left(\frac{ab}{x} + 2\left(\frac{b}{x}\right)^2\right)\right) = u'\left(u'^2 - d\left(v' - \frac{2a}{3}\right)^2 + d\left(4a\left(v' + \frac{a}{3}\right) - 8\left(v' + \frac{a}{3}\right)^2\right)\right)$$
$$= u'(u'^2 - 9v'^2d) = v.$$

So $(\phi \circ f)(u, v) = (u, v)$. Therefore, $\overline{f}$ and $\overline{\pi}_1$ make the diagram commute for $r = 1$. Composing both maps with an isomorphism $(\overline{F_r}')_{\overline{\mathbb{Q}}} \to (\overline{F_1}')_{\overline{\mathbb{Q}}}$, we see that the diagram commutes. □

Again, $\overline{\pi}_r$ is called a *ϕ-covering*.

3.3.2 The case $d \notin (\mathbb{Q}^*)^2$

We want to develop a similar theory for the case that $K_d \neq \mathbb{Q}$, i.e. $\delta \notin \mathbb{Q}^*$. By Proposition 1.3.4, the image of q' is contained in the subfield of $K_d^*/(K_d^*)^3$ consisting of all elements of which the norm is trivial in $\mathbb{Q}^*/(\mathbb{Q}^*)^3$.

Proposition 3.3.5. *Let $r = r_1 - \delta r_2 \in K_d^*$, and let $t \in \mathbb{Q}^*$ be such that*

$$N(r) = (r_1 + \delta r_2)(r_1 - \delta r_2) = t^3.$$

Then $r \in \mathrm{im}(q')$ if and only if the smooth projective curve $F_r \subset \mathbb{P}^2$ given by the equation

$$atW(U^2 - dV^2) + bW^3 = r_2U^3 + 3r_1U^2V + 3dr_2UV^2 + dr_1V^3$$

has a rational point.

Proof. For $[r] = [1]$, the curve has the rational point $[1 : 0 : 0]$, and $[1]$ is also always in $\mathrm{im}(q')$. (And note that we need not to check what happens for the 3-torsion point $(0, b'\delta')$, since it is not rational.)
Suppose that $[r] \neq [1]$, and $[r] \in \mathrm{im}(q')$, then there exists a point $(x, y) \in E(\mathbb{Q})$ together with some $s = s_1 - \delta s_2 \in K_d^*$ such that $y - \delta(ax + b) = rs^3$. Conjugating gives us the algebraic set $E_r \subset \mathbb{A}^4$ (with coordinates x, y, s_1 and s_2) defined by:

$$\begin{cases} y^2 & = x^3 + d(ax + b)^2 \\ y - \delta(ax + b) & = (r_1 - \delta r_2)(s_1 - \delta s_2)^3 \\ y + \delta(ax + b) & = (r_1 + \delta r_2)(s_1 + \delta s_2)^3 \end{cases}$$

Combining the second and the last equation yields that $x^3 = y^2 - d(ax + b)^2 = t^3N(s)^3$, so since $x \in \mathbb{Q}$, it follows that $x = tN(s) = t(s_1^2 - ds_2^2)$. Combining this with the fact that

$$ax + b = \frac{(r_1 + \delta r_2)(s_1 + \delta s_2)^3 - (r_1 - \delta r_2)(s_1 - \delta s_2)^3}{2\delta} = r_2s_1^3 + 3r_1s_1^2s_2 + 3dr_2s_1s_2^2 + dr_1s_2^3$$

we find that

$$at(s_1^2 - ds_2^2) + b = r_2s_1^3 + 3r_1s_1^2s_2 + 3dr_2s_1s_2^2 + dr_1s_2^3 \tag{3.6}$$

so any $[r] \in \mathrm{im}(q')$ gives rise to a rational point on F_r.
On the other hand, if F_r has a rational point $[U : V : W]$, this implies that $[r] \in \mathrm{im}(q')$. If the rational point is not at infinity (i.e. $W \neq 0$), this follows from the construction above. If the rational point satisfies $W = 0$, it follows that $(r_1 + \delta r_2)(U + \delta V)^3 = (r_1 - \delta r_2)(U - \delta V)^3$ which implies that $r(U - \delta V)^3 \in \mathbb{Q}$. So $t^3 N(U - \delta V)^3 = r^2(U - \delta V)^6$, which implies that r^2 is a third power, so r itself is a third power, which implies that $[r] = [1]$, which is always in $\mathrm{im}(q')$. □

