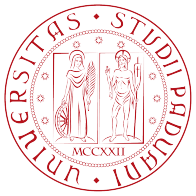
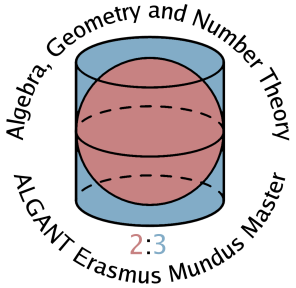
UNIVERSITÀ DEGLI STUDI DI PADOVA
Tesi di Laurea Magistrale

UNIVERSITÉ DE BORDEAUX
Mémoire de Master 2





ARITHMETIC
OF THE
MODULAR CURVE X(7)

Dino DESTEFANO

Advisor: Fabien PAZUKI

July 2014

a Margherita

Contents

Introduction

One of the most famous problems in diophantine geometry is the *Fermat's last theorem*, that states that the equation

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

has no nontrivial integer solutions if $n \geq 3$. This conjecture for centuries stimulated major developments in number theory and, as it is well known, is now a theorem (see [61] and [59]).
Then one can ask for the primitive integer solution of the *generalized Fermat's equation*:

$$Ax^p + By^q = Cz^r, \tag{2}$$

where A, B, C are nonzero integers and $p, q, r \in \mathbb{Z}_{\geq 1}$. A *primitive* solution (a, b, c) is a solution such that $\gcd(a, b, c) = 1$.
One important invariant linked to (2) is

$$\chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1, \tag{3}$$

that allows us to distinguish three cases:

1. The *spherical* case: $\chi > 0$.
   A simple calculation shows that the set $\{p, q, r\}$ is either of the form $\{2, 2, k\}$ with $k \geq 2$ or $\{2, 3, m\}$ with $m = 3, 4, 5$. In this case there are either no solution or infinitely many. In the latter case the solutions are given by a finite set of polynomial parametrizations of the equation, as proved in [5].

2. The *euclidean* case: $\chi = 0$.
   We can easily find that in this case the set $\{p, q, r\}$ equals one of $\{3, 3, 3\}$, $\{2, 4, 4\}$, $\{2, 3, 6\}$. In this case determing the solutions boils down to the determination of the rational points on twists of some elliptic curves over $\mathbb{Q}$ and we find that the set of solutions is finite. See [26].

3. The *hyperbolic* case: $\chi < 0$.
   In this case the number of solutions is at most finite, as proved in [23].

The method of *descent* is the key ingredient used in the proofs of these results: descent relates the primitive integer solutions to the rational points on one or more auxiliary curves of genus g, whose Euler characteristic $2 - 2g$ is a positive integer multiple of χ.

- In the spherical case, we have $\chi > 0$, so $2 - 2g > 0$. Hence we get $g = 0$, and the auxiliary curves are isomorphic to $\mathbb{P}^1$.
- In the euclidean case, from $\chi = 0$ we get $g = 1$ and thus, as previously mentioned, we should look for the rational points on some elliptic curves.
- In the hyperbolic case, we get that the auxiliary curves have $g > 1$, hence finitely many rational points by the theorem of Faltings [29].

A case of particular interest is the hyperbolic case with $A = B = C = 1$. In this case many explicit solutions are found (or the nonexistence of solutions is proved), as summarized in the following table:

$\{p, q, r\}$	notes	references
$\{n, n, n\}$	$n \geq 4$	[61], [59]
$\{n, n, 2\}$	$n = 5, 6, 9$ or $n \geq 7$ prime	[24]
$\{n, n, 3\}$	$n = 4, 5$ or $n \geq 7$ prime	[24]
$\{3, 3, n\}$	$n = 4, 5, 7, 11, 13$ or $17 \leq n \leq 10^9$	[37], [11], [10], [16], [20]
$(2, n, 4)$	includes $(4, n, 4)$	[22], [4]
$(2, 4, n)$	$n \geq 211$ prime	[28]
$(2n, 2n, 5)$	$n = 2, 3, 5$ or $n \geq 7$	[3], [10]
$(2, 2n, 3)$	n prime and $7 < n < 1000$ or $n \equiv -1 \pmod 6$	[14], [21]
$(2, 2n, 5)$	$n > 17$ prime or $n \equiv 1 \pmod 4$	[15]
$\{2, 4, 6\}$		[9]
$\{2, 4, 5\}$		[11]
$\{2, 3, 9\}$		[12]
$\{2, 3, 8\}$		[9], [11]
$\{2, 3, 7\}$		[46]

In the table above, the notation $\{p, q, r\}$ means that the solutions have been determined for every permutation of (p, q, r): this matters only if at least two between p, q, r are even.

The aim of this thesis is to show the tools and some steps to prove the case of $\{2, 3, 7\}$, following [46].
With the solution of this case, now we know the complete list of primitive solutions for every triple (p, q, r) of the hyperbolic case for which nontrivial primitive solutions (excluding $1^n + 2^3 = 3^2$) are known to exist.
The equation $x^2 + y^3 = z^7$ is of particular interest and difficulty for many reasons: First of all, it corresponds to the negative value of χ closest to 0. There exists a naive heuristic that predicts that when χ is negative but close to 0, the set of primitive integer solutions should be relatively large and that some solutions should involce large integers: then if we have big solutions, proving the nonexistence of others could be a difficult task. Indeed the equation has several solutions and some of them involve big integers, like $2213459^2 + 1414^3 = 65^7$. See theorem 2.2 for the complete list of solutions.
Moreover $2, 3, 7$ are primes, that means that we cannot use any parametrization to reduce some computations to previously known cases. Finally, to apply the descent,

we need to find a finite étale covers: this is relatively easy to do in the case of two exponents sharing a common factor. On the other hand, for $\{2, 3, 7\}$ the smallest nontrivial Galois étale covering has a nonabelian Galois group of order 168, as shown in chapter 3.

- In chapter 1 we will show some of the basic tools needed in the following.
- In chapter 2 we state the result and we present a detailed overview of the proof.
- In chapter 3 we will find a Galois étale covering and we will apply the descent method, thus reducing the problem to finding all the rational points on a finite set of twists of the Klein quartic curve X.
- In chapter 4 we exploit the isomorphism between X and the modular curve $X(7)$ to reduce the problem of finding the relevant twists to the classification of some $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules; eventually we explicitly find a list of ten equations describing the relevant twists.
- Finally, chapters 5 and 6 are devoted to finding all the rational points on the ten given curves using diffetent methods, for instance descent on the Jacobians of the curves, Mordell-Weil sieve and Chabauty-Coleman theory.

Chapter 1

Preliminaries

1.1 Algebraic geometry

We assume that the reader is familiar with the common notions in algebraic geometry like scheme, morphism, variety, étale cover, base change. Classical references for these notions are [33] and [39].
We will use a lot definition and tools about divisors, hence here there is a brief introduction that follows mostly [34, §A.2-§A.3].

Definition 1.1. Let X be an algebraic variety. The *group of Weil divisors on* X is the free abelian group generated by the closed subvarieties of codimension one on X. It is denoted by $\mathrm{Div}(X)$.

Example 1.2. If X is a curve, a divisor D on X is a finite formal sum $D = \sum n_P P$ where the n_P's are integers and the P's are points and we can define the *degree of* D to be $\deg(D) = \sum n_P$.

Definition 1.3. The *support* of the divisor $D = \sum n_Y Y$ is the union of all those Y's for which the multiplicity n_Y is nonzero. It is denoted by $\mathrm{supp}(D)$.

Definition 1.4. A divisor $D = \sum n_Y Y$ is *effective* or *positive* if every $n_Y \geq 0$.

Lemma 1.5. *Recall that if Y is an irreducible divisor, then $\mathcal{O}_{Y,X}$ denotes the local ring of functions that are regular in some neighborhood of some points of Y. In particular, if X is nonsingular, then $\mathcal{O}_{Y,X}$ is a discrete valuation ring. We write $\mathrm{ord}_Y : \mathcal{O}_{Y,X} \setminus \{0\} \longrightarrow \mathbb{Z}$ for the normalized valuation on $\mathcal{O}_{Y,X}$ and we can extend it to the field of fractions $k(X)$. Then this function has the following properties:*

a. $\mathrm{ord}_Y(fg) = \mathrm{ord}_Y(f) + \mathrm{ord}_Y(g)$ *for all* $f, g \in k(X)^\times$.

b. Fix $f \in k(X)^\times$. *There are only finitely many* Y*'s with* $\mathrm{ord}_Y(f) \neq 0$.

c. Let $f \in k(X)^\times$. *Then* $\mathrm{ord}_Y(f) \geq 0$ *if and only if* $f \in \mathcal{O}_{Y,X}$ *and* $\mathrm{ord}_Y(f) = 0$ *if and only if* $f \in \mathcal{O}_{Y,X}^\times$.

Proof. See [30, pp. 47-48]. □

Lemma 1.5 allows us to define the divisor of a function.

Definition 1.6. Let X be a variety, and let $f \in k(X)^\times$ be a rational function on X. The *divisor of* f is the divisor

$$\mathrm{div}(f) = \sum_Y \mathrm{ord}_Y(f) Y \in \mathrm{Div}(X).$$

Definition 1.7. A divisor is *principal* if it is the divisor of a function.

Definition 1.8. Two divisors D and D' are said to be *linearly equivalent* if $D - D' = \mathrm{div}(f)$ for some function $f \in k(X)^\times$. We will denote it by $D \sim D'$.

Definition 1.9. The *divisor class group* of X is the group of divisor classes modulo linear equivalence. It is denoted by $\mathrm{Cl}(X)$. The linear equivalence class of a divisor D is denoted by $\mathrm{Cl}(D)$ or by $[D]$.

Definition 1.10. A *Cartier divisor* on a variety X is an equivalence class of collections of pairs $(U_i, f_i)_{i \in I}$ satisfying the following conditions:

a. The U_i's are open sets that cover X.

b. The f_i's are nonzero rational functions $f_i \in k(U_i)^\times = k(X)^\times$.

c. $f_i f_j^{-1} \in \mathcal{O}(U_i \cap U_j)^\times$.

Two collections $\{(U_i, f_i) | i \in I\}$ and $\{(V_j, g_j) | j \in J\}$ are considered to be equivalent if $f_i g_j^{-1} \in \mathcal{O}(U_i \cap V_j)^\times$ for all $i \in I$ and $j \in J$.
The sum of two Cartier divisors is

$$\{(U_i, f_i) | i \in I\} + \{(V_j, g_j) | j \in J\} = \{(U_i \cap V_j, f_i g_j) | (i, j) \in I \times J\}.$$

The group of Cartier divisors of X is denoted by $\mathrm{CaDiv}(X)$. The group of Cartier divisors modulo linear equivalence is called the *Picard group* of X and is denoted by $\mathrm{Pic}(X)$.

Actually the notion of Cartier divisor generalize the notion of Weil divisor:

Lemma 1.11. *Let X be a smooth variety. Then the natural maps* $\mathrm{CaDiv}(X) \to \mathrm{Div}(X)$ *and* $\mathrm{Pic}(X) \to \mathrm{Cl}(X)$ *are isomorphisms.*

Proof. See [33, II.6.11]. □

If X is a curve, we denote by $\mathrm{Pic}^0(X)$ the subgroup of $\mathrm{Pic}(X)$ whose elements are divisors of degree 0 modulo linear equivalence.

Definition 1.12. Let X be a smooth variety of dimension n and let ω be a nonzero differential $n-form$ on X (Note that the value of a differential form at some point makes no sense, but asking ω is nonzero has a meaning). We can contruct a divisor associated to ω as follows. On any affine open subset U of X with local coordinates $x_1, \ldots, x_n$ we can write $\omega = f_U dx_1 \wedge \cdots \wedge x_n$ for some rational functions $f_U \in k(X)$. Then we define the divisor of ω to be the collection $\mathrm{div}(\omega) = \{(U, f_U)\}$. This is a well defined divisor on X independent on the coordinates. Any other nonzero

differential $n-form$ ω' on X has the form $\omega' = f\omega$ for some rational function $f \in k(X)^\times$. It follows immediately that

$$\mathrm{div}(\omega') = \mathrm{div}(\omega) + \mathrm{div}(f),$$

so that the divisor class of $\mathrm{div}(\omega) \in \mathrm{Pic}(X)$ is independent of the chosen form. This divisor class is called the *canonical class* of X, any divisor in the canonical class is called a *canonical divisor* of X.

Definition 1.13. Let D be a divisor on a variety X. The set $L(D)$ defined as follows:

$$L(D) = \{f \in k(C) | (f) + D \geq 0\}$$

is actually a vector space of finite dimension $\ell(D)$.

Definition 1.14. A *linear system* on a variety X is a set of effective divisors all linearly equivalent to a fixed divisor D and parametrized by a linear subvariety of $\mathbb{P}(L(D)) \simeq \mathbb{P}^{\ell(D)-1}$.

Example 1.15. The set of effective divisors linearly equivalent to D is a linear system called the *complete inear system* of D, denoted by $|D|$.

Definition 1.16. A linear system L on a projective variety X is *very ample* if the associated rational map $\phi_L : X \longrightarrow \mathbb{P}^n$ is an embedding. A divisor D is said to be *very ample* if the complete linear system $|D|$ is very ample. A divisor D is said to be *ample* if some positive multiple of D is very ample.

1.2 Algebraic curves, elliptic curves

The main references for the following definition and proofs are the books [56] and [34].

Definition 1.17. A *curve* is a projective variety of dimension 1.

Proposition 1.18. *Let $\phi : C_1 \to C_2$ be a morphism between two curves. Then ϕ is either constant or surjective (cf. [33, II.6.8]).*

Definition 1.19. Let $\phi : C_1 \to C_2$ be a map between two curves. If ϕ is constant, we define the *degree* of ϕ to be 0. Otherwise we say that ϕ is a *finite map* and we define its *degree* to be

$$\deg \phi = [K(C_1) : \phi^* K(C_2)].$$

Definition 1.20. Let C and C' be two curves defined over a field k of characteristic 0. We say that C' is a $k-twist$ of C if there exists an isomorphism between C and C' over an algebraic closure $\bar{k}$ of k, i.e. if there exist an isomorphism of curves $\phi : C \otimes \bar{k} \to C' \otimes \bar{k}$. If the curves are isomorphic over k, the twist is called *trivial*. If the curves are isomorphic over a field $k' \supset k$ such that $[k' : k] = 2$, the twist is called *quadratic*.

Theorem 1.21 (Riemann-Roch)**.** *Let C be a smooth (projective) curve and K_C a canonical divisor on C. There exists an integer $g \geq 0$ such that for all divisors $D \in \mathrm{Div}(C)$*

$$\ell(D) - \ell(K_C - D) = \deg(D) - g + 1$$

Proof. See [33, IV, §1] or [38, Ch.1] for a more elementary proof. □

Definition 1.22. The integer g is called the *genus* of the smooth curve C. When C is not smooth, its genus is defined to be the genus of the smooth projective curve that is birational to C.

Definition 1.23. A point P on an algebraic curve C of genus g is a *Weierstrass point* if there exist a non-constant rational function on C which has at this point a pole of order not exceeding g and which has no singularities at other points of C.

Theorem 1.24 (Faltings, previously Mordell's conjecture)**.** *Let C be a non-singular algebraic curve defined over a number field k. Then, if the genus of the curve is greater or equal to 2, C has finitely many k-rational points.*

Proof. See [29] for Faltings's original proof. For a relatively easier proof by Bombieri that uses Vojta's inequality, see [34, Part E]. □

Definition 1.25. An *elliptic curve* is a pair (E, O) where E is a nonsingular curve of genus 1 and $O \in E$. The elliptic curve is *defined over the field* K, written E/K, if E is defined over K as a curve and $O \in E(K)$.

Remark 1.26. In the following, if this do not bring confusion, we will denote by an elliptic curve simply by E.

Proposition 1.27. *The set of rational points of an elliptic curve is an abelian group with O as neutral element.*

Proof. See [56, III.2], where there are also explicit formulas for the group law. □

Proposition 1.28. *If* $\mathrm{char}(K) \neq 2, 3$ *then any elliptic curve defined over K can be represented (not uniquely) by an equation of the form $y^2 = x^3 + ax + b$, with $a, b \in K$ and the discriminant $\Delta = -16(4a^3 + b^3) \neq 0$. Such an equation is called a* Weierstrass equation *(cf. [56, III.1]).*

Theorem 1.29 (Mordell-Weil)**.** *If E is an elliptic curve defined over a number field k, then the group $E(k)$ of $k-$rational points is a finitely generated abelian group.*

Proof. See [56, VII]. □

Remark 1.30. The above theorem can be generalized in higher dimension. See Theorem 1.46.

Definition 1.31. Let (E, O) and (E', O') be two elliptic curves. An *isogeny* from E to E' is a morphism

$$\phi : E \to E' \text{such that } \phi(O) = O'.$$

Two elliptic curves E and E' are *isogenous* if there is an isogeny between them.

Remark 1.32. Note that, thanks to Proposition 1.18, an isogeny beteween two elliptic curves E and E' is either trivial (i.e. maps every point of E into O'), or is surjective.

Proposition 1.33. *Being isogenous is an equivalence relation between elliptic curves. (cf. [56, III.6.1]).*

Remark 1.34. Unless otherwise stated, from now on all the elliptic curves will be defined over a field K of characteristic zero.

Proposition 1.35. *Let E be an elliptic curve with Weierstrass equation $y^2 = x^3 + ax + b$, then the value*

$$j = 1728\frac{4a^3}{4a^3 + 27b^2},$$

*called the j-*invariant*, is an invariant of the curve indipendent on the choice of the Weierstrass equation. Moreover if E is defined over an algebrically closed field $\bar{K}$, two curves are isomorphic over $\bar{K}$ if and only if they have the same j-invariant (cf. [56, III.1, Proposition 1.4]).*

Definition 1.36. Let E/K be an elliptic curve. For $m \in \mathbb{Z}$, $m \neq 0$ define the *multiplication by m* to be the map $[m] : E(K) \to E(K)$ such that $P \mapsto P + \cdots + P$ (m times). The kernel of this map, denoted by $E[m]$, is the subgroup of $E(K)$ of points of order m.

Proposition 1.37. *Let E be an elliptic curve defined over an algebraically closed field $\bar{K}$ and let $m \in \mathbb{Z}$. Then:*

- $\deg[m] = m^2$
- *If $m \neq 0$, then*

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

Proof. See [56, III.6, Corollary 6.4]. □

Definition 1.38. Let E be an elliptic curve over $\mathbb{Q}$. The *conductor* of E is the product

$$N = \prod_p p^{f_p}$$

Where p runs trough all (finite) primes and f_p is defined as follows:

$$f_p = \begin{cases} 0, & \text{if } E \text{ has good reduction at } p \\ 1, & \text{if } E \text{ has multiplicative reduction at } p \\ \geq 2 & \text{if } E \text{ has additive reduction at } p, \end{cases}$$

The exact defininition of f_p in the case of bad additive reduction is slightly more complicated, but for our purposes it is enough to know that if $p \neq 2, 3$ then $f_p = 2$.

For a complete and detailed exposition about the conductor of an elliptic curve, see [55, Ch. V].

