Torsion on elliptic curves

Jan Vonk

Contents

1 Introduction **3**
1.1 The Mordell–Weil theorem . . . 3
1.2 Classification of torsion . . . 9
1.3 Galois modules of torsion points . . . 10
1.4 Outline and preprequisites . . . 12

2 Descent and the Mordell–Weil theorem **13**
2.1 Selmer groups . . . 13
2.2 The weak Mordell–Weil theorem . . . 14
2.3 The method of 2-descent on elliptic curves . . . 15
2.4 Modular curves . . . 17

3 Modular curves and flat descent **19**
3.1 The flat topology . . . 20
3.2 Torsion points of order 11 . . . 22
3.3 Torsion points of order 13 . . . 25
3.4 Mazur's theorem on torsion . . . 28

4 Exercises **31**

Bibliography **33**

Last updated on August 12, 2022. Comments and corrections are welcome on `j.b.vonk@math.leidenuniv.nl`

1 Introduction

These are notes of a mini-course at the summer school at Baskerville Hall (Hay-on-Wye) held on 8-12 August 2022, organised by Vladimir Dokchitser and Céline Maistret. The meeting marks the 100th anniversary of the Mordell–Weil theorem. The lectures focus on the torsion subgroup of the Mordell–Weil group of elliptic curves over $\mathbf{Q}$, specifically two landmark results proved in the 1970's on this topic:

- Mazur's theorem on torsion [Maz77a].
- Serre's open image theorem [Ser72].

The lectures are intended to be a first initiation to some ideas in these papers. The full extent of these results is too ambitious to treat satisfactorily in three hours of lectures. These written notes are intended to complement the lectures and provide slightly more context, details, and references for the more technical parts of our discussion of Mazur's theorem. Ultimately, their scope remains limited, and students aspiring to study these results seriously are referred to the original sources, which are both masterfully crafted.

1.1 The Mordell–Weil theorem

The study of rational points on elliptic curves has a long and rich tradition that stretches across different historical eras, languages, and geographical borders. Today we celebrate the centenary of the Mordell–Weil theorem, whose development followed efforts of many mathematicians. In this motivational introduction, we discuss a few of them. We do not attempt to give an exhaustive, or even adequate, historical treatment. Instead, we cherry-pick precedents for the later developments we wish to discuss in these notes.

The method of ascent

We begin with (perhaps) the earliest reference to an elliptic curve in recorded history. Already, it involves the mechanism of 'ascent', a way to proliferate solutions to cubic equations. In Diophantus' Artihmetika [DioAD] Problem 24 of Book IV, taken here from the late 19th century reproduction [Dio93], poses the following question:

κδ.

Δοθέντα ἀριθμὸν διελεῖν εἰς δύο ἀριθμούς, καὶ ποιεῖν τὸν ὑπ' αὐτῶν κύβον παρὰ πλευράν.

Diophantus asks the reader to "divide a given number into two numbers whose product is a cube minus its side". By means of an example, the book of Diophantus explains how to solve this problem for the number

6, by finding a rational solution[1] to the equation

$$y(6-y) = x^3 - x. \tag{1.1}$$

The method used by Diophantus is remarkable. It makes in a purely algebraic way use of the doubling formula of a point on an elliptic curve. More precisely, Diophantus considers solutions to the equation (1.1) that satisfy the additional equation $x = 3y - 1$. By substitution, we find the relation

$$27y^3 - 26y^2 = 0.$$

This cubic polynomial has a double root at $y = 0$ and another one at $y = 26/27$ from which Diophantus obtains the solution

$$6 = 26/27 + 136/27.$$

This construction may be summarised in modern language by saying that Diophantus notes the existence of an obvious (but in his eyes utterly unacceptable) solution $(x, y) = (-1, 0)$ and computes that the tangent line to the elliptic curve E defined by (1.1) intersects E again in a rational point with coordinates

$$(x, y) = \left(\frac{17}{9}, \frac{26}{27}\right).$$

The tangent line construction of Diophantus is visualised in Figure 1.1.

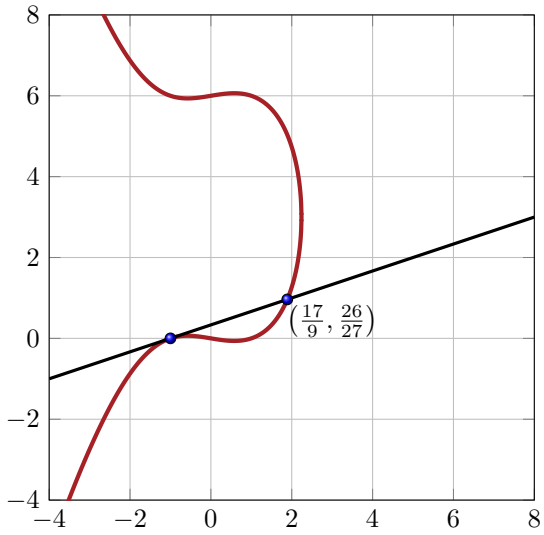


Figure 1.1: The elliptic curve $E : y(6-y) = x^3 - x$

It is quite remarkable that the first widely known historical occurrence of an elliptic curve already uses its group law implicitly, effectively doubling a point (or rather, multiplying it by -2) to obtain a new point. Since typically the complexity of the coordinates grows by applying this procedure of producing new solutions from old ones, we might call it the method of 'ascent'. The true significance of this construction of Diophantus took many centuries to obtain its modern formulation. One of the first explicit modern