Consider the affine curve $K_r \subset \mathbb{A}^4$ given by the equations

$$\begin{cases} x & = t(s_1^2 - ds_2^2) \\ y - \delta(ax + b) & = (r_1 - \delta r_2)(s_1 - \delta s_2)^3 \\ y + \delta(ax + b) & = (r_1 + \delta r_2)(s_1 + \delta s_2)^3 \end{cases}$$

which is a subvariety of E_r. By Theorem 1.1.4, there exists a smooth projective curve $\overline{K_r}$ which is birationally equivalent to K_r, and unique up to isomorphism over $\overline{\mathbb{Q}}$. It follows from the proof of Proposition 3.3.5 that F_r is isomorphic to $\overline{K_r}$ over $\overline{\mathbb{Q}}$, since if we consider the affine part of F_r given by equation (3.6), the rational map

$$\eta \colon K_r \to F_r, (x, y, s_1, s_2) \mapsto (s_1, s_2)$$

is clearly well defined, and it is easy to check that the map

$$\eta' \colon F_r \to K_r, (s_1, s_2) \mapsto (t(s_1^2 - ds_2^2), r(s_1 - \delta s_2)^3 + \delta(at(s_1^2 - ds_2^2) + b), s_1, s_2)$$

provides an inverse. Therefore, η determines an isomorphism $(\overline{K_r})_{\overline{\mathbb{Q}}} \to (F_r)_{\overline{\mathbb{Q}}}$.
Note that F_r is isomorphic to F_1 over $\overline{\mathbb{Q}}$, since we can choose some $\rho = \rho_1 - \delta\rho_2 \in \overline{\mathbb{Q}}$ such that $r = \rho^3$, i.e. $r_1 = \rho_1^3 + 3d\rho_1\rho_2^2$ and $r_2 = 3\rho_1^2\rho_2 + d\rho_2^3$, and from $t^3 = N(r) = N(\rho)^3$ we see that $N(\rho) = t$. Then we have that the map

$$\sigma \colon (F_r)_{\overline{\mathbb{Q}}} \to (F_1)_{\overline{\mathbb{Q}}}, (u, v) \mapsto (\rho_1 u + d\rho_2 v, \rho_2 u + \rho_1 v)$$

is a well defined rational map. In order to see this, let $(u, v) \in F_r$ and denote $\sigma(u, v) = (u', v')$, then we have that

$$\begin{aligned} a(u'^2 - dv'^2) + b &= a(\rho_1^2 u^2 + 2d\rho_1\rho_2 uv + d^2\rho_2^2 v^2 - d(\rho_2^2 u^2 + 2\rho_1\rho_2 uv + \rho_1^2 v^2)) + b \\ &= at(u^2 - dv^2) + b = r_2 u^3 + 3r_1 u^2 v + 3dr_2 uv^2 + dr_1 v^3 \\ &= (3\rho_1^2\rho_2 + d\rho_2^2)u^3 + 3(\rho_1^3 + 3d\rho_1\rho_2^2)u^2 v + 3d(3\rho_1^2\rho_2 + d\rho_2^2)uv^2 \\ &\quad + d(\rho_1^3 + 3d\rho_1\rho_2^2)v^3 \\ &= 3(\rho_1^2 u^2 + 2d\rho_1\rho_2 uv + d^2\rho_2^2 v^2)(\rho_2 u + \rho_1 v) + d(\rho_2 u + \rho_1 v)^3 \\ &= 3u'^2 v' + dv'^3 \end{aligned}$$

so $\sigma(u, v) \in F_1$. Since F_r is smooth, σ is a morphism. Furthermore, it is easy to check that the map $\sigma' \colon (F_1)_{\overline{\mathbb{Q}}} \to (F_r)_{\overline{\mathbb{Q}}}, (u, v) \mapsto (\frac{\rho_1 u - \rho_2 dv}{t}, \frac{-\rho_2 u + \rho_1 v}{t})$ is well defined and provides an inverse for σ, so σ is an isomorphism. Furthermore, we have that if $r' = \gamma^3 r$ for some $\gamma \in \mathbb{Q}^*$, the curves F_r and $F_{r'}$ are isomorphic over $\mathbb{Q}$. Indeed: the map $F_{r'} \to Fr, (u, v) \mapsto (\gamma u, \gamma v)$

is an isomorphism (note that $N(\gamma) = \gamma^2$, so $N(r') = t^3\gamma^6$). Furthermore, up to isomorphism over $\mathbb{Q}$, there are only finitely many r for which F_r has a rational point (since $\mathrm{im}(q')$ is finite by Proposition 3.2.2).
Now, consider the projection map defined by

$$\pi_r \colon F_r \to \mathbb{P}^2, [U : V : W] \mapsto [tW(U^2 - dV^2) : r(U - V\delta)^3 + \delta W(at(U^2 - dV^2) + bW^3) : W^3].$$