1.2.1 The Weil pairing

Let E be an elliptic curve over $\mathbb{Q}$ or, more generally, over any number field k. Let m be a positive integer. Then, over an algebraic closure $\bar{k}$, the group of $m-$torsion points $E[m]$ has the form $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, a free $\mathbb{Z}/m\mathbb{Z}$-module of rank 2 (cfr. 1.37). As for every free module, we have the determinant pairing $\det : E[m] \to \mathbb{Z}/m\mathbb{Z}$ which is of course independent on the choice of the basis. In any case, a major drawback is that the determinant pairing is not invariant under Galois action, that is if $P, Q \in E[m]$ and $\sigma \in \mathrm{Gal}(\bar{k}/k)$, then the values of $\det(P^\sigma, Q^\sigma)$ and $\det(P, Q)^\sigma$ may be different.
The aim is to define a similar pairing invariant under Galois action, using a primitive m^{th} root of unity ζ. We will follow mainly [56, III.8].
Recall that [56, III.3.5] on an elliptic curve E a divisor $\sum n_i(P_i)$ is principal (i.e. is the divisor of some function) if and only if $\sum n_i = 0$ and $\sum [n_i]P_i = O$.
Let $T \in E[m]$. Then there is a function $f \in \bar{K}(E)$ s.t.

$$\mathrm{div}(f) = m(T) - m(O). \tag{1.1}$$

Now let $T' \in E(\bar{K})$ be a point s.t. $[m]T' = T$. Similarly we find a function $g \in \bar{K}(E)$ s.t.

$$\mathrm{div}(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} (T' + R) - (R). \tag{1.2}$$

In fact to check that the sum of the divisor is O, we note that $\#E[m] = m^2$ and that $[m^2]T' = O$.
Looking carefully we find that the functions g^m and $f \circ [m]$ have the same divisor, so, up to multiplying f by a constant from $\bar{K}^*$, we may assume that $f \circ [m] = g^m$.
Now let $S \in E[m]$ be another $m-$torsion point. (It can be $S = T$). Then, for any point $R \in E$, we have:

$$g(R+S)^m = f([m]R + [m]S) = f([m]R) = g(R)^m.$$

Thus if we consider the function $g(R+S)/g(R)$ as a function of R, it takes only finitely many values: for every R it is a m^{th} root of unity. In particular, the morphism

$$E \to \mathbb{P}^1, \qquad S \mapsto \frac{g(R+S)}{g(R)}$$

is not surjective, so by proposition 1.18 it is constant.
So we are allowed to define a pairing

$$e_m : E[m] \times E[m] \to \boldsymbol{\mu}_m$$

by setting

$$e_m(S, T) = \frac{g(R+S)}{g(R)},$$

where $R \in E$ is any point such that $g(R+S)$ and $g(X)$ are both defined and nonzero and $\boldsymbol{\mu}_m$ is the group of m^{th} roots of unity.
This is called the *Weil e_m- pairing*.
This machinary satisfies all the properties that we were looking for:

Theorem 1.39. *The Weil e_m-pairing has the following properties:*

1. *It is bilinear.*
2. *It is alternating, that is $e_m(T,T) = 1$ for all $T \in E[m]$.*
3. *It is nondegenerate: if $e_m(S,T) = 1$ for all $S \in E[m]$, then $T = O$.*
4. *It is Galois invariant: For all $S, T \in E[m]$, we have $e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma)$ for all $\sigma \in G_{\bar{K}/K}$.*
5. *It is compatible: $e_{mm'}(S,T) = e_m([m']S, T)$ for all $S \in E[mm']$ and $T \in E[m]$.*

Proof. See [56, III.8, Proposition 8.1]. □

1.3 Abelian varieties

Intuitively, one can think of abelian varieties as a higher-dimensional generalization of elliptic curves. For references in this section, see [34] and [41].

Definition 1.40. An *abelian variety* is a projective variety that is also an algebraic group.

Actually, the name "abelian" is well chosen:

Lemma 1.41. *An abelian variety is a commutative algebraic group (cf. [34, A.7.1.3]).*

Definition 1.42. Let G_1 and G_2 be two algebraic groups. A map $\phi \in \mathrm{Hom}(G_1, G_2)$ is an *isogeny* if it is surjective, has finite kernel and $\dim G_1 = \dim G_2$. The cardinality of $\ker(\phi)$ is called the *degree* of the map.

Proposition 1.43. *Let A be an abelian variety of dimension g over an algebraically closed field $\bar{K}$ of characteristic 0. Then:*

a. The multiplication-by-m map $[m] : A \to A$ is an isogeny of degree m^{2g}.

b. $A[m] = \ker[m] \simeq (\mathbb{Z}m\mathbb{Z})^{2g}$

Proof. See [34, A.7.2.7]. □

Curves of genus $g \geq 2$ are not abelian varieties. However, we can embed canonically each such a curve in an abelian variety:

Theorem 1.44. *Let C be a smooth projective curve of genus $g \geq 1$. There exist an abelian variety* $\mathrm{Jac}(C)$*, called the* Jacobian *of C, and an injection $j : C \hookrightarrow \mathrm{Jac}(C)$, such that:*

- *Extend j linearly to divisors on C. Then j induces a group isomorphism between* $\mathrm{Pic}^0(C)$ *and* $\mathrm{Jac}(C)$*.*
- *For each $r \geq 0$, define the subvariety $W_r \subseteq \mathrm{Jac}(C)$ by*

$$W_r = j(C) + ... + j(C) \text{ (r copies).}$$

Then $\dim(W_r) = \min(r, g)$ and $W_g = \mathrm{Jac}(C)$. In particular, $\dim(Jac(C)) = g$.

- *Let $\Theta = W_{g-1}$. Then Θ is an irreducible ample divisor on* $\mathrm{Jac}(C)$.

Proof. See [34, A.8.1.1]. □

Remark 1.45. If C is an elliptic curve, i.e. if it is of genus 1 and has a rational point, we have that $C \simeq \mathrm{Jac}(C)$.

Theorem 1.46 (Mordell-Weil)**.** *Let A be an abelian variety defined over a number field k. Then the group $A(k)$ of $k-$rational points of A is finitely generated.*

Proof. See [34, Part C]. □

We say that $X = V/\Lambda$ is a *complex torus* if V is a $\mathbb{C}-$vector space and Λ is a full lattice of V.

Definition 1.47. Consider the complex torus $\mathbb{C}^g/\Lambda$ and let E be a skew-symmetric form $\Lambda \times \Lambda \to \mathbb{Z}$. Since $\Lambda \otimes \mathbb{R} = \mathbb{C}^g$, we can extend E to a skew-symmetric bilinear form $E_{\mathbb{R}} : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$. We say that E is a *Riemann form* if:

a. For all v, w we have $E_{\mathbb{R}}(iv, iw) = E_{\mathbb{R}}(v, w)$,

b. The associated Hermitian form is positive definite.

Definition 1.48. We say that a complex torus X is *polarizable* if admits a Riemann form.

Theorem 1.49. *A complex torus X is an abelian variety over $\mathbb{C}$ if and only if it admits a polarization.*

Proof. See [41, Theorem 2.8]. □

Proposition 1.50. *All complex tori of dimension* 1 *are polarizable. In other words, if Λ is a full $\mathbb{C}-$lattice, then $\mathbb{C}/\Lambda$ is an elliptic curve (cf. [34, A.5.0.3]).*

Definition 1.51. An algebraic curve C defined over $\mathbb{Q}$ has good reduction at some prime p if it is the generic fiber of some smooth proper curve defined over $\mathbb{Z}_p$.

Theorem 1.52 (Néron-Reduction modulo p)**.** *Let A be an abelian variety defined over $\mathbb{Q}_p$. Then there exists a canonical way to attach to A an algebraic group A_0 over $\mathbb{F}_p$.*

Remark 1.53. In fact Néron proves the following: the functor from smooth schemes over $\mathbb{Z}_p$,

$$S \mapsto \mathrm{Hom}_{\mathrm{Spec}\,\mathbb{Q}_p}(S \times_{\mathrm{Spec}\,\mathbb{Z}_p} \mathrm{Spec}\,\mathbb{Q}_p, A)$$

is representable over a smooth group scheme $\mathcal{A}$ over $\mathbb{Z}_p$. The scheme $\mathcal{A}$ is unique and we set

$$A_0 = \mathcal{A} \times_{\mathrm{Spec}(\mathbb{Z}_p)} \mathrm{Spec}(\mathbb{F}_p).$$

The scheme $\mathcal{A}$ is called *Néron model* of A.

Definition 1.54. We say that A has *good reduction at the prime* p if A_0 is an abelian variety.

Definition 1.55. Let B be an abelian variety defined over $\mathbb{Q}$. For each prime p, consider the abelian variety A defined over $\mathbb{Q}_p$ by the same equations of B and let A_0 be the algebraic group of theorem 1.52. Then the *Tamagawa number* of B at p is

$$c_{B,p} = \#\frac{A}{A_0}$$

Proposition 1.56. *Let C be an algebraic curve defined over $\mathbb{Q}$. If C has good reduction at some prime p, then its Jacobian J has good reduction at p.*

See [6] for details about Néron models and [54] for reduction of abelian varieties.

1.4 Galois cohomology

Introductory references to this section are [34, App. C.4-C.5] [1] and [56, App. B]. For a complete discussion, one can look at [53].

In the following let G be a finite or topological group and let A be a G-module. Denote the action of G on A by $(\sigma, a) \mapsto a^\sigma$.

Definition 1.57. The 0^{th} *cohomology group* of G *acting on* A is the group

$$\mathrm{H}^0(G, A) = A^G\{\alpha \in A | \alpha^\sigma = \alpha \text{ for all } \sigma \in G\}.$$

Definition 1.58. A map $\phi : G \to A$ is called a 1-*cocycle from* G to A if it satisfies

$$\phi(\sigma\tau) = \phi(\sigma)^\tau \phi(\tau) \text{ for all } \sigma, \tau \in G.$$

Two $1-$cocycles ϕ, ϕ' are said to be *cohomologous* if there exists an $a \in A$ such that

$$a^\sigma \phi(\sigma) = \phi'(\sigma)a \text{ for all } \sigma \in G.$$

This is an equivalence relation; the set of cohomology classes of $1-$cocycles is denoted by $\mathrm{H}^1(G, A)$ and is called the 1^{st} *cohomology group* of G *acting on* A.

Remark 1.59. If G is a topological group, for example the Galois group of an infinite extension, we will add the requirement that the cocycles should be continuous when A is given the discrete topology. For example, if A is finite, this amounts to requiring that each 1-cocycle factors through a finite quotient group of G.

Proposition 1.60. *Let X_0 be a quasi-projective variety defined over k. Then there is a natural bijection between the $k-$twists of X_0 and the cohomology set $\mathrm{H}^1(\mathrm{Gal}(\bar{k}/k), \mathrm{Aut}(X_0))$.*

Proof. See [34, App. C.5]. □

Now we list some classical properties of H^0 and H^1.

Proposition 1.61. *Let G be a group, and let A and A' be G-modules.*

[1] The book contains also a short but beautiful motivation to the subject: see pp.283-285.

a. *Let $f : A \to A'$ be a G-homomorphism, that is, an homomorphism that commutes with the action of G. Then f induces a natural homomorphism*

$$\begin{aligned} \mathrm{H}^1(G, A) &\longrightarrow \mathrm{H}^1(G, A') \\ [\phi] &\longmapsto [f \circ \phi] \end{aligned}$$

Now let $F : G' \to G$ be a homomorphism. Then G' acts on A via F, and induces a natural homomorphism

$$\begin{aligned} \mathrm{H}^1(G, A) &\longrightarrow \mathrm{H}^1(G', A) \\ [\phi] &\longmapsto [F \circ \phi]. \end{aligned}$$

b. *Let H be a subgroup of G. Then the map $\mathrm{H}^1(G, A) \to \mathrm{H}^1(H, A)$ from* a. *is called the* restriction map. *If further H is a normal subgroup of G, then G/H acts on A^H. In this case, the projection map $\pi : G \to G/H$ and the inclusion $A^H \hookrightarrow A$ induce the* inflation *map defined by the formula*

$$\begin{aligned} \mathrm{H}^1(G/H, A^H) &\longrightarrow \mathrm{H}^1(G, A) \\ [\phi] &\mapsto [\phi \circ \pi]. \end{aligned}$$

The following sequence, called the inflation-restriction sequence, *is exact:*

$$0 \longrightarrow \mathrm{H}^1(G/H, A^H) \xrightarrow{inf} \mathrm{H}^1(G, A) \xrightarrow{res} \mathrm{H}^1(H, A).$$

c. *Let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be a short exact sequence of G-modules. Then there is a canonical long exact sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{H}^0(G, A) &\xrightarrow{f} \mathrm{H}^0(G, B) \xrightarrow{g} \mathrm{H}^0(G, C) \\ &\xrightarrow{\delta} \mathrm{H}^1(G, A) \xrightarrow{f} \mathrm{H}^1(G, B) \xrightarrow{g} \mathrm{H}^1(G, C). \end{aligned}$$

The connecting homomorphism *δ is defined as follows. Let $c \in \mathrm{H}^0(G, C)$. Choose some $b \in B$ such that $g(b) = c$. Then for any $\sigma \in G$, we have*

$$g(b^\sigma - b) = g(b)^\sigma - g(b) = c^\sigma - c = 0 \text{ since } c \in \mathrm{H}^0(G, C) = C^G.$$

Thus b^σ is in $\ker(g) = Im(f)$, and the injectivity of f means that we obtain a well-defined element $f^{-1}(b^\sigma - b) \in A$. The map

$$\begin{aligned} G &\longrightarrow A \\ \sigma &\longmapsto f^{-1}(b^\sigma - b), \end{aligned}$$

is a cocycle representing the cohomology class of $\delta(c)$. Moreover, the long exact sequence gives rise to the following short exact sequene:

$$0 \longrightarrow C^G/g(B^G) \xrightarrow{\delta} \mathrm{H}^1(G, A) \xrightarrow{f} \mathrm{H}^1(G, B)[g] \longrightarrow 0.$$

Proof. These are very classical results. See for instance [56, App. B]. □

Theorem 1.62 (Hilbert's 90)**.** *Let k be a field and let k' be a (finite or infinite) Galois extension of k. Let $G = \mathrm{Gal}(k'/k)$. Then we have that $\mathrm{H}^1(G, k'^{\times}) = 1$.*

Proof. See [51, Ch. 10, Proposition 2]. □

Example 1.63. Let $\mathcal{G}_k = \mathrm{Gal}(\bar{k}/k)$ and let $\boldsymbol{\mu}_m \subset \bar{k}^{\times}$ be the group of m^{th} root of unity. The short exact sequence of $\mathcal{G}_k$-modules

$$0 \longrightarrow \boldsymbol{\mu}_m \longrightarrow \bar{k}^{\times} \xrightarrow{m} \bar{k}^{\times} \longrightarrow 0$$

induces the long exact sequence

$$0 \longrightarrow \boldsymbol{\mu}_m(k) \longrightarrow k^{\times} \xrightarrow{m} k^{\times} \xrightarrow{\delta} \mathrm{H}^1(\mathcal{G}_k, \boldsymbol{\mu}_m) \longrightarrow \mathrm{H}^1(\mathcal{G}_k, \bar{k}^{\times}).$$

By Hilbert's 90 (theorem 1.62) we have that $\mathrm{H}^1(\mathcal{G}_k, \bar{k}^{\times})$ is trivial. This implies that δ is an isomorphism, the *Kummer isomorphism*

$$k^{\times}/k^{\times m} \xrightarrow{\delta}{\simeq} \mathrm{H}^1(\mathcal{G}_k, \boldsymbol{\mu}_m).$$

Example 1.64. Let $\alpha : A \to B$ be an isogeny of two abelian varieties defined over k and let $\mathcal{G}_k = \mathrm{Gal}(\bar{k}/k)$. Then the short exact sequence of $\mathcal{G}_k$-modules

$$0 \longrightarrow \ker(\alpha) \xrightarrow{\iota} A(\bar{k}) \xrightarrow{\alpha} B(\bar{k}) \to 0$$

induces a long exact sequence

$$\begin{aligned} 0 &\longrightarrow \ker(\alpha)(k) \xrightarrow{\iota} A(k) \xrightarrow{\alpha} B(k) \\ &\xrightarrow{\delta} \mathrm{H}^1(\mathcal{G}_k, \ker(\alpha)) \xrightarrow{\iota} \mathrm{H}^1(\mathcal{G}_k, A(\bar{k})) \xrightarrow{\alpha} \mathrm{H}^1(\mathcal{G}_k, B(\bar{k})). \end{aligned}$$

This exact sequence gives rise to the following fundamental short exact sequence

$$0 \longrightarrow B(k)/\alpha A(k) \xrightarrow{\delta} \mathrm{H}^1(\mathcal{G}_k, \ker(\alpha)) \longrightarrow \mathrm{H}^1(\mathcal{G}_k, A(\bar{k}))[\alpha] \longrightarrow 0,$$

where $\mathrm{H}^1(\mathcal{G}_k, A(\bar{k}))[\alpha]$ denotes the kernel of the map

$$\alpha : \mathrm{H}^1(\mathcal{G}_k, A(\bar{k})) \longrightarrow \mathrm{H}^1(\mathcal{G}_k, B(\bar{k})).$$

Definition 1.65. Let $\alpha : A \to B$ be an isogeny of abelian varieties defined over a number field k and let M_k be the set of places of k. Let $\mathcal{G}_k = \mathrm{Gal}(\bar{k}/k)$ and for each $v \in M_k$ set $\mathcal{G}_v = \mathrm{Gal}(\bar{k}_v/k_v)$. The *Selmer group* of A with respect to α is the group

$$\mathrm{Sel}^{(\alpha)}(A/k) = \bigcap_{v \in M_k} \ker\{\mathrm{H}^1(\mathcal{G}_k, \ker(\alpha)) \longrightarrow \mathrm{H}^1(\mathcal{G}_v, A(\bar{k}_v))[\alpha]\}.$$

Definition 1.66. The *Tate-Shafarevich group* of A is the group

$$Ш(A/k) = \bigcap_{v \in M_k} \ker\{\mathrm{H}^1(\mathcal{G}_k, A(\bar{k})) \longrightarrow \mathrm{H}^1(\mathcal{G}_v, A(\bar{k}_v))\}.$$

Remark 1.67. From the exact sequence of example 1.64, we can now deduce the following exact sequence:

$$0 \longrightarrow B(k)/\alpha A(k) \longrightarrow \mathrm{Sel}^{(\alpha)}(A/k) \longrightarrow Ш(A/k)[\alpha] \longrightarrow 0.$$

Proposition 1.68. *Let $\alpha : A \to B$ be an isogeny of abelian varieties defined over a number field k. Then the Selmer group $\mathrm{Sel}^{(\alpha)}(A/k)$ is finite, hence by remark 1.67 also $Ш(A/k)[\alpha]$ is finite.*

Definition 1.69. Let k be a number field and let v be a place of k. Let $I_v \subset \mathrm{Gal}(\bar{k}_v/k_v)$ be an inertia for v. A cohomology class $\phi \in \mathrm{H}^1(\mathcal{G}_k, M)$ is *unramified at* v if its restriction to $H^1(I_v, M)$ is trivial. It is important to note that I_v is defined only up to conjugation, but the triviality or nontriviality of the restriction of ϕ does not depend on the choice of I_v.