[1] We should note that for Diophantus, only positive rational solutions would be considered valid.

descriptions of the group law on elliptic curves and Jacobians of curves may be found in the work of Poincaré [Poi01] at the beginning of the 20th century. In this paper, Poincaré makes the following comments:

PROPRIÉTÉS ARITHMÉTIQUES DES COURBES ALGÉBRIQUES. 171

On peut se proposer de choisir les arguments

$$(2) \qquad \alpha, \quad \alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_q,$$

de telle façon que la formule (1) comprenne tous les points rationnels de la cubique. Les $q+1$ points rationnels qui ont les arguments (2) formeront alors ce que nous appellerons un *système de points rationnels fondamentaux*.

Il est clair que l'on peut choisir d'une infinité de manières le système des points rationnels fondamentaux. On devra tout d'abord dans ce choix s'arranger de telle façon que le nombre $q+1$ des points fondamentaux soit aussi petit que possible. Cette valeur minima de ce nombre $q+1$ sera ce que j'appellerai le *rang* de la cubique; c'est évidemment un élément très important de la classification des cubiques rationnelles.

The realisation that the group law on elliptic curves gives a proliferation of rational solutions begs the question (which is precisely what Poincaré ponders here) what minimum amount of fundamental solutions is needed to produce *all* solutions in this way, a quantity for which Poincaré coins the term "rank".

Fundamentally, we should wonder whether the rank is always *finite*? At its core, this problem asks us to reverse the process of ascent occurring in Diophantus, and backtrack all the way to a fundamental set of generators. The question of finiteness of the rank remained open until the groundbreaking paper of Mordell [Mor22], which develops the important method of descent.

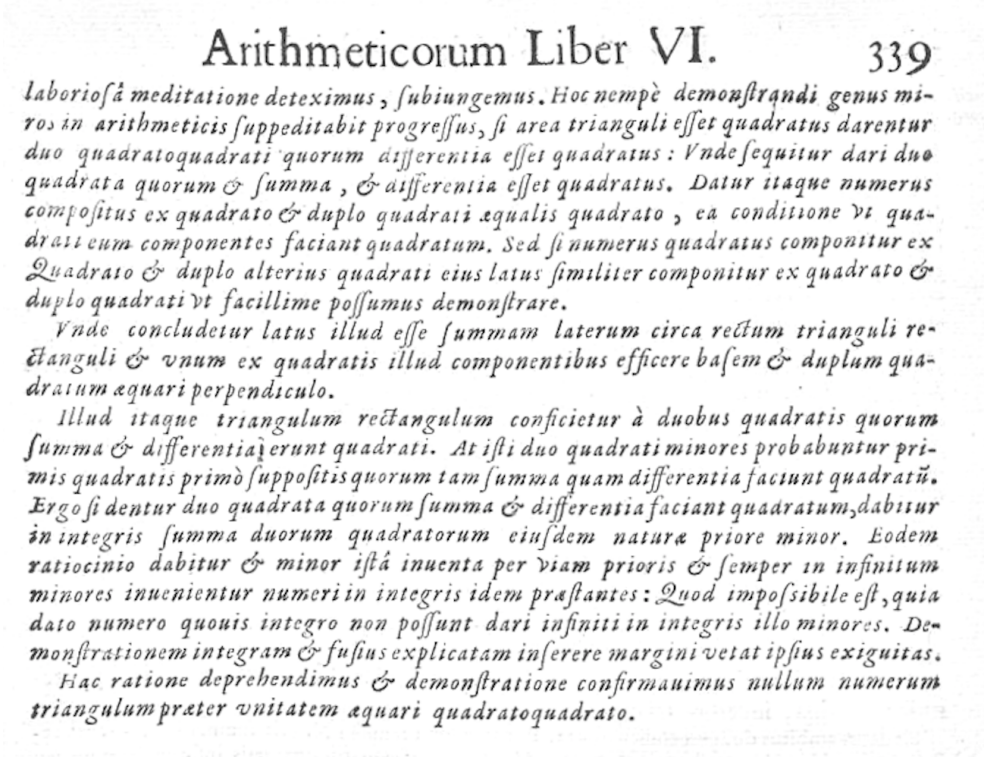
The method of descent

The origins of the method of descent occur in the work of Fermat, who applies it to a variety of problems which he describes in his 1659 letter to Pierre de Carcavi [dF59]. Perhaps his most famous application of this principle survives in the only complete proof of the hand of Fermat that survived today, where he shows that congruent numbers (areas of right angled triangles with rational side lengths) are never squares [Fer70]. Fermat reduces this problem to showing there are no non-trivial solutions to the equation

$$x^4 - y^4 = z^2. \tag{1.2}$$

In the reduction of the problem to this Diophantine equation, Fermat makes use of the explicit parametrisation of Pythagorean triples, a classical result that was certainly well known to him. To solve (1.2) however, Fermat uses a truly remarkable and original method, which we recognise in contemporary language as a descent by 2-isogeny on an elliptic curve. Fermat sounds rather pleased with his argument, stating that

"This type of demonstration will provide excellent progress in arithmetic." The proof appears entirely in prose in the following paragraph of the 1670 edition [Fer70] containing his observations.