(Note that this is in fact the composition of the restriction of the natural projection map $\overline{K_r} \to \mathbb{P}^2$ and the map determined by η'.) Then we have that every element in $E(\mathbb{Q})$ is the image under π_r for exactly one of the curves F_r up to isomorphism over $\mathbb{Q}$, so equivalently

$$E(\mathbb{Q}) = \bigcup_{[r] \in K_d^*/(K_d^*)^3} \pi_r(F_r(\mathbb{Q}))$$

(which is again a disjoint union consisting of only finitely many points).
Analogously to Proposition 3.3.3, there exists an isomorphism $\overline{f}_r \colon (F_r)_{\overline{\mathbb{Q}}} \to E_{\overline{\mathbb{Q}}}$ over $\overline{\mathbb{Q}}$. This can be shown using the fact that over $\overline{\mathbb{Q}}$, F_r is isomorphic to F_1, which is isomorphic to $\overline{K_1}$, then the proof is very similar to that of Proposition 3.3.3. In the same way, one can show that the analog of Proposition 3.3.4 still holds.

Appendix A

A.1 An isomorphism of C_t to a curve in Weierstrass form

Let $t \in \mathbb{Z} \setminus \{0\}$ be a nonzero integer and let C_t be the curve over $\mathbb{Q}$ in the weighted projective plane $\mathbb{P}(1,1,2)$ given by the equation $Z^2 = X^4 + tY^4$, together with the rational point $\mathcal{O} = [1:0:1]$. In Section 2.1, we have shown that $(C_t, \mathcal{O})$ is an elliptic curve, and we claimed that it is isomorphic to the elliptic curve $E_t : v^2 = u^3 - 4tu$ in Weierstrass form in $\mathbb{P}^2$ (which is indeed an elliptic curve, since the discriminant of the Weierstrass equation equals $-16 \cdot 4 \cdot 16t^2 \neq 0$). We will now establish this.

Proposition A.1.1. *Define the map*

$$\tau_t \colon C_t \to E_t, [X:Y:Z] \mapsto \left[2Y(Z+X^2) : 4(ZX+X^3) : Y^3\right]$$

then τ_t is an isomorphism.

Proof. We have that τ_t is a well defined, rational map because for all $[X:Y:Z] \in C_t$, we have that

$$\begin{aligned} 8Y^3(Z+X^2)^3 - 4tY^6(2Y(Z+X^2)) &= 8(Z+X)Y^3(Z^2+2ZX^2+X^4-tY^4) \\ &= 16(Z+X)^2X^2Y^3 = (4X(Z+X))^2Y^3 \end{aligned}$$

so $\tau_t([X:Y:Z]) \in E_t$, and since C_t is smooth, τ_t is a morphism. Furthermore, note that $\tau_t(\mathcal{O}) = [0:1:0] \in E_t$ so it is an isogeny.
We can define an inverse by

$$\tau_t^{-1} \colon E_t \to C_t, [U:V:W] \mapsto \left[WV : 2UW : 2U^3W - V^2W^2\right]$$

This is again a well defined rational map, since we have for all $[U:V:W] \in E_t$ that

$$\begin{aligned} (2U^3W - V^2W^2)^2 &= 4U^6W^2 - 4U^3W^3V^2 + W^4V^4 = 4U^6W^2 - 4U^3W^2(U^3 - 4tUW^2) + W^4V^4 \\ &= 16tU^4W^4 + W^4V^4 \end{aligned}$$

so $\tau_t^{-1}([U:V:W]) \in C_t$, from which we conclude that τ_t^{-1} is also a morphism. Furthermore, $\tau_t^{-1}([0:1:0]) = \mathcal{O}$ so τ_t^{-1} is an isogeny.
It remains to check that τ_t^{-1} provides an inverse for τ_t. Therefore, note that we have for all $[X:Y:Z] \in C_t$ that

$$\begin{aligned}(\tau_t^{-1} \circ \tau_t)[X:Y:Z] &= \tau_t^{-1}\left(\left[2Y(Z+X^2) : 4(ZX+X^3) : Y^3\right]\right) \\ &= [4Y^3X(Z+X^2) : 4Y^4(Z+X^2) : 16Y^6((Z+X^2)^3 - X^2(Z+X^2)^2)] \\ &= [X:Y:Z]\end{aligned}$$