Remark 1.70. It also possible to define the cohomology in the case of A not being an abelian group. See for instance [56, App. B.3] for a brief introduction to nonabelian cohomology.

1.5 Modular forms

The main references for the following definition and proofs are [43] and [55, Ch. I]. Another good reference is [35].
We will work with the complex upper half plane $\mathbb{H}$:

$$\mathbb{H} = \{z \in \mathbb{C} | \Im(z) > 0\}.$$

We want to study Riemann surfaces of the form $\Gamma\backslash\mathbb{H}$ for some discrete group Γ. The most obvious such Γ is the *full modular group* $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ that acts on $\mathbb{H}$ by homography.

Definition 1.71. For any positive integer N, define the *principal congruence subgroup of level N* to be:

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ s.t. } a \equiv 1, b \equiv 0, c \equiv 0, d \equiv 1 \mod N \right\}$$

Then we are mainly interested in *congruence subgroup* Γ of $\mathrm{SL}_2(\mathbb{Z})$ that are the ones that contains a principal congruence subgroup of some level N.

Proposition 1.72. *Let $Y(N) = \Gamma(N)\backslash\mathbb{H}$. Let $p : \mathbb{H} \to Y(N)$ be the projection map. Then there is a unique complex structure on $Y(N)$ such that a function f on a open subset U of $Y(N)$ is holomorphic if and only if $f \circ p$ is holomorphic on $p^{-1}U$.*

Proof. See [43, Proposition 2.7]. □

In this way, by composing with p, we get a bijection between holomorphic functions on some open $U \subset Y(N)$ and holomorphic functions of $p^{-1}U$ invariant under the action of $\Gamma(N)$, that is such that $f(\gamma z) = f(z)$ for each $\gamma \in \Gamma(N)$.
However, the Riemann surface $Y(N)$ is not compact, but it can be naturally compactified by adding a finite number of points (the "cusps"). The compactification of

$Y(N)$ is denoted by $X(N)$.
As an example, the compactification of $Y(1)$ can be symply obtained considering $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. Then $\Gamma(1)$ acts continuously on $\mathbb{H}^*$ and we can take the (compact) quotient space $\Gamma(1)\backslash\mathbb{H}^*$.

Similarly, if Γ is a subgroup of finite index of $\Gamma(1)$ we can define a compact Riemann surface $X(\Gamma)$ taking the quotient $\Gamma\backslash\mathbb{H}^*$ and putting an appropriate complex structure on it.

Definition 1.73. Let Γ be a subgroup of finite index in $\Gamma(1)$. A *modular function* for Γ is a meromorphic function on the compact Riemann surface $X(\Gamma)$.

In this way a modular function f for Γ can bee seen as an holomorphic function on $\mathbb{H}$ such that f is invariant under the action of Γ and that is meromorphic at the cusps. (For precise definition of being "meromorphic at the cusps", see [43, I.4]).

Definition 1.74. An *elliptic modular curve* is a curve of the form $\Gamma\backslash\mathbb{H}^*$ for Γ a congruence subgroup of $\Gamma(1)$.

Definition 1.75. Let Γ be a subgroup of finite index of $\Gamma(1)$. A *modular form of* γ *of weight* 2^k is an holomorphic function on $\mathbb{H}$ such that:

a. $f(\gamma z) = (cz + d)^{2k} \cdot f(z)$, for all $z \in \mathbb{H}$ and for all $\gamma \in \Gamma$.

b. $f(z)$ is holomorphic at the cusps of Γ.

Moreover, if f is zero at all the cusps, it is called a *cusp form*.

Definition 1.76. A *newform* of level N is a normalized cusp form of weight 2 for the full modular group, belonging to the new space at level N, that is a simultaneous eigenfunction for the Hecke operators.

See [43] and [55] for a complete explanation.

However one can think to newforms in term of their $q-$expansions:

$$f(z) = q + \sum_{n \geq 2} c_n q^n, \quad q = \exp(2\pi i z) \tag{1.3}$$

(In principle we could have $c_i \in \mathbb{C}$, but see below).

In the following we state some basic facts about newforms. For details and proofs, see as usual [43].

Theorem 1.77. *Let f be a newform with $q-$adic expansion as in (1.3)*

- *For each fixed positive integer N, there are only finitely many newforms f of level N.*
- *If f is a newform with coefficients c_i and $K = \mathbb{Q}(c_2, c_3, \dots)$ then K is a real number field.*
- *The coefficients c_i in fact belong to the ring of integer $\mathcal{O}_K$ of the number field K.*

- *If l is prime then*

$$|c_l^\sigma| \leq 2\sqrt{l} \qquad \text{for all embeddings } \sigma : K \hookrightarrow \mathbb{R}$$

Remark 1.78. We care only about newforms up to Galois conjugacy.

Remark 1.79. The number of newforms at a particular level N depends in a very erratic way on the level N.

Definition 1.80. If all the coefficients c_i of a newform f lie in $\mathbb{Q}$, then f is said to be *rational*.

Theorem 1.81 (Modularity theorem for Elliptic Curve, previously Taniyama-Shimura-Weil conjecture)**.** *Associated to any rational newform f of level N, there is an elliptic curve $E_f/\mathbb{Q}$ of conductor N such that for all primes $l \nmid N$*

$$c_l = a_l(E_f) \tag{1.4}$$

where c_l is the $l-$th coefficients in the $q-$expansion of f and $a_l(E_f) = l+1-\#E_f(\mathbb{F}_l)$. For any given positive integer N, the association $f \mapsto E_f$ is a bijection between rational newforms of level N and isogeny classes of elliptic curves of conductor N.

The proof is completed in a series of papers by many authors. See [61], [59], [25], [18] and finally [8].

1.5.1 Level-lowering

In this section we will describe a simplified version of Ribet's Level-Lowering theorem stated in [47].

We should use the language of Galois representations, but for our purpose the following is enough. (This presentation is essentialy due to Siksek [2, pp.151–179]).

Definition 1.82. Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N, suppose moreover that f is a newform (of weight 2) of level N' with $q-$expansion as in (1.3) and with coefficients c_i generating the number field K. Then we say that E *arises modulo p* from the newform f (writing $E \sim_p f$) if there is some prime ideal $\mathfrak{p}$ over p of K such that for almost all primes l, we have $a_l(E) \equiv c_l \mod \mathfrak{p}$.

Thanks to theorem 1.81, if f is a newform we know that it corresponds to some elliptic curve F. Then if E arises modulo p from f we can also say that $E \sim_p F$.

Proposition 1.83. *Suppose that E and F are elliptic curves over $\mathbb{Q}$ with conductors N and N' respectively. Suppose that $E \sim_p F$. Then for all primes l (even $p = l$).*

- *if $l \nmid NN'$ then $a_l(E) \equiv a_l(F) \mod p$ and*
- *if $l \nmid N'$, $l|N$ and $l^2 \nmid N$ then $l + 1 \equiv \pm a_l(F) \mod p$.*

Proof. See [36, pp. 262-264]. □

Let E be, as usual, an elliptic curve over $\mathbb{Q}$. Let Δ be the *minimal* discriminant of E and N its conductor. Suppose p is a prime and define

$$N_p = N \Big/ \prod_{\substack{q|N,\ q^2 \nmid N \\ p|ord_q(\Delta)}} q.$$

Theorem 1.84 (Simplified Ribet's Level-Lowering)**.** *Let E be an elliptic curve over $\mathbb{Q}$ and let $p \geq 5$ be a prime. Suppose moreover that E does not have isogenies of degree p. Then there exists a newform f of level N_p such that $E \sim_p f$.*

Proof. See [47] for Ribet's original statement and proof. □

1.5.2 Moduli varieties

Heuristically, *moduli varieties* are geometrical spaces that classifies some algebro-geometric object. Once again, an (introductory) reference is [43].

Definition 1.85. Let k an algebraically closed field. A *moduli problem* over k is a contravariant functor $\mathcal{F}$ from the category of algebraic varieties over k to the category of sets. In particular for each $k-$variety V we are given a set $\mathcal{F}(V)$ and for each regular map $\phi : W \to V$ of $k-$varieties we are given a map $\mathcal{F}(\phi) : \mathcal{F}(V) \to \mathcal{F}(W)$.

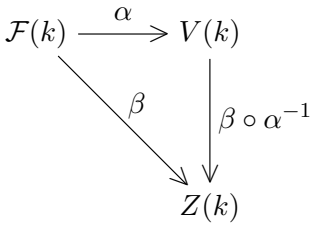
Remark 1.86. Most of the times $\mathcal{F}(V)$ is taken to be the set of isomorphism classes of some objects over V.

Definition 1.87. A pair (V, α), consisting of a $k-$variety and of a bijection $\alpha : \mathcal{F}(k) \to V(k)$; is a *solution to the moduli problem* if it satisfies the following conditions:

a. Let T be a variety over k and let $f \in \mathcal{F}(T)$; a point $t \in T(k)$ can be viewed as a map m-Spec$(k) \to T$, and so by functoriality f defines an element f_t of $\mathcal{F}_t$; we therefore have a map $[t \mapsto \alpha(f_t)] : T(k) \to V(k)$ and we require this map to be regular (i.e. defined by a morphism of algebraic varieties),

$$\begin{aligned} T(k) \to V(k) \qquad & f \in \mathcal{F}(T) \\ t \mapsto \alpha(f_t) \quad & f_t = \mathcal{F}(t)(f) \in \mathcal{F}(k). \end{aligned}$$

b. Let Z be a $k-$variety and let $\beta : \mathcal{F}(k) \to Z(k)$ be a map such that, for every pair (T, f) as in [a.], the map $t \mapsto \beta\mathcal{F}(t) : T(k) \to Z(k)$ is regular, then the map $\beta \circ \alpha^{-1} : V(k) \to Z(k)$ is required to be regular:



A variety V that arises as a solution of a moduli problem is called a *moduli variety*.

Remark 1.88. The condition [b.] implies that there is at most one solution, up to isomorphism, to a moduli problem.

Remark 1.89. The above definitions can be generalized to a field k_0 which is not algebraically closed. Supposing k_0 to be perfect with algebraic closure k, now we take V to be a k_0-variety and α to be a family of maps $\alpha(k') : \mathcal{F}(k') \to V(k')$ (for each k' algebraic extension of k) compatible with the inclusions of fields, and $(V_k, \alpha(k))$ is required to be a solution of the moduli problem over k.

In this last construction we do not require $\alpha(k')$ to be a bijection when k' is not algebraically closed, so that, in general, V does not represent the functor $\mathcal{F}$. This yields to the following definition:

Definition 1.90. If V represents the functor $\mathcal{F}$ is called a *fine* moduli variety; otherwise is called a *coarse* moduli variety.

Example 1.91. Let V be a variety over a field k_0. A *family of elliptic curves over* V is a map of algebraic varieties $E \to V$ such that the coefficients of the Weierestrass equation of E are regular function on V.
For a variety V, let $\mathcal{E}(V)$ be the set of isomorphism classes of elliptic curves over V. Then $\mathcal{E}$ is a contravariant functor, so we can see it as a moduli problem over k_0. For every field k' containing k_0, the $j-$ invariant (1.35) defines a maps

$$\begin{aligned} \mathcal{E}(k') &\to \mathbb{A}^1(k') = k' \\ E &\mapsto j(E) \end{aligned}$$

that is an isomorphism if k' is algebraically closed. In general we have the following result:

The pair $(\mathbb{A}^1, j)$ is a solution to the moduli problem $\mathcal{E}$.

Y(N) as moduli variety

Definition 1.92. Let N be a positive integer. A *primitive level N structure* on an elliptic curve E is a pair of points $t = (t_1, t_2)$ in $E(k)$ such that the maps

$$\begin{aligned} \frac{\mathbb{Z}}{N\mathbb{Z}} \times \frac{\mathbb{Z}}{N\mathbb{Z}} &\to E(k) \\ (m, m') &\mapsto (mt_1, mt_2) \end{aligned}$$

is injective. This means that $E(k)[N]$ has order N^2 and that t_1 and t_2 form a basis for $E(k)[N]$ as a $\mathbb{Z}/N\mathbb{Z}$-module.

Let now $\zeta \in \mathbb{C}$ be a primitve $N-$th rooth of unity. For any variety V over a field $k \supseteq \mathbb{Q}(\zeta)$, we define $\mathcal{E}_N(V)$ to be the set of isomorphism classes of pairs (E, t), where E is an elliptic curve over V and t is a level-N structure on E s.t. $e_N(t_1, t_2) = \zeta$, where e_N is the e_N-Weil pairing defined in 1.2.1. Then $\mathcal{E}_N$ is a contravariant functor, hence a moduli problem:

Proposition 1.93. *The map*

$$\begin{aligned}\mathbb{H} &\to \mathcal{E}_N(\mathbb{C}) \\ \tau &\mapsto \Big(\mathbb{C}/\Lambda(\tau,1), (\tau/N, 1/N) \mod \Lambda(\tau,1)\Big)\end{aligned}$$

induces a bijection $\Gamma(N) \to \mathcal{E}_{\mathbb{C}}$*, where* $\Lambda(\tau,1)$ *is the* $1-$*dimensional lattice* $\Lambda = \tau\mathbb{Z} + \mathbb{Z}$*. (*$\mathbb{C}/\Lambda$ *is an elliptic curve by Proposition 1.50) (cf. [43, Lemma 8.7]).*

Theorem 1.94. *Let* k *be a field containing* $\mathbb{Q}[\zeta]$*, where* ζ *is a primitive* N*-th root of unity. Then the moduli problem* $\mathcal{E}$ *has solution* (M, α) *over* k*. When* $k = \mathbb{C}$*,* M *is canonically isomorphic to* $Y(N)_{\mathbb{C}}$*. Let* M *be the solution of moduli problem* $\mathcal{E}_N$ *over* $\mathbb{Q}[\zeta]$*. Then* M *has good reduction at the prime ideals not dividing* N*.*

Proof. See [42, §1]. □

Chapter 2

The theorem: solving $x^2 + y^3 = z^7$

2.1 The theorem

We begin now the explanation of the main paper [46].

Definition 2.1. Fix integers $p, q, r \geq 1$. An integer solution (x, y, z) to

$$x^p + y^p = z^r$$

is called *primitive* if $\gcd(x, y, z) = 1$

Theorem 2.2. *The primitive integer solution to the equation* $x^2 + y^3 = z^7$ *are the* 16 *triples:*

$$(\pm 1, -1, 0), (\pm 1, 0, 1), \pm(0, 1, 1), (\pm 3, -2, 1), (\pm 71, -17, 2), (\pm 2213459, 1414, 65),$$

$$(\pm 15312283, 9262, 113), (\pm 21063928, -76271, 17).$$

Remark 2.3. The condition on the gcd is really necessary: for example, if $a+b = c$, multiplying by $a^{21}b^{14}c^6$ we get that

$$(a^{11}b^7c^3)^2 + (a^7b^5c^2)^3 = (a^3b^2c)^7,$$

finding infinitely many easy solutions to $x^2 + y^3 = z^7$.

2.2 Notations

- $S_A = \text{Spec}\left(\frac{A[x,y,z]}{(x^2+y^3-z^7)}\right) \setminus \{(x, y, z)\}$, where A is any commutative ring. (The quasi-affine subscheme obtained from $x^2 + y^3 = z^7$ removing the trivial point $x = y = z = 0$);
- $S(\mathbb{Z})$ the set of (primitive) integer solutions to $x^2 + y^3 = z^7$;
- k a number field;
- $\mathcal{G}_k = Gal(\overline{\mathbb{Q}}/k)$. If $k = \mathbb{Q}$, often we will simply denote $\mathcal{G}_{\mathbb{Q}}$ by $\mathcal{G}$;
- $R = \mathbb{Z}[1/42]$;
- $G = \text{PSL}_2(\mathbb{F}_7)$ the smallest Hurwitz group.

2.3 Overview of the strategy

First of all, in **chapter 3** we will look for a suitable étale Galois cover of $S_{\mathbb{Z}}$. We will find that the smallest possible Galois cover X that allows us to apply the *descent* method has $G = \mathrm{PSL}_2(\mathbb{F}_7)$ as Galois group. After identifying X to be the Klein quartic curve, a (nonabelian) descent argument will reduce our problem to explicitly find the relevant twists X' of X together with some maps π' that will allow us to recover the "true" solutions in $S(\mathbb{Z})$ from the rational points on the twists X'.

In **chapter 4** we will sketch the construction of the modular curve $X(7)$ (see also section 1.5.2). Then the isomorphism between $X(7)$ and X allows us to reduce our problem further to the classification of some of the *symplectic twists* of a specific $\mathcal{G}_{\mathbb{Q}}$-module, up to quadratic twist. We will show then that there is one way to assign to each elliptic curve over $\mathbb{Q}$ two of the relevant twists of $X(7)$, thus requiring us to classify the possible $E[7]$, seen as $\mathcal{G}_{\mathbb{Q}}$-module. This will be done first in the case of $E[7]$ reducible and then in the case of $E[7]$ irreducible. With a little bit of theory about *covariants* then we will finally find an explicit list of ten equations describing the relevant twists of X. Moreover we will give a formula for the maps π' of chapter 1.

At this point what is left to do is to find all the $\mathbb{Q}$-rational points on the ten curves. This task is far from being trivial and we will start by constructing the Jacobian of each of the given curves. The aim of **chapter 5** is to compute the Mordell-Weil ranks of the ten Jacobians. For three of them this will be sketched using an argument previously appeared in literature. For the remaining seven, a different cohomological descent argument will be shown in details. The basic idea in the latter case is to exploit an analogy between the Klein quartic X with *triangles* of its inflection points with a genus-3 hyperelliptic curve with its Weierstrass points.

Finally, in **chapter 6**, we will show that all the rational points that one can find on the ten curves with a naive search (listed in appendix B) are actually all the rational points on those curves. To do that we will first briefly explain two classical tools in the theory of rational points: the Mordell-Weil sieve and the Chabauty-Coleman method. Finally, we will sketch these arguments applied to the curves. We will discover that one of the curve cannot be treated in the same way as the others and we will give for it the sketch of an ad-hoc argument.

Chapter 3

Descent

3.1 Étale covers

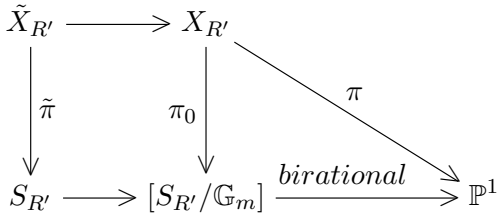
To apply the descent method, we need a finite étale cover of $S_{\mathbb{Z}}$ or at least of $S_{\mathbb{Z}[1/N]}$ for some $N \geq 1$. First, we will find such a cover for $S_{\mathbb{C}}$.
Using some basics facts about *stacks*, we find that a convenient cover of $S_{\mathbb{C}}$ is $X_{\mathbb{C}}$ s.t $\mathrm{Aut}(X_{\mathbb{C}}) = G = \mathrm{PSL}_2(\mathbb{F}_7)$, the smallest Hurwitz group, of order 168.
Now, using the Hurwitz formula for *orbifolds* (see the Remark 3.2), we recognize $X_{\mathbb{C}}$ to be the only genus 3 curve with 168 automorphism, the Klein quartic curve defined by the equation

$$X^3Y + Y^3Z + Z^3X = 0. \tag{3.1}$$

A good reference for many facts about this curve and its automorphism group G is [27].
To be able to apply the descent method later (Section 3.2), we work with the stack quotient $[S_{\mathbb{C}}/\mathbb{G}_m]$ (that is birational to $\mathbb{P}^1(\mathbb{C})$), so that we actually consider $\tilde{X}_{\mathbb{C}}$ the base extension of $X_{\mathbb{C}}$ by the projection $S_{\mathbb{C}} \to [S_{\mathbb{C}}/\mathbb{G}_m]$.