Arithmeticorum Liber VI. 339

laborioſâ meditatione deteximus, ſubiungemus. Hoc nempè demonſtrandi genus miros in arithmeticis ſuppeditabit progreſſus, ſi area trianguli eſſet quadratus darentur duo quadratoquadrati quorum differentia eſſet quadratus: Vnde ſequitur dari duo quadrata quorum & ſumma, & differentia eſſet quadratus. Datur itaque numerus compoſitus ex quadrato & duplo quadrati æqualis quadrato, ea conditione vt quadrati eum componentes faciant quadratum. Sed ſi numerus quadratus componitur ex Quadrato & duplo alterius quadrati eius latus ſimiliter componitur ex quadrato & duplo quadrati vt facillime poſſumus demonſtrare.

Vnde concludetur latus illud eſſe ſummam laterum circa rectum trianguli rectanguli & vnum ex quadratis illud componentibus efficere baſem & duplum quadratum æquari perpendiculo.

Illud itaque triangulum rectangulum conficietur à duobus quadratis quorum ſumma & differentia erunt quadrati. At iſti duo quadrati minores probabuntur primis quadratis primò ſuppoſitis quorum tam ſumma quam differentia faciunt quadratũ. Ergo ſi dentur duo quadrata quorum ſumma & differentia faciant quadratum, dabitur in integris ſumma duorum quadratorum eiuſdem naturæ priore minor. Eodem ratiocinio dabitur & minor iſtâ inuenta per viam prioris & ſemper in infinitum minores inuenientur numeri in integris idem præſtantes: Quod impoſsibile eſt, quia dato numero quouis integro non poſſunt dari infiniti in integris illo minores. Demonſtrationem integram & fuſius explicatam inſerere margini vetat ipſius exiguitas.

Hac ratione deprehendimus & demonſtratione confirmauimus nullum numerum triangulum præter vnitatem æquari quadratoquadrato.

In modern language, we may describe the proof of Fermat as follows. Suppose we have a non-trivial solution (x, y, z) to the quartic equation (1.2), then we may assume x, y and z are coprime positive integers. From this coprime solution, Fermat constructs a new (smaller) solution, in two steps.

Step 1. We factorise the equation (1.2) as follows:

$$z^2 = x^4 - y^4 = (x^2 - y^2)(x^2 + y^2).$$

Note that the factors on the right hand side are coprime to each other. This implies that they must both be squares, i.e. there are positive integers s, t such that

$$\begin{cases} x^2 - y^2 &= s^2 \\ x^2 + y^2 &= t^2. \end{cases}$$

Observe that s and t must both be odd integers, and by changing the sign of s if necessary we may assume that $s - t \equiv 0 \pmod 4$. We then note that y must be even, and that we therefore have the following decomposition into integer factors:

$$\left(\frac{t+s}{2}\right)\left(\frac{t-s}{4}\right) = \left(\frac{y}{2}\right)^2.$$

The factors on the left hand side are coprime positive integers. We may once again conclude they are both perfect squares, so that we find odd coprime positive integers u, v that satisfy the equalities

$$\begin{cases} s &= u^2 - 2v^2 \\ t &= u^2 + 2v^2. \end{cases} \tag{1.3}$$

Note that we have now produced a triple (u, v, x) that satisfies $u^4 + 4v^4 = x^2$. Moreover, the triple (x, y, z) may be recovered from the triple (u, v, x) by the identities $y = 2uv$ and $z = u^4 - 4v^4$.

Step 2. Note that the relation

$$u^4 + 4v^4 = x^2$$

satisfied by the triple (u, v, x) constructed in step 1 implies in particular that $(u^2, 2v^2, x)$ is a Pythagorean triple. As such, we may find coprime positive integers m, n satisfying

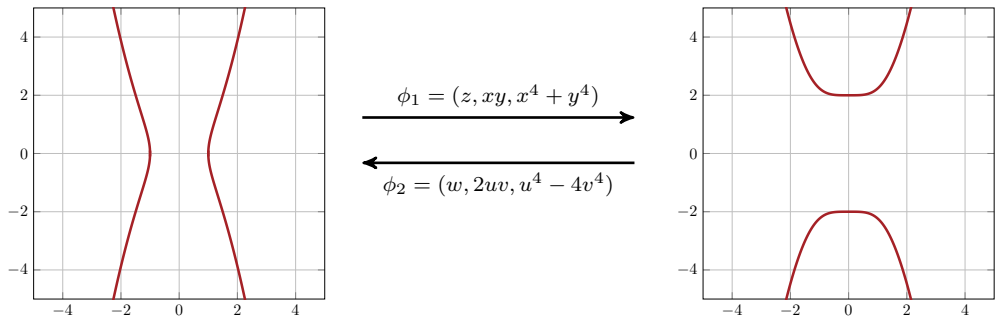
$$\begin{cases} u^2 &= m^2 - n^2 \\ 2v^2 &= 2mn \\ x &= m^2 + n^2 \end{cases} \tag{1.4}$$

Since $v^2 = mn$ we see that m and n are both squares. Writing $m = a^2, n = b^2$ with $a, b > 0$ we find that the triple (a, b, u) is a solution to (1.2), i.e. $a^4 - b^4 = u^2$. We see that $a < a^4 + b^4 = x$ so that we constructed a new solution whose first coordinate is strictly smaller than that of the original solution. This shows that if a non-trivial solution exists, we can keep descending ad infinitum, which is absurd.