On the other hand, we have for all $[U:V:W] \in E_t$ that

$$\begin{aligned}(\tau_t \circ \tau_t^{-1})([U:V:W]) &= \tau_t\left(\left[WV : 2UW : 2U^3W - V^2W^2\right]\right) \\ &= \left[8U^4W^2 : 8U^3W^2V : 8U^3W^3\right] = [U:V:W]\end{aligned}$$

Hence, τ_t is an isomorphism, which maps C_t into a curve in Weierstrass form. □

Note that once we know that τ_t is an isogeny, there is another way to show that it is an isomorphism: for $[X:Y:Z] \in C_t$, we have that $[X:Y:Z] \in \ker(\tau_t)$ if and only if $Y = 0$ and $Z + X^2 \neq 0$. It follows from the equation of C_t that $[X:Y:Z] = \mathcal{O}$, so the kernel of τ_t is trivial. Since τ_t is separable, we have that $\deg(\tau_t) = 1$, so τ_t is an isomorphism.

A.2 Smoothness of the Fermat curve

Let $n \geq 3$ be a positive integer and C be the curve over $\mathbb{Q}$ given by

$$X^n + Y^n = Z^n$$

in $\mathbb{P}^2$. Then C is a smooth curve. In order to see this, let $P = [a:b:c] \in C$ be a point, and assume $a \neq 0$. Then we consider the affine patch $1 + y^n = z^n$, where $y = \frac{Y}{X}$ and $z = \frac{Z}{X}$. Define $f(x,y) = 1 + y^n - z^n$, then we have that

$$\frac{\partial f}{\partial y}(P) = n\left(\frac{b}{a}\right)^{n-1} \text{ and } \frac{\partial f}{\partial z}(P) = -n\left(\frac{c}{a}\right)^{n-1} \text{ so if } \frac{\partial f}{\partial y}(P) = \frac{\partial f}{\partial z}(P) = 0$$

we must have $b^{n-1} = c^{n-1} = 0$, so $b = c = 0$. But since $a^n + b^n = c^n$, such P cannot exist. So the rank of $\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right)$ is always equal to 1, which means that C is smooth at P.
If $a = 0$, it follows from the equation of C that $b \neq 0$, and by symmetry, C is also smooth at P in that case. We conclude that C is smooth at all points $P \in C$.

Bibliography

[BL76] E.J. Barbeau and P.J. Leah. Euler's 1760 paper on divergent series. *Historia Mathematica*, 3(2):141 – 160, 1976.

[Bri15] M. Bright. Descent by 2-isogeny (after Cassels), 2015. (Used in the MasterMath course "Elliptic Curves").

[Cas91] J. W. S. Cassels. A 2-isogeny. In *24 Lectures on Elliptic Curves*, London Mathematical Society Student Texts, chapter 14. Cambridge University Press, Cambridge, 1991.

[Coh07] H. Cohen. Diophantine aspects of elliptic curves. In *Number Theory: Volume I: Tools and Diophantine Equations*, chapter 8. Springer-Verlag New York, New York, 2007.

[Eul70] L. Euler. *Vollständige Anleitung zur Algebra*. Royal Academy of Science, St. Petersburg, 1770. (In German).

[Fer91] P. de Fermat. Commentaire sur la question 24 du Livre VI de Diophante. In *Oeuvres de Fermat (Publiées par les soins de MM. Paul Tannery et Charles Henry sous les auspices du Ministre de l'instruction publique)*. Gauthier-Villars et fils, Paris, 1891. (In French).

[Har77] R. Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer-Verlag New York, New York, 1977.

[Rib99] P. Ribenboim. Special cases. In *Fermat's Last Theorem for Amateurs*, chapter 1. Springer-Verlag New York, New York, 1999.

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer-Verlag New York, New York, 2009.

[Sta18] The Stacks Project Authors. *Stacks Project*. `https://stacks.math.columbia.edu`, 2018.

[Ste17] P. Stevenhagen. Number rings, 2017. (Lecture notes for the MasterMath course "Algebraic Number Theory").

[The18] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.4)*, 2018. `http://www.sagemath.org`.

[vB10] M. van Beek. On elliptic curves of the form $y^2 = x^3+A(x-B)^2$, 2010. (Masterthesis).

[Wil95] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics*, 141(3):443–551, 1995.