Similarly we define, with the same equations, the varieties X, $\tilde{X}$ over $\mathbb{Q}$ and X_R $\tilde{X}_R$ over the ring $R = \mathbb{Z}[1/42]$. This particular choice will allow us to apply the descent method as in R we have $2, 3$ and 7 invertibles (since $42 = 2 \cdot 3 \cdot 7$).
The map $\tilde{X}_{\mathbb{C}} \to S_{\mathbb{C}}$, of degree 168, arises from a map $\tilde{\pi} : \tilde{X}_R \to S_R$; the associated morphism π will be explicitly described later. (See Section 3.2 and Lemma 4.15).

The situation is shown by the following diagram:



Here the maps $\tilde{\pi}, \pi_0, \pi$ are of degree 168. The schemes can be considered either over $\mathbb{C}$ or more generally over any ring R' containing R.
On the bottom row, the map $j : S \to \mathbb{P}^1$ arises from our construction and is defined

by

$$(a, b, c) \longmapsto \frac{1728b^3}{c^7} \tag{3.2}$$

Remark 3.1. The map defined by the equation (3.2) is a crucial point: looking for the subfield of the function field $\mathbb{C}(S_{\mathbb{C}})$, we choose $\mathbb{C}(j)$ where $j = 1728y^3/z^7$. We do this because we would like to have the quotient $S_{\mathbb{C}}$ by the action of $\mathbb{G}_m$ being birational to $\mathbb{P}^1$. (Note that this choice is not unique, but it will lead to easier computations). What we will do at the end will be to find explicit values for j and from them recovering the triples (a, b, c) with $a^2 + b^3 = c^7$ (cf. Remark 4.17).

Remark 3.2. For (very) basic facts about stacks, see for example [31]. For orbifolds one can look at [44] and [1].
$[S/\mathbb{G}_m]$ is not a scheme, but one can think about it as $\mathbb{P}^1$ except that the points $1728, 0$ and ∞ are replaced by a $\frac{1}{2}-$point, a $\frac{1}{3}-$point, and a $\frac{1}{7}-$point, respectively. See [1] for details.

3.2 The first descent

Since G is not abelian we have to work with nonabelian cohomology, in this case $\mathrm{H}^1(\mathcal{G}_{\mathbb{Q}}, G)$ is simply a pointed set. From descent theory [57, §5.3], we get that:

- The set of classes in the Galois cohomology set $\mathrm{H}^1(\mathcal{G}_{\mathbb{Q}}, G)$ that are unramified outside $2, 3$ and 7 is finite.
- Each such class corresponds to an isomorphism class of twists $\tilde{\pi}' : \tilde{X}' \to$ of $\tilde{\pi} : \tilde{X} \to S$.
- the set $S(R)$ is the disjoint union of the sets $\tilde{\pi}'(\tilde{X}'(R))$.

Remark 3.3. Recall that (cf. definition 1.69) an element of $\mathrm{H}^1(\mathcal{G}_{\mathbb{Q}}, G)$ is unramified at p if its restriction in $\mathrm{H}^1(I_p, G)$ is trivial, where I_p is the inertia group of p. Thus "unramified outside $2, 3, 7$", for an element of $\mathrm{H}^1(\mathcal{G}_{\mathbb{Q}}, G)$, means that its restriction to $\mathrm{H}^1(I_p, G)$ is trivial for all $p \neq 2, 3, 7$.

So choosing a cocycle in a class of $\mathrm{H}^1(\mathcal{G}_{\mathbb{Q}}, G)$, we are able to construct an isomorphism class of twists of X. Actually each such cocycle twist the upper half of the square

$$\begin{array}{ccc} \tilde{X} & \longrightarrow & X \\ \downarrow{\scriptstyle \tilde{\pi}} & & \downarrow{\scriptstyle \pi} \\ S & \xrightarrow{\ j\ } & \mathbb{P}^1 \end{array} \quad \text{obtaining} \quad \begin{array}{ccc} \tilde{X}' & \longrightarrow & X \\ \downarrow{\scriptstyle \tilde{\pi}'} & & \downarrow{\scriptstyle \pi'} \\ S & \xrightarrow{\ j\ } & \mathbb{P}^1 \end{array}$$

Since $\operatorname{Pic} R$ is trivial, each map $\tilde{X}'(R) \to X'(R)$ is surjective. Thus we have $S(\mathbb{Z}) \subseteq S(R) = \bigcup j^{-1}(\pi'(X'(\mathbb{Q})))$; so that in the following we will need to do:

a. Find explicitly the equations for each twist X' and the maps π' arising from cocycles unramified outside $2, 3, 7$.

b. Determine $X'(\mathbb{Q})$ for each twist X'.

Remark 3.4. Note that, since X' has genus 3, $X'(\mathbb{Q})$ is finite by the theorem of Faltings 1.24.

Remark 3.5. The task [b.] is obviously not know to reduce to a finite computation, in general.

Remark 3.6. Since we want to find only $S(\mathbb{Z})$ and not all $S(R)$, we will compute only the rational points inside some "residue classes" on each curve: see section 3.3.

3.3 The local test

Definition 3.7. We say that the curve X' *passes the local test* if the subset $\pi'(X'(\mathbb{Q}_p))\cap j(S(\mathbb{Z}_p)$ of $\mathbb{P}^1(\mathbb{Q}_p)$ is nonempty for all primes p.

Hence our task actually will be:

a.' For each X' passing the local test, find an equation for X' and a formula for π'. (See Lemma 4.15 for the latter).

b.' For each such X', determine the set $\{P \in X'(\mathbb{Q}) : \pi'(P) \in j(S(\mathbb{Z})_p))$ for all primes $p\}$.

Chapter 4

Finding the twists of $X(7)$

4.1 Modularity

In this part of the proof, we observe that the map $j : X \to \mathbb{P}^1$ is equivalent to a map of modular curves $X(7) \to X(1)$: this will help us finding the required twists of X.

Here, in contrast with what was said in section 1.5, the construction of the modular curves $X(7)$ and $X(1)$ is algebraic: starting from $Y(N)$ as given in section 1.5.2, we take $X(N)$ to be its usual compactification. Details can be found in [43]. Recall that if E is an elliptic curve defined over a number field k, then $E[m]$ denotes the kernel of the multiplication by $m \in \mathbb{Z}_{\geq 1}$ on the k-rational points; moreover $E[m]$ has a natural structure of $\mathcal{G}_k$-module.

4.1.1 Twists of $X(7)$ associated to elliptic curves

Let $Y(1)$ be the (coarse) moduli space of elliptic curves over $\mathbb{Q}$. By Example 1.91, we know that $Y(1) \simeq \mathbb{A}^1$ and so $X(1) = \mathbb{P}^1$. The forgetful functor mapping a pair (E, ϕ) to E induces a morphism $Y(7) \to Y(1)$ and thus a morphism $X(7) \to X(1)$.

Definition 4.1. Now let M_k be the $\mathcal{G}_k$-module $\boldsymbol{\mu}_7 \times (\mathbb{Z}/7\mathbb{Z})^3$. When we write $\phi : M_k \tilde{\to} E[7]$, we mean that ϕ is a *symplectic isomorphism*, that is, an isomorphism of $\mathcal{G}_k$-modules such that $\bigwedge^2 \phi : \bigwedge^2 M_k \to \bigwedge^2 E[7]$ is the identity $\boldsymbol{\mu}_7 \to \boldsymbol{\mu}_7$.

Remark 4.2. From the isomorphism $M_{\bar{\mathbb{Q}}} \simeq (\mathbb{Z}/7\mathbb{Z})^2$ mapping (ζ^a, b) to the column vector $\begin{pmatrix} a \\ b \end{pmatrix}$ induces the following equality on the groups of symplectic automorphisms of $M_{\bar{\mathbb{Q}}}$:

$$\mathrm{Aut}_\Lambda(M_{\bar{\mathbb{Q}}}) = \mathrm{Aut}_\Lambda((\mathbb{Z}/7\mathbb{Z})^2) = \mathrm{SL}_2(\mathbb{F}_7)$$

Lemma 4.3. *Over $\bar{\mathbb{Q}}$, the covering $X(7) \to X(1)$ is Galois, moreover we have that*

$$\mathrm{Gal}(X(7)_{\bar{\mathbb{Q}}}/X(1)_{\bar{\mathbb{Q}}}) \simeq G = \mathrm{PSL}_2(\mathbb{F}_7).$$

(cf. [46, 4.2]).

Now we note (see [27] for many details) that X and $X(7)$ are isomorphic as $\mathbb{Q}$-varieties. However, the isomorphism is not unique, so we choose a particular

one that will lead to easier computations: in this way we get that the isomorphism $X(1) \to \mathbb{P}^1$ is the standard one given by the $j-$invariant; suppose $(a,b,c) \in S(\mathbb{Z})$ and a,b,c nonzero. Then $j = 1728b^3/c^7$ is not $1728, 0$ or ∞. The corresponding point on $X(1)$ is represented by the elliptic curve

$$E = E_{(a,b,c)} : Y^2 = X^3 + 3bX - 2a.$$

(to verify that this works, one has just to recall that $(a,b,c) \in S(\mathbb{Z})$ means $a^2 + b^3 = c^7$).

$$S(\mathbb{Z}) \xrightarrow{\quad j \quad} \mathbb{P}^1 \longrightarrow X(1)$$

$$(a,b,c) \longmapsto \frac{1728b^3}{c^7} \longmapsto E_{(a,b,c)}$$

Since $\mathcal{G}_\mathbb{Q}$ acts on $M_{\overline{\mathbb{Q}}}$, it acts also on $\mathrm{Aut}_\Lambda(M_{\overline{\mathbb{Q}}})$. The homomorphism $\mathrm{Aut}_\Lambda(M_{\overline{\mathbb{Q}}} \longrightarrow \mathrm{Aut}(X(7)_{\overline{\mathbb{Q}}})$ is clearly $\mathcal{G}_\mathbb{Q}$-equivariant, so we can find the following cohomological map:

$$\mathrm{H}^1(\mathcal{G}_\mathbb{Q}, \mathrm{Aut}_\Lambda(M_{\overline{\mathbb{Q}}})) \longrightarrow \mathrm{H}^1(\mathcal{G}_\mathbb{Q}, \mathrm{Aut}(X(7)_{\overline{\mathbb{Q}}})),$$

that can be seen as a map

$$\gamma : \{\text{symplectic twists of } M\} \longrightarrow \{\text{twists of } X(7)\}$$

where by *symplectic twist* of M we mean a $\mathcal{G}_\mathbb{Q}$-module M' with an isomorphism $\bigwedge^2 M' \simeq \boldsymbol{\mu}_7$ such that there is an isomorphism $\iota : M_{\overline{\mathbb{Q}}} \to M'_{\overline{\mathbb{Q}}}$ such that $\bigwedge^2 \iota$ is the identity $\boldsymbol{\mu}_7 \to \boldsymbol{\mu}_7$ over $\overline{\mathbb{Q}}$.
Let $X_{M'}(7)$ be the image trough γ of M'. Then $X_{M'}(7)$ is the smooth projective model of the smooth affine curve whose points classify pairs (E,ϕ) where E is an elliptic curve and $\phi : M' \hat{\simeq} E[7]$.

Remark 4.4. Since by Lemma 4.3 acts as automorphism of $X(7)_{\overline{\mathbb{Q}}}$ over $X(1)_{\overline{\mathbb{Q}}}$, there is a canonical morphism $X_{M'} \to X(1)$. From the moduli space point of view, this is nothing else that the forgetful functor mapping (E,ϕ) to E.

Definition 4.5. Now let E be an elliptic curve over $\mathbb{Q}$. Define $X_E(7) = X_{E[7]}(7)$ and define $X_E^-(7) = X_{E[7]^{-1}}(7)$, where $E[7]$ is saw as a $\mathcal{G}_\mathbb{Q}$-module and $E[7]^{-1}$ is one induced from $E[7]$ by the map

$$\begin{aligned} \boldsymbol{\mu}_7 &\to \boldsymbol{\mu}_7 \\ \alpha &\mapsto \alpha^{-1}. \end{aligned}$$

Remark 4.6. By our construction, if E is an elliptic curve and F is a quadratic twist of E, then $X_E(7) \simeq X_F(7)$ and $X_E^-(7) \simeq X_F^-(7)$.

Lemma 4.7. *Let $\mathcal{G} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. To classify relevant twists X' of X of section 3.2 for which $j \in \pi'(X'(\mathbb{Q}))$, it suffices to list the possibilities for the $\mathcal{G}$-module $E[7]$, up to quadratic twist (cf. [46, Lemma 4.4]).*

So we begin finding restriction on $E[7]$:

Definition 4.8. Suppose that we have ρ_p a Galois representation of $\mathcal{G}_{\mathbb{Q}}$ that takes value in $\mathrm{GL}_2(\mathbb{F}_p)$ and so defines an étale group scheme of type (p,p) over the field $\mathbb{Q}_p$. If this group scheme extends to a group scheme over $\mathbb{Z}_p$ that is finite and flat, we say that the representation ρ_p is *finite* at p.

See [52, p.189] for the definition in its original context and for more details.

Lemma 4.9. *If $(a,b,c) \in S(\mathbb{Z})$ and a,b,c are nonzero, then $1728b^3/c^7$ is the j-invariant of an elliptic curve E over Q such that*

a. the conductor N of E is of the form $N = 2^r 3^s \prod_{P\in T} p$ where $r \leq 6$, $s \leq 3$, and T is a finite set of primes ≥ 5.

b. $E[7]$ is finite at 7 in the sense of definition 4.8.

Proof. For (a.) it's pretty much a straightforward check with the p-adic valuations. For (b.) here we note that if E has good reduction at 7, the result is obvious. See [46, p.10] for the full details. □

4.2 Classification of admissible $E[7]$

Remark 4.10. Lemma 4.7 say that we need only to list the possibilities of $E[7]$, up to quadratic twist, such that $E[7]$ is unramified outside $2,3,7$. We will do that in the two distinct cases of $E[7]$ reducible and irreducible.

4.2.1 Reducible $E[7]$

Here the proof involves different combined technics on modular curves and cohomolgy, with the addition of the Kronecker-Weber theorem (a nice proof of this theorem can be find in [60]) and the use of lemma 4.9. We end up with a finite list of parametrized twists.

4.2.2 Irreducible $E[7]$

Let $\mathcal{H}$ be the specific set of 13 elliptic curves over $\mathbb{Q}$ given in Appendix A, that follows the notation of [19].

Lemma 4.11. *Suppose that E is an elliptic curve as in Lemma 4.9, and that $E[7]$ is an irreducible $\mathcal{G}$-module. Then there exists a quadratic twists E' of some $E'' \in \mathcal{H}$ such that $E[7] \simeq E'[7]$ as $\mathcal{G}$-modules.*

The proof works by level-lowering (theorem 1.84) a particular weight-2 newform associated to E, then one proceed by a case-by-case analysis to show the result (cf. [46, p.15] for details).

Corollary 4.12. *Suppose $(a,b,c) \in S(\mathbb{Z})$ and $a,b,c \neq 0$. If $E_{(a,b,c,)}[7]$ is irreducible, then $j = 1728b^3/c^7 \in X(1)(\mathbb{Q})$ is the image of a rational point on one of the 26 curves $X_E(7)$ or $X_E^-(7)$ with $E \in \mathcal{H}$.*

Here $X_E(7)$ and $X_E^-(7)$ are twists of $X(7)$ coming from the relevant twists of the $\mathcal{G}$-module $E[7]$. (cf. Definition 4.5)

4.3 Explicit equations

$X = X(7)$ is a non-hyperelliptic curve of genus 3 and so are its twists. The aim of this part is to find explicit equations for the relevant twists, exploiting their symmetries and using the local test (definition 3.7).

The left action of $\mathrm{GL}_n(\mathbb{C})$ on $V = \mathbb{C}^n$ induces a right action of the same group on the $\mathbb{C}$-algebra $\mathbb{C}[x_1, \ldots, x_n] = \mathrm{Sym}\, V^*$: if $g \in \mathrm{GL}_n(\mathbb{C})$ and $F \in \mathbb{C}[x_1, \ldots, x_n]$, we have that $F^g(v) = F({}^g v)$ for all $v \in V$. Let $\mathbb{C}[x_1, \ldots, x_n]_d = \mathrm{Sym}^d V^*$ be the subspace of $\mathrm{Sym}\, V^*$ consisting of homogeneous polynomials of degree d.

Definition 4.13. Fix n and d. A *covariant* of *order* j and *degree* δ is a function $\Psi : \mathbb{C}[x_1, \ldots, x_n] \longrightarrow \mathbb{C}[x_1, \ldots, x_n]_j$ such that:

a. The coefficients of a fixed monomial $x_1^{i_1} \ldots x_n^{i_n}$ in $\Psi(F)$ depends polynomially on the coefficients of F, as F varies in $\mathbb{C}[x_1, \ldots, x_n]$.

b. For each $g \in \mathrm{SL}_n(\mathbb{C})$, we have $\Psi(F^g) = \Psi(F)^g$.

c. For each $t \in \mathbb{C}^\times$, we have $\Psi(tF) = t^\delta \Psi(F)$.

Similarly a *contravariant* of *order* j and *degree* δ is a polynomial map $\Psi : \mathrm{Sym}^d V^* \longrightarrow \mathrm{Sym}^j V$ that is homogeneous of degree δ in the coefficients and equivariant with respect of the right action of $\mathrm{SL}_n(\mathbb{C})$ on the two spaces, that is, $\Psi(F^g) = \Psi(F)^{g^{-t}}$ for all $F \in \mathrm{Sym}^d V^*$ and $g \in \mathrm{SL}_n(\mathbb{C})$. Choosing a base for V, we induce an isomorphism $V \simeq V^*$, so that each contravariant may be expressed as a polynomial in the same variables $x_1, \ldots, x_n$.

Later on, we will consider only covariants and contravariants of ternary quartic forms that is, with the above notation, $n = 3$ and $d = 4$, with variables x, y, z.

In the following, 5 specific covariants and one contravariant (Ψ_{-4}) will be used:

name	order	degree
Ψ_0	0	3
Ψ_4	4	1
Ψ_6	6	3
Ψ_{14}	14	8
Ψ_{21}	21	12
Ψ_{-4}	4	2

See [48] for an (old-fashioned) complete list of the definitions.