If we unpack Fermat's argument a little further, we see that it considers two genus 1 curves defined by homogeneous equations in the weighted projective plane, namely

$$\begin{array}{rcl} E_1 & : & \left\{ (x, y, z) \in \mathbf{P}^2_{[1,1,2]} \quad : \quad x^4 - y^4 = z^2 \right\} \\ E_2 & : & \left\{ (u, v, w) \in \mathbf{P}^2_{[1,1,2]} \quad : \quad u^4 + 4v^4 = w^2 \right\} \end{array} \tag{1.5}$$

They define elliptic curves after the choice of base points $(1, 0, 1) \in E_1(\mathbf{Q})$ and $(1, 0, 1) \in E_2(\mathbf{Q})$. These elliptic curves admit a pair (ϕ_1, ϕ_2) of dual rational 2-isogenies, described by:



The argument of Fermat produces for any purported non-trivial point $(x, y, z) \in E_1(\mathbf{Q})$ a preimage (a, b, u) for the multiplication by 2 map $[2] = \phi_2 \circ \phi_1$. The procedure consists of two steps, and first constructs a preimage for ϕ_2, then a preimage for ϕ_1. When taken to its natural conclusion, Fermat therefore really shows two things: First, his arguments suffice to show that

$$E_1(\mathbf{Q})/\phi_2(E_2(\mathbf{Q})) \simeq \mathbf{Z}/2\mathbf{Z} \simeq E_2(\mathbf{Q})/\phi_1(E_1(\mathbf{Q})),$$

and second, his descent argument on the ever shrinking first coordinate of a solution may be used to deduce that any solution must have one of its coordinates equal to zero. From this, one concludes that

$$\begin{array}{rcccl} E_1(\mathbf{Q}) & = & \{(1,0,1),(1,0,-1),(1,1,0),(1,-1,0)\} & \simeq & \mathbf{Z}/4\mathbf{Z} \\ E_2(\mathbf{Q}) & = & \{(1,0,1),(1,0,-1),(0,1,2),(0,1,-2)\} & \simeq & \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}\,. \end{array}$$

Nearly three centuries later, Mordell showed in his landmark paper [Mor22] how an argument of this sort can be carried out for general elliptic curves E over $\mathbf{Q}$. Mordell shows how to establish finiteness of the group $E(\mathbf{Q})/2E(\mathbf{Q})$ and deduces by an infinite descent that the group $E(\mathbf{Q})$ is finitely generated. The first paragraph of the paper of Mordell [Mor22] reads as follows.

[*Received* 1 May, *read* 22 May, 1922.]

§ 1. Mathematicians have been familiar with very few questions for so long a period with so little accomplished in the way of general results*, as that of finding the rational solutions†, or say for shortness, the solutions of indeterminate equations of genus unity of the forms

$$\left.\begin{aligned} \zeta^2 &= a\xi^4 + b\xi^3\eta + c\xi^2\eta^2 + d\xi\eta^3 + e\eta^4 \\ y^2 &= ax^4 + bx^3 + cx^2 + dx + e \end{aligned}\right\} \quad \ldots\ldots\ldots(1),$$

$$0 = f(x, y, z) \quad \ldots\ldots\ldots(2),$$

where f is a ternary homogeneous cubic in x, y, z, including as a particular case

$$y^2 = 4x^3 - g_2x - g_3 \quad \ldots\ldots\ldots(3);$$

Today another century has passed, and we might make a remark similar to what Mordell observes above. Indeed, the method for obtaining finiteness pioneered by Mordell remains essentially the only known approach. The work of Weil [Wei29] represents a very important step in the process of developing this approach. What Weil observes is that the infinite descent procedure depends on a notion of "size" which may be formalised in the notion of heights, extending the argument to general number fields, and abelian varieties. The theory of heights is the subject of Joseph Silverman's mini-course at this summer school, and I will therefore leave its discussion in his far more capable hands. The insight of Weil yielded the statement that is nowadays most commonly referred to as the *Mordell–Weil theorem*.

Theorem 1 (Mordell–Weil)**.** *Let A be an abelian variety defined over a number field K. The Mordell–Weil group $A(K)$ is finitely generated, i.e. there exist a finite subgroup $A(K)_{\mathrm{tors}} \subset A(K)$ and $r \geq 0$ such that*

$$A(K) \;\simeq\; A(K)_{\mathrm{tors}} \times\; \mathbf{Z}^r\,.$$

Suppose we are given an abelian variety A defined over a number field K. The determination of its Mordell–Weil group in practice is a widely studied computational problem. There is a striking dichotomy between the determination of the torsion subgroup, and the determination of the rank.

To fix ideas, let us consider the case of an elliptic curve E defined over K, given (say) by an explicit Weierstraß equation. The torsion subgroup $E(K)_{\mathrm{tors}}$ is usually easily determined in practice, for instance using Silverman [Sil09, VII.3, VIII.7]. Determining the rank $r \geq$ requires a comparatively much deeper

analysis, and an elaboration of the arguments appearing in Mordell [Mor22] has given us the celebrated method of *descent*, which in its present form is the most effective and systematic (essentially, the only one) to determine the Mordell–Weil group of particular examples. We assume here the reader is familiar with computations of a 2-descent as appearing in Silverman [Sil09, Chapters VIII and X], though we will recall the method in Chapter 2 and illustrate it on an explicit example.

1.2 Classification of torsion

We may wonder, for a given number field K, what the possible torsion subgroups $E(K)_{\mathrm{tors}}$ of an elliptic curve over K are. A folklore conjecture, whose origins are difficult to track down, states that the size of this torsion group is bounded by an absolute constant $B(K)$. A breakthrough on this question came from Manin [Man69], who built on methods of Demjanenko to show the following:

> В своем обзоре [(3), § 22] Касселс отмечает:
> «Следующая гипотеза вошла уже в фольклор:
> Гипотеза. *Для заданного k (и, в частности, для $k = \mathbf{Q}$) порядок групп* Ф *ограничен*».
> В этой заметке доказана справедливость соответствующего утверждения для p-компонент групп Ф:
> ТЕОРЕМА 0. *Пусть p — фиксированное простое число. Существует такая константа c (зависящая лишь от p и k), что порядок группы p-кручения k-точек эллиптической кривой, определенной над k, не превосходит c.*

In other words, Manin shows that for a fixed number field K and a fixed prime ℓ, the ℓ-part of the torsion of an elliptic curve over K is bounded by a constant. This constant depends on K and ℓ. While this falls short of establishing the boundedness conjecture stated above, the proof is rather simple and contains many ingenious ideas. The setup is to prove the theorem by showing that $X_1(\ell^n)$ has finitely many K-rational points when n is large enough. This is a trivial consequence of the Mordell conjecture, since the genus of $X_1(\ell^n)$ is unbounded as n grows. However, Manin proved his theorem before Faltings showed the Mordell conjecture, by showing that its Jacobian contains a K-simple isogeny factor A with multiplicity m satisfying

$$m > \mathrm{rk}_{\mathbf{Z}}\, A(K) \,/\, \mathrm{rk}_{\mathbf{Z}}\, \mathrm{End}_K(A)$$

using the theory of heights. To finish the proof, Manin then shows that the ℓ-torsion of elliptic curves E over K with *fixed j-invariant* $j = j(E) \in K$ is bounded. The proof is striking: Suppose that for any $n \geq 1$ there is a twist of E with a rational point of order ℓ^n. Choosing isomorphisms over an algebraic closure, Manin transports these points to the ℓ-adic Tate module of E, and shows the existence of a non-trivial submodule

$$L \subset T_\ell(E) = \varprojlim_n E[\ell^n], \qquad \text{as } G_K\text{-modules.}$$

Then, he can invoke methods of Serre [Ser68] to show that if E does not have complex multiplication, then the ℓ-adic Tate module must be irreducible. We will return to these ideas later.

For $K = \mathbf{Q}$, the spectacular work of Mazur [Maz77b, Maz77a, Maz78] completely settles these questions. Mazur brings a wealth of new ideas to the table. Like Manin, it considers the modular Jacobians $J_1(N)$ and $J_0(N)$ for sufficiently large N. We will discuss his proof in more detail in Chapter 3, and mention here only that a crucial ingredient is the existence of a nontrivial *Eisenstein quotient*

$$J_0(N) \longrightarrow J_{\mathrm{eis}}(N)$$

which is of rank zero. The methods of Mazur and subsequent developments by Kamienny [Kam92b, KM95, Edi95] developed into the work of Merel [Mer96], who showed the famous *strong uniform boundedness conjecture*:

Theorem 2. *For any $d \in \mathbf{Z}_{\geq 1}$ there exists a constant $B(d)$ such that for all elliptic curves E over a number field K with $[K : \mathbf{Q}] = d$ we have*

$$E(K)_{\mathrm{tors}} \leq B(d).$$

This result completely settles the question of boundedness in the strongest possible sense, since the bound appearing does not depend on K, only on its degree over $\mathbf{Q}$. This leaves open the question of giving an explicit list of possible torsion groups, whose determination for number fields of small degree is an ongoing effort, see for instance [KM88, Kam92a] for $d = 2$, and [JKL11, DN19, DKSS21].

The key innovation of Merel was to pass to a different quotient of the Jacobian, namely the *winding quotient*. The intricate flat descent arguments of Mazur are here replaced by the works of Gross–Zagier [GZ85, GZ86] and Kolyvagin [Kol89] which establish a sufficiently large part of the Birch–Swinnerton-Dyer conjecture to show that the rank of the winding quotient is zero. It should be pointed out however that the Eisenstein quotient has by no means left the stage, and there has been renewed recent interest in Eisenstein quotients, see for instance [WWE20, Lec21].