In the paper [32] is explicitly find the equation of $X_E(7)$ in terms of the coefficients of E. If E is given in Weierstrass form $Y^2 = X^3 + aX + b$, then the equation is:

$$ax^4 + 7bx^3z + 3x^2y^2 - 3a^2x^2z^2 - 6bxyz^2 - 5abxz^3 + 2y^3z^2 + 2a^2yz^3 - 4b^2z^4 = 0. \quad (4.1)$$

What we miss at this point is an explicit equation for $X_E^-(7)$ given the equation of E. We will fix this small gap with the following result:

Lemma 4.14. *Let M be a $\mathcal{G}$-module. If F is a ternary quadratic form describing $X_M(7)$, then $\Psi_{-4}(F)$ is a ternary quartic form describing $X_M^-(7)$.*

Proof. See [46, Proposition 7.5]. □

Then $X_E^-(7)$ is defined by the following equation:

$$\begin{aligned}-a^2x^4 + a(3a^3 + 19b^2)y^4 + 3z^4 + 6a^2y^2z^2 + 6az^2x^2 - 6(a^3 + 6b^2)x^2y^2 - 12aby^2zx)\\ +18bz^2xy + 2abx^3y - 12bx^3z - 2(4a^3 + 21b^2)y^3z + 2a^2by^3x - 8az^3y = 0.\end{aligned} \tag{4.2}$$

As we saw in the section 3.2, for each twist of X' of X, we need to find explicitly the associated morphism $X' \longrightarrow \mathbb{P}^1$, to be able to recover the "true" solutions over $\mathbb{Z}$.

Lemma 4.15. *Let X' be a twist of X defined by a ternary quartic form F. Then the canonical morphisms is:*

$$\begin{aligned}\pi' : X' &\longrightarrow \mathbb{P}^1\\ (x : y : z) &\longmapsto \frac{\Psi_{14}(F)^3}{\Psi_0(F)\Psi_6(F)^7}\end{aligned}$$

where we take $\mathbb{P}^1$ parametrized by the $j-$invariant.

Proof. It suffices to chek this for the Klein quartic X, and this is done in [27, 2.13]. □

Proposition 4.16. *It is possible to write explicitly an algorithm for the local test (cf. section 3.3) that terminates.*

Proof. See [46, 7.4]. □

4.3.1 Equations

Since we are not interested in all the solutions $S(R)$, we have to run the local test algorithm on the (finite) list of twists of X coming from both reducibles and irreducibles $E[7]$. We end up with exactly 10 twists that passes the test: 3 of them coming from reducibles $E[7]$, the other 7 from the irreducible ones. At this point we are able to compute explicitly the 10 equations that define the same number of quartic plane curves of genus 3 denoted by $C_1, \ldots, C_{10}$, where C_1, C_2 and C_3 are the

one coming from the reducible case.

$$
\begin{aligned}
C_1 &: 6x^3y + y^3z + z^3x = 0\\
C_2 &: 3x^3y + y^3z + 2z^3x = 0\\
C_3 &: 3x^3y + 2y^3z + z^3x = 0\\
C_4 &: 7x^3z + 3x^2y^2 - 3xyz^2 + y^3z - z^4 = 0\\
C_5 &: -2x^3y - 2x^3z + 6x^2yz + 3xy^3 - 9xy^2z + 3xyz^2 - xz^3 + 3y^3z - yz^3 = 0\\
C_6 &: x^4 + 2x^3y + 3x^2y^2 + 2xy^3 + 18xyz^2 + 9y^2z^2 - 9z^4 = 0\\
C_7 &: -3x^4 - 6x^3z + 6x^2y^2 - 6x^2yz + 15x^2z^2 - 4xy^3 - 6xyz^2 - 4xz^3 + 6y^2z^2\\
&\quad - 6yz^3 = 0\\
C_8 &: 2x^4 - x^3y - 12x^2y^2 + 3x^2z^2 - 5xy^3 - 6xy^2z + 2xz^3 - 2y^4 + 6y^3z\\
&\quad + 3y^2z^2 + 2yz^3 = 0\\
C_9 &: 2x^4 + 4x^3y - 4x^3z - 3x^2y^2 - 6x^2yz + 6x^2z^2 - xy^3 - 6xyz^2 - 2y^4 + 2y^3z\\
&\quad - 3y^2z^2 + 6yz^3 = 0\\
C_{10} &: x^3y - x^3z + 3x^2z^2 + 3xy^2z + 3xyz^2 + 3xz^3 - y^4 + y^3z + 3y^2z^2 - 12yz^3\\
&\quad + 3z^4 = 0
\end{aligned}
$$

See Appendix B for the known rational points of each C_i found with a naive search.

Remark 4.17. What we have to do at this point is the following:

a. For each curve $C_1, \ldots, C_{10}$ we find all its $\mathbb{Q}$-rational points;

b. For each such rational point, we compute the corresponding value $j \in \mathbb{P}^1$ using Lemma 4.15;

c. For each such j, we list all the primitive integer solutions (a, b, c) to $a^2+b^3 = c^7$ with $1728b^3/c^7 = j$, if such solutions exist.

See appendix B for the list of the rational points on $C_1, \ldots, C_{10}$.

Example 4.18. $P_{28} = (0 : 0 : 1)$ is a rational point of C_8. The corresponding $j-$invariant, computed with the formula of Lemma 4.15, is $j = -2^9 3^3$. Hence we have (recall that $(a, b, c) \in S(\mathbb{Z})$):

$$
\begin{aligned}
j = -2^9 3^3 = \frac{1728b^3}{c^7}&\\
-2^3 c^7 = b^3&\\
-8(a^2 + b^3) = b^3&\\
8a^2 = -9b^3.&
\end{aligned}
$$

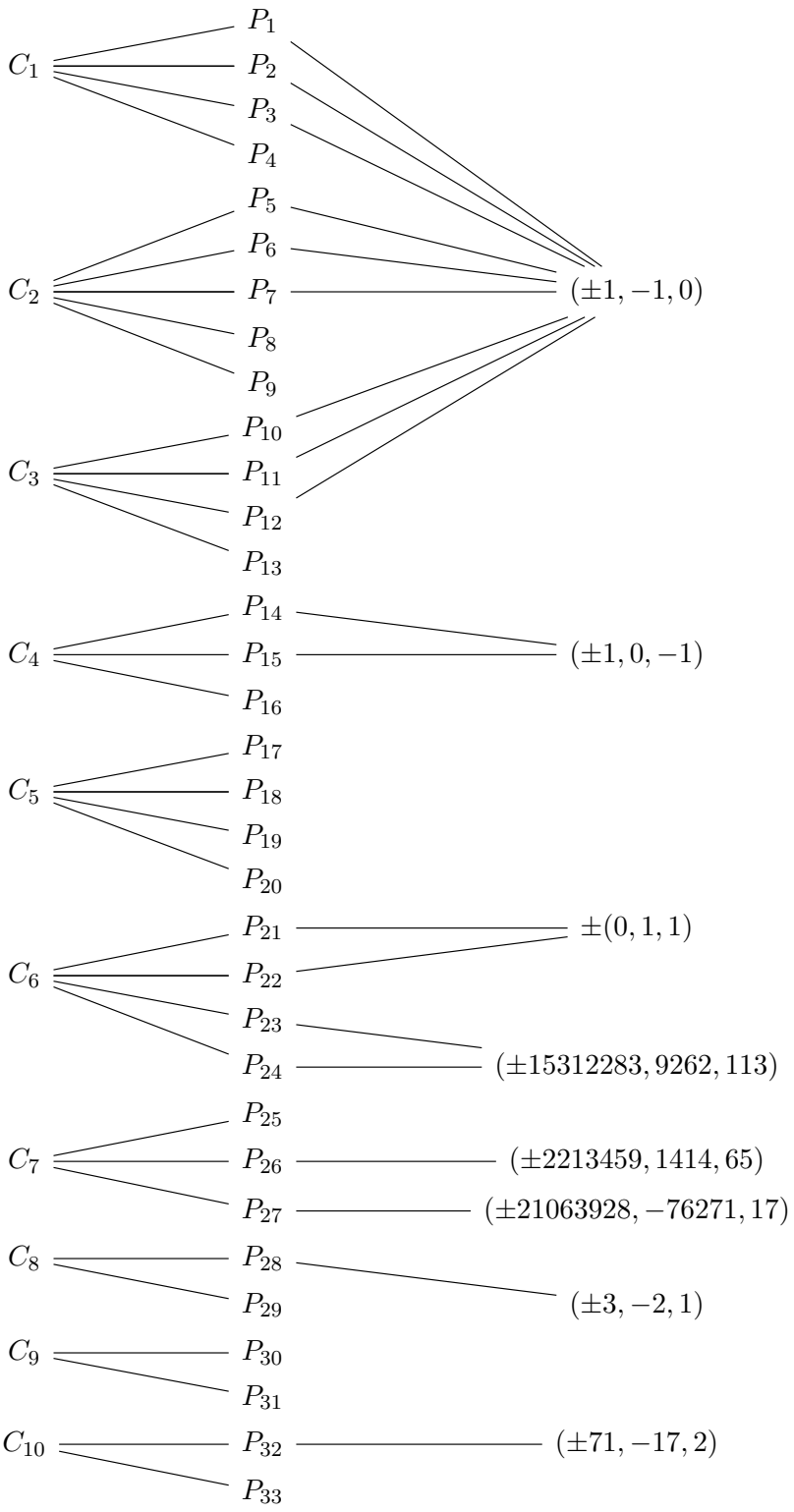
Now, since $\gcd(a, b, c) = 1$, we have also $\gcd(a, b) = 1$. It follows that $v_2(b^3) = 3$ and $v_2(a^2) = 0$, hence $v_2(b) = 1$ and $v_2(a^2) = 0$. Similarly we have that $v_3(a) = 1$ and $v_3(b) = 0$. Finally, if $p \geq 5$, $v_p(a) = v_p(b) = 0$. In this way we get that $(\pm 3, -2, 1)$ are two solutions to our original equation that comes from P_{28}.

Example 4.19. $P_{25} = (0 : 1 : 0)$ is a rational point of C_7. The corresponding $j-$invariant is $j = -2^3 3^3$. So we have:

$$\begin{aligned} j = -2^3 3^3 &= \frac{1728 b^3}{c^7} \\ -3c^7 &= 2^3 b^3 \\ -3(a^2 + b^3) &= 8b^3 \\ 3a^2 &= -11b^3. \end{aligned}$$

The assumption $\gcd(a, b) = 1$ implies that there are no primitive solutions to $x^2 + y^3 = z^7$ coming from this specific rational point.

In the following page there is a picture that explains the situation: for each relevant twist C_j of $X(7)$ are listed all its known $\mathbb{Q}$-rational points, following the notation of the appendix B. Then for each such P_i we list, if any, the elements of $S(\mathbb{Z})$ (that are primitive integer solutions to $x^2 + y^3 = z^7$) coming from P_i. It is important to note that, since we worked with the quasi-affine punctured scheme $S_{\mathbb{Z}}$, we cannot obtain the trivial solution $(0, 0, 0)$ from this contruction.


$C_j \simeq X(7)$
$P_i \in C_j$
$S(\mathbb{Z})$
C_1
C_2
C_3
C_4
C_5
C_6
C_7
C_8
C_9
C_{10}
P_1
P_2
P_3
P_4
P_5
P_6
P_7
P_8
P_9
P_{10}
P_{11}
P_{12}
P_{13}
P_{14}
P_{15}
P_{16}
P_{17}
P_{18}
P_{19}
P_{20}
P_{21}
P_{22}
P_{23}
P_{24}
P_{25}
P_{26}
P_{27}
P_{28}
P_{29}
P_{30}
P_{31}
P_{32}
P_{33}
$(\pm 1, -1, 0)$
$(\pm 1, 0, -1)$
$\pm(0, 1, 1)$
$(\pm 15312283, 9262, 113)$
$(\pm 2213459, 1414, 65)$
$(\pm 21063928, -76271, 17)$
$(\pm 3, -2, 1)$
$(\pm 71, -17, 2)$

Chapter 5

Computing the ranks of the ten Jacobians

In order to determine the sets of rational points of $C_1, \ldots, C_{10}$ first we need to determine the Mordell-Weil ranks of their corresponding Jacobians $J_1, \ldots, J_{10}$. (cf. Theorem 1.44 for the construction of the Jacobian of a curve).

5.1 Ranks of J_1, J_2, J_3

The curves C_1, C_2, C_3 are $\boldsymbol{\mu}_7$ -twists of X, that is $C_i \simeq X$ over $L = \mathbb{Q}[\zeta_7]$ for $i = 1, 2, 3$; rather than more general twist; so that we can apply more methods to compute the ranks of J_1, J_2 and J_3.

First we note that C_1, C_2 and C_3 are birational to the (singular) plane curves of equations:

$$C_1' : u^7 = (6v - w)w^4$$
$$C_2' : u^7 = (18v - w)w^4$$
$$C_3' : u^7 = (12v - w)w^4.$$

By [45] this three curves are Galois cover of $\mathbb{P}^1$ with Galois group $\boldsymbol{\mu}_7$; hence their Jacobians have complex multiplication by $\mathbb{Z}[\zeta_7]$ and we can perform a $(1 - \zeta_7)$ descent on these Jacobians, following [45] and [49].

Let $L = \mathbb{Q}[\zeta_7]$. The descent map is given by the function $f = v/w$ that takes values in

$$H = L(\{2, 3, 7\}, 7) = \{\theta \in L^\times / L^{\times 7} : L(\theta^{\frac{1}{7}}/L) \text{ is unramified outside } \{2, 3, 7\}\}.$$

If $\theta \in H$, $\theta^7 = 1$, so that H is a $\mathbb{F}_7-$vector space. Moreover we have that $\dim H = 7$ (cf. [60, Theorem I.2.13]). Performing a $1-\zeta_7$ descent, we find that the Mordell-Weil rank of $J_i(L)$ is 6, for $i = 1, 2, 3$.
To conclude we apply the following lemma (cf. [45, p. 31]):

Lemma 5.1. *Let k be a number field not necessarily containing a primitive $p-$th root of unity $\zeta_p \in \bar{\mathbb{Q}}$. Let $f(x)$ be a $p-$th power free polynomial with zeros in $\bar{\mathbb{Q}}$, and let J be the Jacobian of $y^p = f(x)$. Then*

$$\operatorname{rank} J(k) = \frac{\operatorname{rank} J(k(\zeta_p))}{[k(\zeta_p) : k]}$$

Hence, we get that $\operatorname{rank} J_i = 1$ for $i = 1, 2, 3$.

5.2 Ranks of $J_4, \ldots, J_{10}$

The Klein quartic (hence its twists) has 24 flexes. These points can be partitioned into eight sets with the following property. Choose one set of three and denote the points by W_1, W_2, W_3. The tangent line at W_j intersects X with multiplicity 3 at W_j and multiplicity 1 at W_{j+1} (The subscripts are considered modulo 3). We will call such a set of three flexes a *triangle*. By abuse of notation, let T_i denote both a triangle and the effective divisor of degree 3 given by the sum of the points. Let us denote by $T = \{T_i | i = 1, \leq i \leq 8\}$ the set of the eight triangles.

Lemma 5.2. *Let X' be a twist of X, then the set T is a Galois-stable set. In other words, if $\sigma \in \operatorname{Gal}(\bar{K}/K)$, then ${}^{\sigma}T_i = T_j$ where $T_j \in T$.*

Proof. The tangent-intersection procedure involves only algebraic operations. □

Remark 5.3. For $i \leq i \leq j \leq 8$, we can find a function with divisor $2T_i - 2T_j$ whose numerator and denominator are cubics. Therefore the divisor class $[T_i - T_j]$ is killed by 2, moreover since the points in each T_i are not collinear, we have that the order of $[T_i - T_j]$ is exactly 2 (cf. Remark 5.16).

Proposition 5.4. *The $[T_i - T_1]$ for $i = 1, \ldots, 8$ sum to 0, and any six of them with $i \neq 1$ form a basis for $\operatorname{Jac}(X)[2]$. Let $Q_1 = [\sum_{i=1}^{8} a_i T_i]$ and $Q_2 = [\sum_{i=1}^{8} b_i T_i]$ with $\sum a_i = \sum b_i = 0$. Let e_2 be the $2-$Weil pairing. Then*

$$e_2(Q_1, Q_2) = (-1)^{\sum_{i=1}^{8} a_i b_i}.$$

Remark 5.5. There is an analogy (cf. [46, p. 26] for details) between X with its T_i and a genus-3 hyperelliptic curve with its Weierstrass points. This will allow us to reformulate many of the results in [45] in our situation.

Lemma 5.6. *For each curve $C_4, ..., C_{10}$ the following holds: for each T_i there is a cubic whose intersection divisor with C is $2T_i + 3P + R_i$, where R_i is an effective divosr of degree 3 defined over $\mathbb{Q}$ and supported on three non-collinear $\bar{\mathbb{Q}}$.*

Proof. This is a straightforward computation. See [46, p. 27]. □

In the following we develop the theory for a generic twist C of X. (C=C_i for some $i = 4, \ldots, 10$). Let us denote by J the Jacobian of C and let $P \in C(\mathbb{Q})$ be a $\mathbb{Q}-$rational poins of C.
Choose functions $f_1, \ldots, f_8$ with $\operatorname{div}(f_i) = 2T_i + 3P + R_i - 3\Omega$, where Ω is a canonical divisor over $\mathbb{Q}$; and such that if $\sigma \in \mathcal{G}$, then ${}^{\sigma}T_i = T_j$. Then $\operatorname{div}(f_i/f_j) = 2T_i - 2T_j + R_i - R_j$. Since $sT_i - 2T_j$ is principal, so is $R_i - R_j$.

Lemma 5.7. *We have that $R_i = R_j$ for each $i, j \in \{1, \ldots, 8\}$. Denote by R this common value.*

Proof. The R_i are effective, of degree 3, and are supported on three non-collinear points by our construction. The Riemann-Roch theorem (cf. 1.21) then implies that $R_i = R_j$. □

In the following let K be one of the following fields: $\mathbb{Q}, \mathbb{Q}_p$ or $\mathbb{Q}_\infty = \mathbb{R}$.
Let us denote by $\bar{A}_K$ the $\bar{K}$-algebra of maps $\{\alpha : T \to \bar{K}\}$. Since $\mathcal{G}_K = \mathrm{Gal}(\bar{K}/K)$ acts on T and on $\bar{K}$, it acts also on $\bar{A}_K$. Denote by A_K the algebra of $\mathcal{G}_K$-invariant elements of $\bar{A}_K$.

Definition 5.8. We say that D is a *good* divisor if it is of degree 0, defined over K and if its support is disjoint from the support of $\mathrm{div}(f_i)$ for every $i \in \{1, \ldots, 8\}$.