1.3 Galois modules of torsion points

The argument of Manin we discussed above in the context of torsion crucially relied on investigations of Serre [Ser68]. These investigations resulted in his famous *open image theorem*, a landmark result that shows that when ℓ is a large prime, a given elliptic curve $E_{/K}$ is not only free of ℓ-torsion, but in fact the Galois module $E[\ell]$ is as irreducible as possible. More precisely, for any $m \geq 1$ we have an action of the Galois group of K on the m-torsion $E[m]$, which gives a morphism

$$\rho_{E,m} : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(E[m]) = \mathrm{GL}_2(\mathbf{Z}/m\mathbf{Z}).$$

Suppose that the elliptic curve has a cyclic subgroup of order m defined over K, then the image of the morphism is contained in a Borel subgroup. In other words, with respect to a suitable choice of basis for $E[m]$, it is of the form

$$\rho_{E,m} : G_K \longrightarrow \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \leq \mathrm{GL}_2(\mathbf{Z}/m\mathbf{Z}).$$

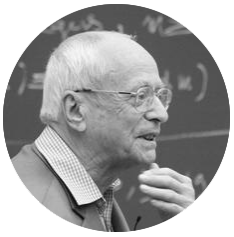
Likewise, if it has a rational point of order m defined over K, the diagonal entries must furthermore be zero, i.e. the Galois group G_K acts by transvections. The morphisms $\rho_{E,m}$ defined in this way are compatible in the choice of m under the natural transition maps $\mathrm{Aut}(E[m_1]) \longrightarrow \mathrm{Aut}(E[m_2])$ for $m_2 \mid m_1$ and hence result in a representation

$$\rho_E : \mathrm{Gal}(\overline{K}/K) \longrightarrow \varprojlim_m \mathrm{Aut}(E[m]) = \mathrm{GL}_2(\widehat{\mathbf{Z}}).$$

The following theorem was proved in [Ser72].

Theorem 3 (Serre)**.** *If E/K is an elliptic curve that does not have complex multiplication, the image of the morphism $\mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}_2(\widehat{\mathbf{Z}})$ has finite index.*

The techniques utilised by Serre [Ser68, Ser72] are highly original and clever, and rely on subtle properties of ℓ-adic Galois representations that would easily merit an entire mini-course (or several) by themselves.



The work of Serre proves in particular that for any given elliptic curve without CM, the Galois representation on $E[\ell]$ has surjective image for $\ell > C(E)$, for some constant $C(E)$ depending only on the elliptic curve. Serre raises the question whether this constant can be taken independently of the elliptic curve over K. For $K = \mathbf{Q}$ one suspects that $\ell > 37$ should always suffice. This question remains open, though much is known. To solve this question, we might reverse it by picking an open subgroup $H \leq \mathrm{GL}_2(\widehat{\mathbf{Z}})$ and ask for a classification of all elliptic curves E such that the image of ρ_E is contained in H. The work of Mazur [Maz77a, Maz78] effectively solves the cases where H is defined to be maximal at all primes except a single prime ℓ, where the image on the ℓ-adic Tate module is

$$\mathrm{Im}\,(\rho_{E,l^\infty}) \leq \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \leq \mathrm{GL}_2(\mathbf{Z}_\ell), \qquad \mathrm{Im}\,(\rho_{E,l^\infty}) \leq \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \leq \mathrm{GL}_2(\mathbf{Z}_\ell),$$

respectively, which amount to finding all rational points on the modular curves $X_1(\ell)$ and $X_0(\ell)$ respectively. For Serre's uniformity question, we see that whenever the map from $G_{\mathbf{Q}}$ to $\mathrm{Aut}(E[\ell]) = \mathrm{GL}_2(\mathbf{F}_\ell)$ is not surjective, the image of its quotient $\rho_{E,\ell}$ must be contained in a maximal subgroup of $\mathrm{GL}_2(\mathbf{F}_\ell)$ for some prime ℓ. The maximal subgroups of $\mathrm{GL}_2(\mathbf{F}_\ell)$ may be classified, and are as follows:

- Borel subgroups, conjugate to
$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \leq \mathrm{GL}_2(\mathbf{Z}_\ell)$$
As we noted before, the work of Mazur [Maz77a, Maz78] completely classifies the elliptic curves whose Galois image is contained in this subgroup. In other words

- Exceptional subgroups: These are subgroups with projective image A_4, S_4 or A_5, which Serre settles in his original paper [Ser72]. This question turns out to be approachable purely locally at ℓ, and Serre shows that when $\ell > 13$ the curves $X_{S_4}(\ell)$ have no $\mathbf{Q}_\ell$-points, so in particular it has no $\mathbf{Q}$-points. The case $X_{S_4}(13)$ was settled more recently [BDM$^+$21].

- Normalisers of split Cartan subgroups $\mathbf{F}_\ell^\times \times \mathbf{F}_\ell^\times \leq \mathrm{GL}_2(\mathbf{F}_l)$, which are conjugate to
$$\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \bigsqcup \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$$
This case was settled much more recently in the beautiful work of Bilu–Parent [BP11] and Bilu–Parent–Rebolledo [BPR13] using Runge's method, for $\ell > 13$. The case $\ell = 13$ has genus 3 and became known as the *cursed* modular curve. It was settled in [BDM$^+$19].

- Normalisers of non-split Cartan subgroups $\mathbf{F}_{\ell^2}^\times \leq \mathrm{GL}_2(\mathbf{F}_l)$. This case remains very mysterious today, and essentially we only know the rational points on a handful of examples. Historically, the first success came from Heegner [Hee52] and Stark [Sta66], who effectively determined all the integral points on $Y_{\mathrm{ns}}^+(24)$, which is an elliptic curve, to prove the famous class number one problem of Gauss.

This Diophantine interpretation was pointed out retrospectively by Serre [Ser97]. The first ℓ for which the curve does not have genus 0 is $\ell = 11$, and we have

$$X_{\mathrm{ns}}^{+}(11) : y^2 + y = x^3 - x^2 - 7x + 10.$$

The rational points were first determined by Ligozat [Lig77], but do not take anything for granted and solve this problem yourself, using a 2-descent as we do below for a different modular curve of level 11. For $\ell > 11$ very little is known about the set of rational points. The only examples where the set was fully determined are the genus 3 curve $X_{\mathrm{ns}}^{+}(13)$ in [BDM^{+}19] and the genus 6 curve $X_{\mathrm{ns}}^{+}(17)$ in [BDM^{+}21]. The methods rely on the non-abelian Chabauty techniques developed by Kim [Kim05, Kim09, Kim10] and they are at present only equipped to deal with specific examples, relying on explicit equations.

Even after the many results obtained by all these people, many open questions remain. The possible ambitions one can have in this direction are unlimited, and encapsulated in what is typically referred to as *Mazur's Program B*, see for instance [Maz77b].

Program B. *Given a number field K and a subgroup H of $\mathrm{GL}_2(\widehat{\mathbf{Z}}) = \prod_p \mathrm{GL}_2(\mathbf{Z}_p)$, classify all elliptic curves E over K whose associated Galois representation on torsion points maps G_K into $H \leq \mathrm{GL}_2(\widehat{\mathbf{Z}})$.*

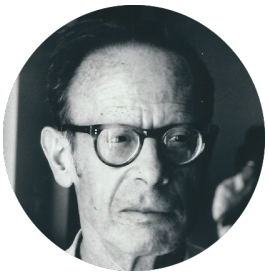
This program may be paraphrased as finding all the rational points over all number fields K on all the modular curves X_H associated to any congruence subgroup H. Needless to say, it is difficult to imagine that Mazur's Program B will ever be able to be fully settled, and clearly we are only at the beginning of this journey. This goes especially when we start to consider also higher dimensional abelian varieties in place of elliptic curves, and it is clear that there is work for several future generations in this program.

1.4 Outline and preprequisites

As all other courses during this meeting, this course is aimed at graduate students who are already familiar with the basic theory of elliptic curves, at the level of Silverman [Sil09]. In addition, the chapter discussing the work of Mazur on torsion of elliptic curves over $\mathbf{Q}$ will assume familiarity with some more advanced algebro-geometric notions such as sheaves and cohomology on the flat site. Students familiar with Milne [Mil80] will have knowledge that far surpasses what we need here, and in any case we recall some of the language that is required in the appendices.

2 Descent and the Mordell–Weil theorem

In this chapter, we quickly review the Mordell–Weil theorem and the method of descent on elliptic curves, which we illustrate in a few explicit examples. All the material here is classical, and is discussed in much more detail in Silverman [Sil09, Chapter VIII, X], which we assume students to be familiar with. The aim is to recap the necessary results, and offer a slightly more technological treatment that foreshadows the algebro-geometric considerations in the next chapter.



2.1 Selmer groups

Let A be an abelian variety defined over a number field K, and let $n \geq 1$ be an arbitrary integer. The short exact sequence of G_K-modules defined by the multiplication by n map

$$0 \longrightarrow A[n] \longrightarrow A \xrightarrow{\cdot n} A \longrightarrow 0 \tag{2.1}$$

defines a long exact sequence in Galois cohomology, from which we extract the following short exact sequence

$$0 \longrightarrow A(K)/nA(K) \longrightarrow \mathrm{H}^1(K, A[n]) \longrightarrow \mathrm{H}^1(K, A)[n] \longrightarrow 0 \tag{2.2}$$

The group $A(K)/nA(K)$ is usually called the *weak* Mordell–Weil group. The first step towards the proof of the Mordell–Weil theorem is to show that the weak Mordell–Weil group is finite. If $A(K)$ is finitely generated, this must clearly be true. The converse is shown using the theory of heights, which will be abundantly studied in the lectures of Silverman at this summer school.