Define now the following homomorphism of groups:

$$\{\text{good divisors}\} \longrightarrow A_K^\times$$

$$D \longmapsto (T_i \mapsto f_i(D)).$$

Lemma 5.9. *If D is a good principal divisor, then $f(D) \in A_K^{\times 2} K^\times$.*

Now, since C has at least one rational point, every element of $J(K)$ can be represented by a good divisor. Therefore, f induces a well-defined homomorphism

$$f : \frac{J(K)}{2J(K)} \longrightarrow \frac{A_K^\times}{A_K^{\times 2} K^\times}.$$

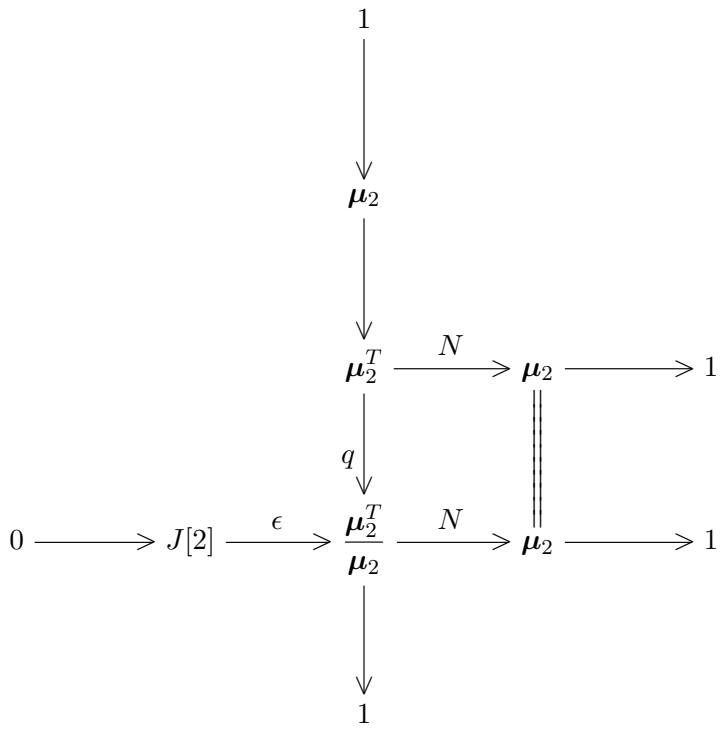
Let $\boldsymbol{\mu}_2^T = \{\beta : T \to \boldsymbol{\mu}_2 \subset \bar{K}\}$ be the 2−torsion in A_K; let $\boldsymbol{\mu}_2^T/\boldsymbol{\mu}_2$ be its quotient by the set of constant maps. Let q be the projection $\boldsymbol{\mu}_2^T \to \boldsymbol{\mu}_2^T/\boldsymbol{\mu}_2$. Let $N : \boldsymbol{\mu}_2^T \to \boldsymbol{\mu}_2$ be the restriction of the norm map $\bar{A}_K \to \bar{K}$.
Define the map

$$\epsilon : \quad J[2] \longrightarrow \frac{\boldsymbol{\mu}_2^T}{\boldsymbol{\mu}_2}$$

$$Q \longmapsto (T_i \mapsto e_2(Q, [T_i - T_1])).$$

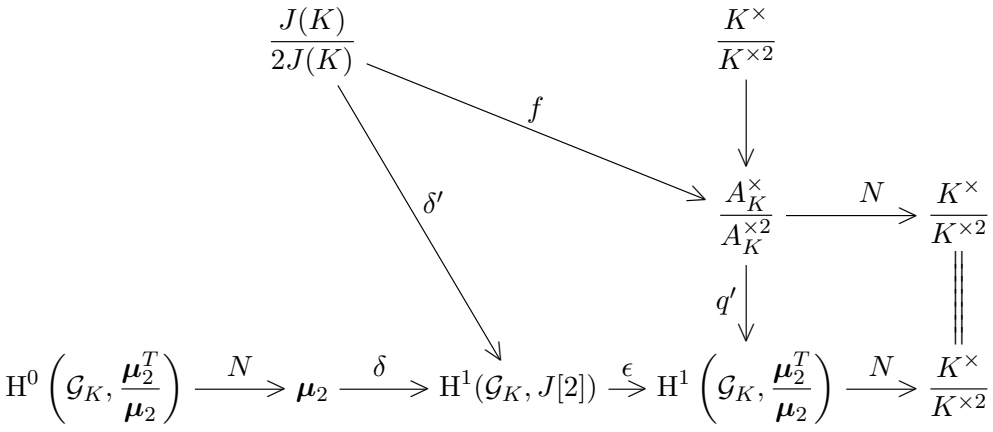
Note that ϵ is well-defined by Proposition 5.4.

We obtain the following commutative diagram of $\mathcal{G}_k-$modules:



Using proposition 5.4 one can check that the vertical and horizontal lines are exact.

Now we compute the long exact exact cohomology sequences for the rows and the columns. Since $\mathrm{H}^1(\mathcal{G}_K, \bar{K}^\times)$ and $\mathrm{H}^1(\mathcal{G}_K, \bar{A}_K^\times)$ are trivial by Hilbert's 90 (theorem 1.62), we have that $\mathrm{H}^1(\mathcal{G}_K, \boldsymbol{\mu}_2) \simeq K^\times/K^{\times 2}$ and that $\mathrm{H}^1(\mathcal{G}_K, \boldsymbol{\mu}_2^T) \simeq A_K^\times/A_K^{\times 2}$ by Kummer isomorphisms (example 1.63).
We get the following diagram with exact rows and columns:



The map $f : J(K)/2J(K) \longrightarrow A^\times/A^{\times 2}$ is the map induced from $f : J(K) \to A^\times$, modulo 2.
The map q' is the composition of the Kummer isomorphism $A^\times/A^{\times 2} \simeq \mathrm{H}^1(\mathcal{G}_K, \boldsymbol{\mu}_2^T)$

with the map induced by q in the cohomology. The map δ' is the connecting homomorphis obtained taking the cohomology of the following sequence:

$$0 \longrightarrow J(K)[2] \longrightarrow J(K) \xrightarrow{\cdot 2} J(K) \longrightarrow 0.$$

Proposition 5.10. *The above diagram commutes, that is, $f \circ q' = \delta' \circ \epsilon$ (cf. [46, Proposition 11.2]).*

Lemma 5.11. *We have that $\delta'[R - 3P] = \delta(-1)$.*

Proof. Let C^1 be the cubic curve defined by the union of the three lines tangent at the points of T_1. By definition we have $R = R_1$, so that $2T_1 + 3P + R$ is the intersection of C with a cubic. So it is linearly equivalent to the intersection of C with any other cubic; thus we can take the intersection between C and C^1. So $[2T_1 + 3P + R] = [4T_1]$ by definition of T_1, hence $[R - 3P] = [4T_1 - 6P] = 2[T_1 - 3P]$, therefore $\delta'([R - 3P])$ is in the class of the 1-cocycle $(\sigma \mapsto [{}^\sigma T_1 - T_1])$. By Proposition 5.4, we have that $\epsilon([{}^\sigma T_1 - T_1]) = [{}^\sigma M - M]$, where M is the following map:

$$M(T_i) = \begin{cases} 1, & \text{if } i = 1 \\ -1 & \text{if } i = 2, \dots, 8. \end{cases}$$

Moreover we have that $N(M) = (-1)^7 = -1$, so that, by definition, $\delta(-1)$ is in the class of the 1-cocycle $(\sigma \mapsto [{}^\sigma T_1 - T_1])$ in $\mathrm{H}^1(\mathcal{G}_K, J[2])$. □

Proposition 5.12. *The kernel of $f : J(K)/2J(K) \longrightarrow A_K^\times / A_K^{\times 2}$ is generated by $[R - 3P]$. This element is trivial in $J(K)/2J(K)$ if and only if the $\mathcal{G}_K$-set T has an orbit of odd size.*

Proof. The maps $\delta' : J(K)/2J(K) \to \mathrm{H}^1(\mathcal{G}_K, J[2])$ and $q' : A_K^\times / A_K^{\times 2} \longrightarrow \mathrm{H}^1(\mathcal{G}_K, \boldsymbol{\mu}_2^T / \boldsymbol{\mu})$ are injective by construction. Hence we have that

$$\ker f = (\delta')^{-1}(\ker \epsilon) = (\delta')^{-1}(\delta(\boldsymbol{\mu}_2)).$$

Now, since $\boldsymbol{\mu}_2$ is generated by -1, by Lemma 5.11 we have that $\delta(\boldsymbol{\mu}_2) = \delta'(< [R - 3P] >)$. It follows that

$$\ker f = (\delta')^{-1}(\delta(\boldsymbol{\mu}_2)) = (\delta')^{-1}\delta'(< [R - 3P] >) =< [R - 3P] > .$$

For the second part of the proof, see [45, Lemma 11.2 case b]. □

Now set $A = A_{\mathbb{Q}}$ and $A_p = A_{\mathbb{Q}_p}$. In section 5.2.1 we will compute the $\mathcal{G}_{\mathbb{Q}}$ orbits of T and we will see that for each of $C_4, \dots, C_{10}$ there are no orbits of odd size (cf. Remark 5.20). Hence the kernel of the map f has size 2 and is generated by $[R - 3P] \in J(\mathbb{Q})/2J(\mathbb{Q})$.
Let $A \simeq \prod A_i$, where the A_i are number fields. Let p ve a prime number; let a be an element of $A^\times$ and a_i its image in A_i. We say that $a \in A^\times / A^{\times 2}$ is *unramified at p* if for each i, the field extension $A_i(\sqrt{a_i}/A_i)$ is unramified at all primes over p. Let S be a set of places of $\mathbb{Q}$ including 2, ∞ and all primes at which J has bad reduction, excluding the odd primes at which the Tamagawa (definition 1.55) number is odd. Let $(A^\times / A^{\times 2}\mathbb{Q}^\times)_S$ be the image in $A^\times / A^{\times 2}\mathbb{Q}^\times$ of the elements of $A^\times / A^{\times 2}$ that are unramified outside the primes of S. Finally, let H be the kernel of the norm map from $(A^\times / A^{\times 2}\mathbb{Q}^\times)_s$ to $\mathbb{Q}^\times / \mathbb{Q}^{\times 2}$.

Proposition 5.13. *The image of $f : J(\mathbb{Q}) \longrightarrow A^\times/A^{\times 2}\mathbb{Q}^\times$ is contained in H.*

Proof. See [46, Proposition 11.5]. □

Let p be a prime of $\mathbb{Q}$ (it could be ∞). We have the following commutative diagram:

$$\begin{array}{ccc} \dfrac{J(\mathbb{Q})}{\ker(f)} & \xrightarrow{\ f\ } & H \\ \downarrow & & \downarrow{\scriptstyle \rho_p} \\ \dfrac{J(\mathbb{Q}_p)}{\ker(f_p)} & \xrightarrow{\ f_p\ } & \dfrac{A_p^\times}{A_p^{\times 2}\mathbb{Q}_p^\times} \end{array}$$

where f denotes the map f in the case $K = \mathbb{Q}_p$; and ρ_p is the composition $H \hookrightarrow A^\times/A^{\times 2}\mathbb{Q}^\times \to A_p^\times/A_p^{\times 2}\mathbb{Q}_p^\times$.
Recall that (definition 1.65), in our setting, the 2-*Selmer group* $\mathrm{Sel}^2(J,\mathbb{Q})$ is the set of elements in $\mathrm{H}^1(\mathcal{G}_\mathbb{Q}, J[2])$, unramified outside S, which map to the image of $J(\mathbb{Q}_p) \longrightarrow \mathrm{H}^1(\mathcal{G}_{\mathbb{Q}_p}, J[2])$ for all $p \in S$.

Definition 5.14. Define the *fake* 2-*Selmer group* to be

$$\mathrm{Sel}^2_{\mathrm{fake}}(J,\mathbb{Q}) = \{\theta \in H | \rho_p(\theta) \in f(J(\mathbb{Q}_p)) \text{for all } p \in S\}.$$

Lemma 5.15. *The sequence*

$$\boldsymbol{\mu}_2 \xrightarrow{\ \delta\ } \mathrm{Sel}^2(J\mathbb{Q}) \xrightarrow{\ \epsilon\ } \mathrm{Sel}^2_{fake}(J,\mathbb{Q}) \longrightarrow 0$$

is exact.

Proof. See [45, Theorem 13.2]: in our case we have $p = 2$. □

We will see that $\delta'(R - [R - 3P])$ is not zero (cf. 5.18). By Lemmas 5.11 and 5.15 we find that $\dim_{\mathbb{F}_2} \mathrm{Sel}^2(J,\mathbb{Q}) = 1 + \dim_{\mathbb{F}_2} \mathrm{Sel}^2_{\mathrm{fake}}(J,\mathbb{Q})$.
To compute $\mathrm{Sel}^2_{\mathrm{fake}}(J,\mathbb{Q})$ first we need to explicitly find A. Let Λ be a subset of $\{1,\ldots,8\}$ such that the set $4\{T_j\}_{j\in\Gamma}$ contains one representative of each $\mathcal{G}_\mathbb{Q}$-orbit of T. Let $A_j = \mathbb{Q}(T_j)$. Then we can find an isomorphism

$$A \simeq \prod_{j\in\Lambda} A_j \tag{5.1}$$

The composition of f and this isomorphim is $\prod_{f\in\Lambda} f_j$.
Then, to find a basis of $(A^\times/A^{\times 2}\mathbb{Q}^\times)_S$ we can use the algorithm described in [45, §12].

Remark 5.16. Now, to find the function f_j we first find a cubic form defined over A_j, with the property that the curve defined by this cubic meets C at P with multiplicity at least 3 and at each of the three points of T_j with multiplicity at least 2. The jth component of f then can be find by taking this cubic divided by any cubic defined over $\mathbb{Q}$, like z^3.

At this point we need a "local" basis for each $J(\mathbb{Q}_p)/\ker(f)$. First we gather some informations about the dimension:

Lemma 5.17. *a. If p is odd, then $\#J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) = \#J(\mathbb{Q}_p)[2]$;*

b. If $p = 2$, then $\#J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = 2^3\#J(\mathbb{Q}_2)[2]$;

c. If $p = \infty$, then $\#J(\mathbb{R})/2J(\mathbb{R}) = \#J(\mathbb{R})[2]/2^3$.

Proof. It is [45, Lemma 12.10], in the special case where the isogeny ϕ is the multiplication by 2, the field k_v is simply $\mathbb{Q}_p$ and the dimension g of the Jacobian is 3. □

Then, by Lemma 5.11 we have that in our cases $J(\mathbb{Q}_p)/\ker(f)$ has half of the size of $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$. Then we determine the intersection of all $\rho_p^{-1}(f(J(\mathbb{Q}_p)))$ for all $p \in S$. That intersection is equal to $\mathrm{Sel}^2_{\mathrm{fake}}(J,\mathbb{Q})$ which is half the size of $\mathrm{Sel}^2(J,\mathbb{Q})$. Then we have:

$$\dim \mathrm{Sel}^2(J,\mathbb{Q}) = \mathrm{rank}\, J(\mathbb{Q}) + \dim J(\mathbb{Q})[2] + \dim Ш(J,\mathbb{Q})[2]. \tag{5.2}$$

In each of our cases we have that the number of independent elements we found so far in $J(\mathbb{Q})/2J(\mathbb{Q})$ equals $\dim \mathrm{Sel}^2(J,\mathbb{Q})$, so $Ш(J,\mathbb{Q})[2] = 0$, so subtracting $\dim J(\mathbb{Q})[2]$ from $\dim \mathrm{Sel}^2(J,\mathbb{Q})$ gives us the rank of $J(\mathbb{Q})$.

5.2.1 Results for $J_4, \ldots, J_{10}$

Here we apply the technics developed in 5.1 to explicitly compute the ranks of $J_4, \ldots, J_{10}$. First of all, for each of the C_i we list all the known rational points that we are able to find with a naive search. (See Appendix B).
Then we will discover the following:

Remark 5.18. For the curves $C_4, \ldots, C_{10}$ we have that $\delta'([R - 3P])$ is nonzero.

Remark 5.19. In each J_i, for $i = 4, \ldots, 10$, we have that $\rho_2^{-1}(f(J_i(\mathbb{Q}_2)/\ker f))$ is the same as the image of the subgroup of $J_i(\mathbb{Q})$ generated by the known rational points. This means that, in each case, $\mathrm{Sel}^2_{\mathrm{fake}}(J_i,\mathbb{Q}) = \rho_2^{-1}(f(J_i(\mathbb{Q}_2)/\ker f))$.

Remark 5.20. In each case, the $\mathcal{G}_\mathbb{Q}$-set T has no orbit of odd size, therefore the dimension of $\mathrm{Sel}^2(J_i,\mathbb{Q}) \simeq J_i(\mathbb{Q})/2J_i(\mathbb{Q})$ equals $1 + \dim \mathrm{Sel}^2_{\mathrm{fake}}(J_i,\mathbb{Q})$.

Now we summarize the steps needed in such computations. See [46, §11.2] for the full details concerning the computation of $\mathrm{rank}\, J_4$ and a sketch of the computation of the ranks of $J_5, \ldots, J_{10}$.

- For any smooth plane curve, the flex points are the points on the curve where the Hessian vanishes. We dehomogenize each model of C_i $(4 \le i \le 10)$ and their Hessians with respect to z, getting two polynomials in $u = x/z$ and $v = y/z$.
- We compute the resultant of such two polynomials to eliminate v and we get a product of polynomials $h_{\alpha_1}(u) \cdots h_{\alpha_k}(u)$, each of them irreducible over $\mathbb{Q}$. From this decomposition we are able to compute the sizes of the $\mathcal{G}_k$-orbits of the triangles.

- We explicitly compute, for each orbit T_{α_j}, the number field $\mathbb{Q}(\alpha_j)$ containing all the triangles $T_k \in T_{\alpha_j}$, so that we get $A \simeq \mathbb{Q}(\alpha_1) \times \cdots \times \mathbb{Q}(\alpha_n)$.
- Let $S = \{\infty, 2, 3, 7\}$. For each $\mathbb{Q}_{\alpha_j}$, we find a basis for the subgroup of $\mathbb{Q}(\alpha_j)/\mathbb{Q}(\alpha)^{\times 2}$ that is unramified outside S.
- Using this result and the norm map, we find a basis for $(A^\times/A^{\times 2}\mathbb{Q}^\times)_S$; then we compute the kernel H of the norm map $(A^\times/A^{\times 2}\mathbb{Q}^\times)_S \to \mathbb{Q}/\mathbb{Q}^{\times 2}$. We have that this group H contains the fake 2-Selmer group (cf. Definition 5.14).
- Now we find the function f, in order to do that we express f as an n-tuple $(f_1, \ldots, f_n)$ where each f_j is defined over the component $\mathbb{Q}(\alpha_j)$.
- We compute explicitly $\mathrm{Sel}^2_{\mathrm{fake}}(J_i, \mathbb{Q})$: first we perform global computations to obtain relations between $\dim J_i(\mathbb{Q})/\ker(f)$ and $\operatorname{rank} J_i(\mathbb{Q})$. Then we give a lower bound on $\operatorname{rank} J_i(\mathbb{Q})$ looking at the image in H under the map f of the subgroup of $J_i(\mathbb{Q})$ generated by the known rational points on C_i.
- Then we perform a local computation finding a basis for $J_i(\mathbb{Q}_2)/\ker f$; we conclude retrieveng the rank of the Jacobians using the Lemma 5.15.

The final results are summarized in the following table:

Curve	$\operatorname{rank} J_i(\mathbb{Q})$
C_4	2
C_5	3
C_6	2
C_7	2
C_8	2
C_9	2
C_{10}	2

Chapter 6

Rational points on the ten curves

The aim of this chapter is to prove that all the points that we found on $C_1, \dots, C_{10}$ with a naive search (see Appendix B) are actually all the rationals points on the curves $C_1, \dots, C_{10}$, except perharps for C_5. In order to do that, two classical diophantine geometry technics will be applied: the Mordell-Weil Sieve and the Chabauty-Coleman theory. See Remark 6.7 to understand why the latter cannot be applied to C_5: this curve need one ad-hoc argument that will be explained in section 6.4.

6.1 Mordell-Weil sieve

The main reference for this section is [50], where the method is explicitly introduced for the first time.
Let C be a curve over $\mathbb{Q}$ and J its Jacobian; suppose furthermore that we know explicitly an embedding $C \to J$. The *Mordell-Weil sieve* is a method that uses reduction modulo p, for several primes p, to show that certain points in $J(\mathbb{Q})$ cannot lie in the image of C. Suppose moreover that we explicitly know the generators for $J(\mathbb{Q})$: then the points of $C(\mathbb{Q})$ are simply the points of $J(\mathbb{Q})$ that lies on C. In general, it is not known wheter there exists an algorithm to solve this problem.
Therefore we take a prime p of good reduction for C (hence for J, cf. Proposition 1.56), and we ask that reduction modulo p of a point $P \in J(\mathbb{Q})$ lies in $C(\mathbb{F}_p)$. For each p this weaker condition allow us to "sieve out" certain cosets of a finite-index subgroup in $J(\mathbb{Q})$. After using these sieve conditions at few primes, maybe no point on $J(\mathbb{Q})$ remain, in this case we conclude that $C(\mathbb{Q})$ is empty.

Remark 6.1. If $C(\mathbb{Q})$, as in our cases, is known *a priori* to be nonempty, obviously no complete obstruction to rational points can be found. In this case, one can try to use the sieve information as input to a Chabauty-Coleman argument.

Remark 6.2. One can obtain sieve conditions also at primes p of bad reduction, using the Néron model of J over $\mathbb{Z}_p$. See [46, Remarks 12.1] for details.

Remark 6.3. We assumed that we know the generators of $J(\mathbb{Q})$, however it may be enough to know the generators for a subgroup $\mathcal{Q}$ of finite index in $J(\mathbb{Q})$. For instance, if one can prove that the index $(J(\mathbb{Q}) : \mathcal{Q})$ is relatively prime to the order of $J(\mathbb{F}_p)$, then $\mathcal{Q}$ and $J(\mathbb{Q})$ will have the same image in $J(\mathbb{F}_p)$.

6.2 Chabauty-Coleman theory

Here we explain a method that originates with Chabauty [13], while he was trying to prove the Mordell conjecture. Coleman [17] later realized that Chabauty's idea could be done explicitly. In this very introductory exposition, we follow mostly [40]. If J is the Jacobian of the curve C, defined over $\mathbb{Q}$, denote by $J_{\mathbb{Q}_p}$ the variety defined by the same equations as J, but defined over $\mathbb{Q}_p$ for some fixed prime p where C has good reduction. Finally denote by $\mathrm{H}^0(J_{\mathbb{Q}_p}, \Omega^1)$ the $\mathbb{Q}_p$-vector space of regular 1-form on $J_{\mathbb{Q}_p}$.

Proposition 6.4. *If $\omega \in \mathrm{H}^0(J_{\mathbb{Q}_p}, \Omega^1)$, then one can define an "antiderivate" λ_ω:*

$$\begin{aligned} \lambda_\omega : J(\mathbb{Q}_p) &\to \mathbb{Q}_p \\ Q &\mapsto \int_0^Q \omega. \end{aligned}$$

characterized uniquely by the following two properties:

a. *It is an homomorphism;*

b. *There is an open subgroup U of $J(\mathbb{Q}_p)$ such that if $Q \in U$, then $\int_0^Q \omega$ can be computed by expanding ω in power series in local coordinates, finding a formal antiderivative and evaluating the formal power series at the local coordinates of Q. For a sufficiently small U, the formal antiderivative converges.*

Proof. See [7, III.§7.6]. □

Now denote by $\overline{J(\mathbb{Q})}$ the closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$ with respect to the $p-$adic topology. Then we have the following result:

Lemma 6.5. *Let $r' = \dim \overline{J(\mathbb{Q})}$ and $r = \operatorname{rank} J(\mathbb{Q})$. Then $r' \leq r$.*

Chabauty theorem was an important results towards the Mordell's conjecture, before Faltings proved the conjecture in full:

Theorem 6.6 (Chabauty)**.** *Let C be a curve of genus $g \geq 2$ defined over $\mathbb{Q}$. Let J be the Jacobian of C and let p be a prime. Let r and r' be as above. Suppose $r' < g$, then $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite. In particular, $C(\mathbb{Q})$ is finite.*

Proof. See [13]. □

Remark 6.7. The condition of $r' \leq g$, difficult to verify in general, is automatically satisfied if $r < g$, thanks to Lemma 6.5. In our case, as shown in chapter 5, we have that $\operatorname{rank} J_i(\mathbb{Q}) < g = 3$ for all the $J_i's$ but J_5; in the latter we have $\operatorname{rank} J_5(\mathbb{Q}) = 3$ and this is exactly why the curve C_5 needs a separate treatment.

We say that the $1-$form ω kills a subset $S \subset J(\mathbb{Q}_p)$ if $\lambda_\omega|_s = 0$. By linear algebra, we can find at least $g - r > 0$ indepentents $1-$forms ω killing $J(\mathbb{Q})$ (and hence $C(\mathbb{Q})$). By "finding" a $1-$form, we mean computing its formal power series expansion inl local coordinates. Coleman's method consists essentially in bounding

the number of common zeros of the corresponding integrals λ_ω on $J(\mathbb{Q}_p)$ and hoping that enough points in $C(\mathbb{Q})$ are found to meet the bound: in this case these points are all of them. If this fail, we can try with a different prime, or we can combine it with the Mordell-Weil sieve to exclude some residue classes on $C(\mathbb{F}_p)$ and thus obtaining a sharper bound.

In the following we summarize the steps that we need to perform for each C_i ($i \neq 5$) to apply Coleman's theorem 6.8 in the sequel, in order to get the rational points of C_i ($i \neq 5$).
Let C be the smooth projective model of our quartic curve defined by the affine equation $g(u, v) = 0$, obtatained dehomogenizing the equations given in section 4.3.1 and let J be its Jacobian. We pick a point $P \in C(\mathbb{Q})$ (this can be always done for our curves) and identify C as the subvariety of J given by the following embedding:

$$\begin{aligned} C &\hookrightarrow J \\ T &\mapsto [T - P], \end{aligned}$$

where $[T - P]$ is the class of $T - P$ in J.

- For the computations, we need $G_1, \ldots, G_r \in J(\mathbb{Q})$, where $r = \operatorname{rank} J(\mathbb{Q})$, in such a way that the group generated by these points has finite index in $J(\mathbb{Q})$. Usually we obtain this information during the computation of r done in chapter 5.

- We pick t uniformizing parameter at P that is also a uniformizer at P modulo p. (Recall that C is smooth and that has good reduction at p).

- For each i, $1 \leq i \leq r$, we compute $m_i \in \mathbb{Z}_{\geq 1}$ such that $m_i G_i$ reduces to 0 modulo p.

- For each i we find a divisor of the form $D_i - 3P$ linearly equivalent to $m_i G_i$, where $D_i = P_{i,1} + P_{i,2} + P_{i,3}$ is an effective divisor of degree 3 defined over $\mathbb{Q}$.

- If we choose P such that its reduction modulo p is not an inflection point, then we have that each of the $P_{i,j}$ is congruent to P modulo p.

- Since the genus of C is 3, the space of holomorphic differentials of C has dimension 3, and we can compute a basis $\omega_1, \omega_2, \omega_3$. Then we can express formally each such ω_j as an element of $\mathbb{Q}[[t]]dt$. A formal integration gives us $\lambda_j = \int_0^t \omega_j \in t\mathbb{Q}[[t]]$ with $j = 1, 2, 3$.

- Now we compute, for each $1 \leq i \leq r$ and each $1 \leq j \leq 3$, the following expression:

$$\begin{aligned}\lambda_{\omega_j}(m_iG_i) &= \int_0^{m_iG_i} \iota_*\omega_j = \int_0^{[D_i-3P]} \iota_*\omega_j \\ &= \int_P^{P_{i,1}} \omega_j + \int_P^{P_{i,2}} \omega_j + \int_P^{P_{i,3}} \omega_j \\ &= \lambda_j(t(P_{i,1})) + \lambda_j(t(P_{i,2})) + \lambda_j(t(P_{i,3}));\end{aligned}$$

where $\iota_*\omega$ denotes the pushforward of ω induced by $C \hookrightarrow J$.

- Since the $P_{i,k}$ are congruent to P modulo p, we have that the $t(P_{i,k})$ have positive p-adic valuation, hence the series converge $p-$adically.
- With linear algebra we can compute the kernel of the map $\omega \mapsto (\lambda_\omega(m_1G_1), \dots, \lambda_\omega(m_rG_r))$. This way we find $s = 3 - r$ independent holomorphic differentials $\eta_1, \dots, \eta_s$ such that the related 1-forms on $J_{\mathbb{Q}_p}$ kill $J(\mathbb{Q})$.
- For each $1 \leq i \leq s$, we rescale η_i such that modulo p it reduces to a nonzero differential $\tilde{\eta}_i$.
- For $Q \in C(\mathbb{F}_p)$, set

$$\nu = \min_{1 \leq i \leq s} v_Q(\tilde{\eta}_i).$$

Then a (slightly sharper) version of Coleman's original result says the following:

Theorem 6.8 (Coleman improved version)**.** *Let $Q \in C(\mathbb{F}_p)$ and let ν be as above. Then, if $p > \nu + 1$, then there are at most $\nu + 1$ rational points on C that reduce to Q modulo p.*

Proof. See [17] for Coleman's original proof; or [58] and [40] for the sharper results. □

Remark 6.9. For some of our C_i, in particular for $i = 1, 3, 7, 8, 9, 10$; we want to do a Chabauty argument using the prime 7 where C_i has bad reduction. The argument is essentially the same, but we have to consider the Néron model of J_i. In all of the cases we consider, we find that $J_i(\mathbb{F}_7) \simeq (\mathbb{Z}/7\mathbb{Z})^3$.
See [40, Appendix A] for the general approach to this case.

6.3 The strategy for the C_i's, $i \neq 5$

In this section we sketch the Mordell-Weil sieve and the Chabauty's arguments for the curves C_i, $i \neq 5$. We refer to the notation of appendix B for the known rational points on the curves.
Define the *known part* $J_i(\mathbb{Q})_{known}$ of $J_i(\mathbb{Q})$ as the subgroup generated by the rational points of appendix B and the element $[R - 3P]$ of lemma 5.11.

6.3.1 Computing $C_1(\mathbb{Q})$

We want to show that

$$C_1(\mathbb{Q}) = \{P_1, P_2, P_3, P_4\}.$$

As prime we use $p = 7$. As said in remark 6.9, we have that $J_1(\mathbb{F}_7) \simeq (\mathbb{Z}/7\mathbb{Z})^3$. From section 5.1 we also get that $\dim_{\mathbb{F}_7} J_1(\mathbb{Q}/7J_1(\mathbb{Q}) = 2$. Moreover the reduction of $J_1(\mathbb{Q})_{known}$ has also dimension 2, so that is the reduction of the whole $J_1(\mathbb{Q})$. Using P_4 as a basepoint, we easily see that there are four points in $C_1(\mathbb{F}_7)$: they are the reductions of the four known rational points on C_1. So it suffices to show that there is only one point of $C_1(\mathbb{Q})$ in each of those residue classes.
Now we compute the reductions modulo 7 of the differentials killing $J_1(\mathbb{Q})$ and we find

$$\tilde{\eta}_1 \longleftrightarrow x + 2y$$
$$\tilde{\eta}_2 \longleftrightarrow x - z.$$

Since their common zero in $\mathbb{P}^2(\mathbb{F}_7)$ is not on C_1, we have that $\min\{v_Q(\tilde{\eta}_1, v_Q(\tilde{\eta}_2)\} = 0$ and so there is at most one rational point per residue class by theorem 6.8.

6.3.2 Computing $C_2(\mathbb{Q})$

We want to show that

$$C_2(\mathbb{Q}) = \{P_5, P_6, P_7, P_8, P_9\}.$$

As prime we use $p = 5$; we get that $J_2(\mathbb{F}_5) \simeq \mathbb{Z}/126\mathbb{Z}$ and the reduction of $J_2(\mathbb{Q})_{known}$ is the cyclic subgroup of order 63. Using P_8 as a basepoint, we find that the five known rational points reduce to different points in $C_2(\mathbb{F}_5)$, which has size 6. The reductions of the differentials killing $J_2(\mathbb{Q})$ are

$$\tilde{\eta}_1 \longleftrightarrow z$$
$$\tilde{\eta}_2 \longleftrightarrow x + 2y.$$

Their common zero in $\mathbb{P}^2(\mathbb{F}_5)$ is not on C_2, so each of the six residue classes contains at most one rational point. Since five of the six do contain a rational point, the last thing that we prove is that there are no rational points on C_2 that reduces into the sixth class.

6.3.3 Computing $C_3(\mathbb{Q})$

We want to show that

$$C_3(\mathbb{Q}) = \{P_{10}, P_{11}, P_{12}, P_{13}\}.$$

As prime we use $p = 7$ and, as for C_1, we have again that $J_1(\mathbb{F}_7) \simeq (\mathbb{Z}/7\mathbb{Z})^3$ and $\dim_{\mathbb{F}_7} J_1(\mathbb{Q}/7J_1(\mathbb{Q}) = 2$. Moreover the reduction of $J_2(\mathbb{Q})_{known}$ has also dimension 2, so that it is the reduction of the whole $J_3(\mathbb{Q})$. Using P_{13} as basepoint, we find that there are exactly four points of $C_3(\mathbb{F}_7)$ in the reduction of $J_3(\mathbb{Q})$: they are the reductions of the four known rational points on C_3. The reductions of the differentials killing $J_3(\mathbb{Q})$ are

$$\tilde{\eta}_1 \longleftrightarrow 2x - y$$
$$\tilde{\eta}_2 \longleftrightarrow x + 2z.$$

And as before we can conclude that there is at most one rational point per residue class.

6.3.4 Computing $C_4(\mathbb{Q})$

We want to show that

$$C_4(\mathbb{Q}) = \{P_{14}, P_{15}, P_{16}\}.$$

As prime we use $p = 5$; we get that $J_4(\mathbb{F}_5) \simeq (\mathbb{Z}/6\mathbb{Z})^3$. The reduction of $J_4(\mathbb{Q})_{known}$ is isomorphic to $(\mathbb{Z}/6\mathbb{Z})^2$. From section 5.2.1 we get that $J_4(\mathbb{Q})$ and $J_4(\mathbb{Q})_{known}$ are both isomorphic to $\mathbb{Z}^2 \times \mathbb{Z}/4\mathbb{Z}$ and $J_4(\mathbb{Q})_{known}$ has odd index in $J_4(\mathbb{Q})$, the whole $J_4(\mathbb{Q})$ must reduce to the same $(\mathbb{Z}/6\mathbb{Z})^2$ subgroup. Using P_{14} as basepoint, we show as before that the only elements in $C_4(\mathbb{F}_5)$ in the reduction of $J_4(\mathbb{Q})$ are the restrictions of the three known rational points. Since the rank is 2, there is only one differential

$$\tilde{\eta} \longleftrightarrow x + y$$

that does not vanish on $C_4(\mathbb{F}_5)$, so that, as before, there is only one rational point in each residue class.

6.3.5 Computing $C_6(\mathbb{Q})$

We want to show that

$$C_6(\mathbb{Q}) = \{P_{21}, P_{22}, P_{23}, P_{24}\}.$$

As primes we use $p = 11, 23$. From section 5.2.1 we get again that $J_6(\mathbb{Q})$ and $J_6(\mathbb{Q})_{known}$ are both isomorphic to $\mathbb{Z}^2 \times \mathbb{Z}/4\mathbb{Z}$ and that $J_6(\mathbb{Q})_{known}$ has odd index in $J_6(\mathbb{Q})$. We have that $J_6(\mathbb{F}_{11}) \simeq (\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})$ and that the reduction of $J_6(\mathbb{Q})_{known}$ is isomorphic to $(\mathbb{Z}/8\mathbb{Z})^2 \times (\mathbb{Z}/4\mathbb{Z})$. So, as for C_4, $J_6(\mathbb{Q})$ and $J_6(\mathbb{Q})_{known}$ have the same reduction. There are five points in $C_6(\mathbb{F}_{11})$ that lye in the reduction of $J_6(\mathbb{Q})$; four of them are the reductions of the four known rational points. To prove that there are no points that reduces to the fifth class, we consider the reduction at $p = 23$; finally we show that the differential modulo 11

$$\tilde{\eta} \longleftrightarrow x + 5y$$

does not vanish at the four relevant residue classes modulo 11.

6.3.6 Computing $C_7(\mathbb{Q})$

We want to show that

$$C_7(\mathbb{Q}) = \{P_{25}, P_{26}, P_{27}\}.$$

As primes we use $p = 7, 13$. We have that $J_7(\mathbb{F}_7) \simeq (\mathbb{Z}/7\mathbb{Z})^3$, and from section 5.2.1 we get that $J_7(\mathbb{Q})$ has rank 2 and no 7-torsion. Moreover the reduction of $J_7(\mathbb{Q})_{known}$ is isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$. We use P_{25} as a basepoint; we discover that the only elements in $C_7(\mathbb{F}_7)$ in the reduction of $J_7(\mathbb{Q})$ are the reductions of the three known rational points. Our differential modulo 7 is

$$\tilde{\eta} \longleftrightarrow x - 2z,$$

it does not vanish at P_{26} and at P_{27}, but it has a simple zero at P_{25}. So in principle we may have two rational points in the third residue class of P_{25}.
We repeat the Chabauty argument with $p = 13$: its differential is

$$\tilde{\omega} \longleftrightarrow x - 2y,$$

that does not vanish at P_{25}. So there is only one point of $C_7(\mathbb{Q})$ in the residue class.

6.3.7 Computing $C_8(\mathbb{Q})$

We want to show that

$$C_8(\mathbb{Q}) = \{P_{28}, P_{29}\}.$$

As prime we use $p = 7$. We have that $J_8(\mathbb{F}_7) \simeq (\mathbb{Z}/7\mathbb{Z})^3$, and from section 5.2.1 we get that $J_8(\mathbb{Q})$ has rank 2 and no 7-torsion. The reduction of $J_7(\mathbb{Q})_{known}$ is isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$, soo that is also the reduction of the whole $J_8(\mathbb{Q})$. We use P_{28} as a basepoint. Then the only elements of $C_8(\mathbb{F}_7)$ in the reduction of $J_8(\mathbb{Q})$ are the reductions of the two known rational points. The differential modulo 7 is

$$\tilde{\eta} \longleftrightarrow x - y - 3z.$$

It does not vanishes at P_{28} and P_{29}, so that there is only one point of $C_8(\mathbb{Q})$ in each of those residue classes.

6.3.8 Computing $C_9(\mathbb{Q})$

We eant to show that

$$C_9(\mathbb{Q}) = \{P_{30}, P_{31}\}.$$

As primes we use $p = 7, 11, 13$ and we use P_{30} as basepoint. We know that $J_9(\mathbb{Q})_{known} \simeq \mathbb{Z}^2$ and that $J_9(\mathbb{Q})$ has rank 2 and not $7 - torsion$. We have that $J_8(\mathbb{F}_7) \simeq (\mathbb{Z}/7\mathbb{Z})^3$. There are four points of $C_9(\mathbb{F}_7)$ in the reduction of $J_9(\mathbb{Q})$: two of them correspond to the reductions of the two known rational points. We eliminate the other two possibilities with a similar argument at $p = 13$.
Now the differential modulo 7 is

$$\tilde{\eta} \longleftrightarrow x - y - 2z.$$

it does not vanish at P_{30} but it has a simple zero at P_{31}. So in principle we may have two rational points in the third residue class of P_{31}.
We repeat the Chabauty argument with $p = 11$: its differential is

$$\tilde{\omega} \longleftrightarrow x - 5y + 4z,$$

that does not vanish at P_{31}. So there is only one point of $C_9(\mathbb{Q})$ in this residue class.

6.3.9 Computing $C_{10}(\mathbb{Q})$

We want to show that

$$C_{10}(\mathbb{Q}) = \{P_{32}, P_{33}\}.$$

As prime we use 7. As before wfe have that $J_{10}(\mathbb{F}_7) \simeq (\mathbb{Z}/7\mathbb{Z})^3$. Also the group $J_{10}(\mathbb{Q})$ has rank 2 and no 7-torsion. The reduction of $J_{10}(\mathbb{Q})_{known}$ is isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$, so that as before is also the reduction of the whole $J_{10}(\mathbb{Q})$. We use P_{32} as a basepoint. Then we show that the only elements in $C_{10}(\mathbb{F}_7)$ in the reduction of $J_{10}(\mathbb{Q})$ come from the two known rational points. So, as usually, it suffices to show that there is only one point of $C_{10}(\mathbb{Q})$ in each of the residue classes. The differential modulo 7 is

$$\tilde{\eta} \longleftrightarrow x + y + 3z;$$

it does not vanish on the reductions of P_{32} and P_{33} and this proves the claim.

6.4 The strategy for C_5

See [46, §13] for the full details of this section.
To approach C_5, first of all we need to define the following sets:

$$\begin{aligned} C_5(\mathbb{Q}_2)_{\text{subset}} &= \{P \in C_5(\mathbb{Q}_2) : P \equiv P_{17} \text{ or } P_{20} \mod 2\} \\ C_5(\mathbb{Q}_3)_{\text{subset}} &= \{P \in C_5(\mathbb{Q}_3) : P \equiv P_{18} \mod 3\} \\ C_5(\mathbb{Q})_{\text{subset}} &= \{P \in C_5(\mathbb{Q}) : P \in C_5(\mathbb{Q}_2)_{\text{subset}} \cap C_5(\mathbb{Q}_3)_{\text{subset}}\}. \end{aligned}$$

Remark 6.10. If $Q_1, Q_2 \in \mathbb{P}^2(\mathbb{Q}_p)$, we say that $Q_1 \equiv Q_2 \mod p$ if the image of Q_1 and Q_2 under the restricion map $\mathbb{P}^2(\mathbb{Q}_p) \longrightarrow \mathbb{P}^2(\mathbb{F}_p)$ are equal.

Lemma 6.11. *Let p be 2 or 3. If $P \in C_5(\mathbb{Q}_p)$ and the image of P in $\mathbb{P}^1(\mathbb{Q}_p)$ is in $j(S(\mathbb{Z}_p))$, then $P \in C_5(\mathbb{Q}_p)_{\text{subset}}$.*

Proof. The proof is pretty much a straightforward computation reducing the equation defining C_5 modulo 2 and 3. See [46, lemma 7.8]. □

Remark 6.12. Thanks to lemma 6.11, it will be enough to determine $C_5(\mathbb{Q})_{\text{subset}}$ instead of the whole $C_5(\mathbb{Q})$. In this section eventually we will show that $C_5(\mathbb{Q})_{\text{subset}}$ is empty.

To prove the result, we must use the sieve information at the bad primes 2 and 3: in fact we will use only the component groups of the Néron models at 2 and 3. Finally we will retrieve some sieve information at some primes of good reductions to get a contradition.
Let $Q_i \in J()$ be the class of the divisor $P_i - P_{17}$, for $i = 17, 18, 19, 20$. Let $\mathcal{Q}$ be the subgroup of $J(\mathbb{Q})$ generated by the Q_i. We will show that the index $(J_5(\mathbb{Q}) : \mathcal{Q})$ is relatively prime to 14, and we will use groups of order divisible only by 2 and 7 in the sieve. We will determine the set $(n_{18}, n_{19}, n_{20}) \in \mathbb{Z}^3$ such that $n_{18}Q_{18} + n_{19}Q_{19} + n_{20}Q_{20}$ satisfies the siece conditions.

- From the sieve information at 3, we get that if $P \in C_5(\mathbb{Q})_{\text{subset}}$ and $n_{18}Q_{18} + n_{19}Q_{19} + n_{20}Q_{20} = [P - P_{17}]$, then

$$n_{18} + 3n_{20} \equiv 1 \mod 7. \tag{6.1}$$

- From the sieve information at 2, if $P \in C_5(\mathbb{Q})_{\text{subset}}$ we get that

$$n_{18}(0,3) + n_{19}(0,3) + n_{20}(1,2) \equiv (0,0) \text{ or } (1,0) \text{ or } (1,2) \mod 4. \tag{6.2}$$

- From the sieve information at 23 (of good reduction) we get that n_{18} and n_{19} should be both even.

- From the sieve information at 97 (of good reduction) and all the previous conditions we get that (n_{18}, n_{19}, n_{20}) is congruent modulo 14 to one of the following:

$$(2,10,9), \quad (6,2,10), \quad (6,10,10), \quad (8,0,7). \tag{6.3}$$

- From the sieve information at 13 (of good reduction) we get that the image of $C_5(\mathbb{F}_{13})$ in $J_5(\mathbb{F}_{13})/14J_5(\mathbb{F}_{13})$ has size 6, and the resulting conditions on (n_{18}, n_{19}, n_{20}) modulo 14 contradict those of (6.3).

To conclude the proof, we need this last result:

Lemma 6.13. *The index* $(J_5(\mathbb{Q}) : \mathcal{Q})$ *is relatively prime to* 14.

Proof. By the resuts in chapter 5, we get that $J_5(\mathbb{Q}) \simeq \mathbb{Z}^3$. The image of $\mathcal{Q}$ under $J_5(\mathbb{Q}) \longrightarrow J_5(\mathbb{F}_{23})/2J_5(\mathbb{F}_{23})$ has $\mathbb{F}_2$-rank 3, so $2 \nmid (J(_5(\mathbb{Q}) : \mathcal{Q})$. Finally the image of $\mathcal{Q}$ under

$$J_5(\mathbb{Q}) \to \frac{J_5(\mathbb{F}_{13})}{7J_5(\mathbb{F}_{13})} \times \frac{J_5(\mathbb{F}_{97})}{7J_5(\mathbb{F}_{97})}$$

has $\mathbb{F}_7$- rank 3, so $7 \nmid (J(_5(\mathbb{Q}) : \mathcal{Q})$. Thus $14 \nmid (J(_5(\mathbb{Q}) : \mathcal{Q})$. □

So we get that $C_5(\mathbb{Q})_{\text{subset}}$ is empty, hence thanks to lemma 6.11 we have that there are no points on $C_5(\mathbb{Q})$ giving us solutions in $S(\mathbb{Z})$.

This concludes the proof of the main theorem 2.2.

Appendix A

The set $\mathcal{H}$

In section 4.2.2 is shown that all the irreducibles relevants $\mathcal{G}$-modules $E[7]$ comes from quadratic twists of curves in a specific set $\mathcal{H}$ (cf. Lemma 4.11). Here follows the list of equations of these elliptic curves, with the Cremona label from [19] for each one. The equations are written in terms of the classical minimal projective model

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

(24A1): $Y^2Z = X^3 - X^2Z - 4XZ^2 + 4Z^3$

(27A1): $Y^2Z + YZ^2 = X^3 - 7Z^3$

(32A1): $Y^2Z = X^3 + 4XZ^2$

(36A1): $Y^2Z = X^3 + Z^3$

(54A1): $Y^2Z + XYZ = X^3 - X^2Z + 12XZ^2 + 8Z^3$

(96A1): $Y^2Z = X^3 + X^2Z - 2XZ^2$

(108A1): $Y^2Z = X^3 + 4Z^3$

(216A1): $Y^2Z = X^3 - 12XZ^2 + 20Z^3$

(216B1): $Y^2Z = X^3 - 3XZ^2 - 34Z^3$

(288A1): $Y^2Z = X^3 + 3XZ^2$

(864A1): $Y^2Z = X^3 - 3XZ^2 + 6Z^3$

(864B1): $Y^2Z = X^3 - 24XZ^2 + 48Z^3$

(864C1): $Y^2Z = X^3 + 24XZ^2 - 16Z^3$

If we want to recover the standard Weirestrass equation over a field of char $\neq 2, 3$, following [56, III.1], we define the following quantities:

$$
\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= 2a_4 + a_1 a_3 \\
b_6 &= a_3^2 + 4a_6 \\
c_4 &= b_2^2 - 24 b_4 \\
c_6 &= -b_2^3 + 36 b_2 b_4 - 216 b_6.
\end{aligned}
$$

Then the (affine) model is given by the Weierstrass equation

$$y^2 = x^3 - 27 c_4 x - 54 c_6.$$

Appendix B

Known rational points on $C_1, \ldots, C_{10}$

Here we list all the known $\mathbb{Q}$-rational points on the quartic curves $C_1, \ldots, C_{10}$, whose equations can be found in section 4.3.1. In sections 6.3 and 6.4 we proved that this points are actually all the rational points of the curves except perharps for C_5. In the latter case, we proved instead that a primitive integer solution to $x^2 + y^3 = z^7$ coming from a rational point of C_5 (in the sense of section 4.3.1), should come from one of the rational points listed below: this suffices to our purpose. The table also lists the Mordell-Weil rank of each Jacobian J_i computed in chapter 5 and the primitive solutions to $x^2 + y^3 = z^7$ that comes from each rational points (if any).

In section 4.3.1 there is a picture that shows the connection between the curves C_j's, their rational points P_i's and the primitive integer solutions of $x^2 + y^3 = z^7$.

Curve	rank $J_i(\mathbb{Q})$	Points		Primitive solutions
C_1	1	P_1	$(1:0:0)$	$(\pm1,-1,0)$
		P_2	$(0:1:0)$	$(\pm1,-1,0)$
		P_3	$(0:0:1)$	$(\pm1,-1,0)$
		P_4	$(1:-1:2)$	–
C_2	1	P_5	$(1:0:0)$	$(\pm1,-1,0)$
		P_6	$(0:1:0)$	$(\pm1,-1,0)$
		P_7	$(0:0:1)$	$(\pm1,-1,0)$
		P_8	$(1:1:-1)$	–
		P_9	$(1:-2:-1)$	–
C_3	1	P_{10}	$(1:0:0)$	$(\pm1,-1,0)$
		P_{11}	$(0:1:0)$	$(\pm1,-1,0)$
		P_{12}	$(0:0:1)$	$(\pm1,-1,0)$
		P_{13}	$(1:1:-1)$	–
C_4	2	P_{14}	$(1:0:0)$	$(\pm1,0,1)$
		P_{15}	$(0:1:0)$	$(\pm1,0,1)$
		P_{16}	$(0:1:1)$	–
C_5	3	P_{17}	$(1:0:0)$	–
		P_{18}	$(0:1:0)$	–
		P_{19}	$(0:0:1)$	–
		P_{20}	$(1:1:1)$	–
C_6	2	P_{21}	$(0:1:0)$	$\pm(0,1,1)$
		P_{22}	$(1:-1:0)$	$\pm(0,1,1)$
		P_{23}	$(0:1:1)$	$(\pm15312283,9262,113)$
		P_{24}	$(0:1:-1)$	$(\pm15312283,9262,113)$
C_7	2	P_{25}	$(0:1:0)$	–
		P_{26}	$(0:0:1)$	$(\pm2213459,1414,65)$
		P_{27}	$(0:1:1)$	$(\pm21063928,-76271,17)$
C_8	2	P_{28}	$(0:0:1)$	$(\pm3,-2,1)$
		P_{29}	$(2:-1:0)$	–
C_9	2	P_{30}	$(0:0:1)$	–
		P_{31}	$(1:1:0)$	–
C_{10}	2	P_{32}	$(1:0:0)$	$(\pm71,-17,2)$
		P_{33}	$(1:1:0)$	–

Bibliography

[1] Alejandro Adem, Johann Leida, and Yongbin Ruan. *Orbifolds and stringy topology*, volume 171 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2007.

[2] Karim Belabas, Frits Beukers, Pierrick Gaudry, William McCallum, Bjorn Poonen, Samir Siksek, Michael Stoll, and Mark Watkins. *Explicit methods in number theory*, volume 36 of *Panoramas et Synthèses [Panoramas and Syntheses]*. Société Mathématique de France, Paris, 2012. Rational points & Diophantine equations, Lectures from the Special Trimester held at the Institut Henri Poincaré, Paris, September–December 2004.

[3] Michael A. Bennett. The equation $x^{2n}+y^{2n} = z^5$. *J. Théor. Nombres Bordeaux*, 18(2):315–321, 2006.

[4] Michael A. Bennett and Chris M. Skinner. Ternary Diophantine equations via Galois representations and modular forms. *Canad. J. Math.*, 56(1):23–54, 2004.

[5] Frits Beukers. The Diophantine equation $Ax^p + By^q = Cz^r$. *Duke Math. J.*, 91(1):61–88, 1998.

[6] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[7] Nicolas Bourbaki. *Lie groups and Lie algebras. Chapters 1–3*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[8] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[9] Nils Bruin. The Diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$. *Compositio Math.*, 118(3):305–321, 1999.

[10] Nils Bruin. On powers as sums of two cubes. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 169–184. Springer, Berlin, 2000.

[11] Nils Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[12] Nils Bruin. The primitive solutions to $x^3 + y^9 = z^2$. *J. Number Theory*, 111(1):179–189, 2005.

[13] Claude Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C. R. Acad. Sci. Paris*, 212:882–885, 1941.

[14] Imin Chen. On the equation $s^2 + y^{2p} = \alpha^3$. *Math. Comp.*, 77(262):1223–1227, 2008.

[15] Imin Chen. On the equation $a^2 + b^{2p} = c^5$. *Acta Arith.*, 143(4):345–375, 2010.

[16] Imin Chen and Samir Siksek. Perfect powers expressible as sums of two cubes. *J. Algebra*, 322(3):638–656, 2009.

[17] Robert F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[18] Brian Conrad, Fred Diamond, and Richard Taylor. Modularity of certain potentially Barsotti-Tate Galois representations. *J. Amer. Math. Soc.*, 12(2):521–567, 1999.

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

[20] Sander R. Dahmen. *Classical and modular methods applied to Diophantine equations*. PhD thesis, Univ. of Utrecht, 2008. Available at dspace.library.uu.nl/handle/1874/29640.

[21] Sander R. Dahmen. A refined modular approach to the Diophantine equation $x^2 + y^{2n} = z^3$. *Int. J. Number Theory*, 7(5):1303–1316, 2011.

[22] Henri Darmon. The equation $x^4 - y^4 = z^p$. *C. R. Math. Rep. Acad. Sci. Canada*, 15(6):286–290, 1993.

[23] Henri Darmon and Andrew Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[24] Henri Darmon and Loïc Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

[25] Fred Diamond. On deformation rings and Hecke rings. *Ann. of Math. (2)*, 144(1):137–166, 1996.

[26] Johnny Edwards. A complete solution to $X^2 + Y^3 + Z^5 = 0$. *J. Reine Angew. Math.*, 571:213–236, 2004.

[27] Noam D. Elkies. The Klein quartic in number theory. In *The eightfold way*, volume 35 of *Math. Sci. Res. Inst. Publ.*, pages 51–101. Cambridge Univ. Press, Cambridge, 1999.

[28] Jordan S. Ellenberg. Corrigendum to: "Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$" [Amer. J. Math. **126** (2004), no. 4, 763–787; mr2075481]. *Amer. J. Math.*, 127(6):1389, 2005.

[29] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[30] William Fulton. *Algebraic curves. An introduction to algebraic geometry.* W. A. Benjamin, Inc., New York-Amsterdam, 1969. Notes written with the collaboration of Richard Weiss, Mathematics Lecture Notes Series.

[31] Tomás L. Gómez. Algebraic stacks. *Proc. Indian Acad. Sci. Math. Sci.*, 111(1):1–31, 2001.

[32] Emmanuel Halberstadt and Alain Kraus. Sur la courbe modulaire $X_E(7)$. *Experiment. Math.*, 12(1):27–40, 2003.

[33] Robin Hartshorne. *Algebraic geometry.* Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[34] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2000. An introduction.

[35] Neal Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1993.

[36] A. Kraus and J. Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293(2):259–275, 1992.

[37] Alain Kraus. Sur l'équation $a^3 + b^3 = c^p$. *Experiment. Math.*, 7(1):1–13, 1998.

[38] Serge Lang. *Introduction to algebraic and abelian functions*, volume 89 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, second edition, 1982.

[39] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics.* Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[40] William McCallum and Bjorn Poonen. The method of Chabauty and Coleman. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 99–117. Soc. Math. France, Paris, 2012.

[41] James S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[42] James S. Milne. Shimura varieties and moduli (v2.00), 2011. Available at www.jmilne.org/math/.

[43] James S. Milne. Modular functions and modular forms (v1.30), 2012. Available at www.jmilne.org/math/.

[44] Ieke Moerdijk. Orbifolds as groupoids: an introduction. In *Orbifolds in mathematics and physics (Madison, WI, 2001)*, volume 310 of *Contemp. Math.*, pages 205–222. Amer. Math. Soc., Providence, RI, 2002.

[45] Bjorn Poonen and Edward F. Schaefer. Explicit descent for Jacobians of cyclic covers of the projective line. *J. Reine Angew. Math.*, 488:141–188, 1997.

[46] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll. Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$. *Duke Math. J.*, 137(1):103–158, 2007.

[47] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[48] G. Salmon. *A Treatise on the Higher Plane Curves: Intended as a Sequel to a Treatise on Conic Sections.* Hodges, Foster and Figgis, Dublin, third edition, 1879.

[49] Edward F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. *Math. Ann.*, 310(3):447–471, 1998.

[50] Victor Scharaschkin. The Brauer-Manin obstruction for curves, December 2004. Preprint.

[51] Jean-Pierre Serre. *Groupes algébriques et corps de classes.* Publications de l'institut de mathématique de l'université de Nancago, VII. Hermann, Paris, 1959.

[52] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[53] Jean-Pierre Serre. *Galois cohomology.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.

[54] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[55] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1994.

[56] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, Dordrecht, second edition, 2009.

[57] Alexei Skorobogatov. *Torsors and rational points*, volume 144 of *Cambridge Tracts in Mathematics.* Cambridge University Press, Cambridge, 2001.

[58] Michael Stoll. Independence of rational points on twists of a given curve. *Compos. Math.*, 142(5):1201–1214, 2006.

[59] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[60] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1997.

[61] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.