Since the cohomology group $\mathrm{H}^1(K, A[n])$ is infinite, the sequence (2.2) does not yet prove the finiteness of the weak Mordell–Weil group. To this end, we consider also the local variants of (2.2), and obtain the following commutative diagram with exact rows, where the products are taken over all places v of K, and the vertical maps are the product of the corresponding localisation maps.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A(K)/nA(K) & \longrightarrow & \mathrm{H}^1(K, A[n]) & \longrightarrow & \mathrm{H}^1(K, A)[n] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & \overset{\varphi}{\searrow} & \downarrow & & \\
0 & \longrightarrow & \prod_v A(K_v)/nA(K_v) & \longrightarrow & \prod_v \mathrm{H}^1(K_v, A[n]) & \longrightarrow & \prod_v \mathrm{H}^1(K_v, A)[n] & \longrightarrow & 0
\end{array}$$

By the commutativity of this diagram and the exactness of the rows, we see that the image of the weak Mordell–Weil group must lie in the kernel of the map φ. This observation allows us to refine the sequence

(2.2), by defining the *Selmer group* $\mathrm{Sel}_n(A)$ and the *Tate–Shafarevich group* $Ш(A)$ as the kernels of the natural localisation maps

$$\begin{array}{rcccc} \mathrm{Sel}_n(A) & := & \mathrm{Ker}\big(\mathrm{H}^1(K, A[n]) & \longrightarrow & \prod_v \mathrm{H}^1(K_v, A)\big) \\ Ш(A) & := & \mathrm{Ker}\big(\ \mathrm{H}^1(K, A) & \longrightarrow & \prod_v \mathrm{H}^1(K_v, A)\big) \end{array}$$

so that we obtain a short exact sequence

$$0 \longrightarrow A(K)/nA(K) \longrightarrow \mathrm{Sel}_n(A) \longrightarrow Ш(A)[n] \longrightarrow 0. \tag{2.3}$$

2.2 The weak Mordell–Weil theorem

The finiteness of the weak Mordell–Weil group follows from the finiteness of the Selmer group. For this latter fact, many excellent resources exist, see for instance Silverman [Sil09, Chapter VIII] and Milne [Mil06, Chapter IV.3]. Since the target audience is assumed to be acquainted with these proofs, we take this as an opportunity to sketch a proof that relies on algebro-geometric language. This proof will prepare us for the arguments of Mazur to come.

Theorem 4. *Let A be an abelian variety defined over a number field K. For any integer $n \geq 1$, the weak Mordell–Weil group $A(K)/nA(K)$ is finite.*

Proof. Let U be the Zariski open subset of $\mathrm{Spec}(\mathcal{O}_K)$ obtained by inverting the set S consisting of all the primes of bad reduction of A, and the primes dividing n. Then A extends to an abelian variety $\mathscr{A}$ over U, and we have an exact sequence of sheaves on the étale site of U defined by

$$0 \longrightarrow \mathscr{A}[n] \longrightarrow \mathscr{A} \xrightarrow{\cdot n} \mathscr{A} \longrightarrow 0$$

and since $\mathscr{A}(U) = A(K)$ we extract from the long sequence in cohomology that

$$0 \longrightarrow A(K)/nA(K) \longrightarrow \mathrm{H}^1_{\text{ét}}(U, \mathscr{A}[n])$$

and therefore it suffices to show that $\mathrm{H}^1_{\text{ét}}(U, \mathscr{A}[n])$ is finite. By the Hochschild–Serre spectral sequence [Mil80, Theorem 2.20], it suffices to show this after replacing U by a finite étale covering $V \longrightarrow U$. Since the finite flat group scheme $\mathscr{A}[n]$ has invertible order on U, we may take $V = \mathrm{Spec}\,\mathcal{O}_L[1/S]$, where L/K is a finite Galois extension over which

$$\mathscr{A}[n] \simeq (\mathbf{Z}/n\mathbf{Z})^g$$

is constant. We may furthermore assume that $\mathcal{O}_L$ contains the n-th roots of unity, so that also $\mu_n \simeq \mathbf{Z}/n\,\mathbf{Z}$. The short exact Kummer sequence

$$0 \longrightarrow \mu_n \longrightarrow \mathbf{G}_m \xrightarrow{\cdot n} \mathbf{G}_m \longrightarrow 0$$

over V induces a long exact sequence of étale cohomology groups, from which we extract the following short exact sequence:

$$0 \longrightarrow \mathcal{O}_L[1/S]^\times/(\mathcal{O}_L[1/S]^\times)^n \longrightarrow \mathrm{H}^1_{\text{ét}}(V, \mathbf{Z}/n\mathbf{Z}) \longrightarrow \mathrm{Pic}(V)[n] \longrightarrow 0.$$

Note that $\mathrm{H}^1_{\text{ét}}(V, \mathbf{Z}/n\mathbf{Z})$ is flanked by two terms that are finite: the left follows from Dirichlet's unit theorem, whereas the right follows from the finiteness of class groups. □

In the above proof, it is shown that when U is a Zariski open of $\operatorname{Spec}\mathcal{O}_K$ where A has good reduction and n is invertible, then the étale cohomology group $\mathrm{H}^1_{\text{ét}}(U, \mathscr{A}[n])$ is finite. This group consists of classes of the Galois cohomology group

$$\mathrm{H}^1(K, A[n]) \simeq \mathrm{H}^1_{\text{ét}}(\operatorname{Spec}(K), A[n])$$

that are unramified at all finite places of the set S containing the primes of bad reduction of A, and the prime divisors of n. Therefore the Selmer group $\mathrm{Sel}_n(A)$ is contained in it. It is described by the additional finiteness conditions at the bad places in S as explained in § 2.1.

The proof of the weak Mordell–Weil theorem may often be turned into an algorithm for determining the weak Mordell–Weil group, or in any case, the Selmer group. Depending on the chosen example, the setup may be a variation of the above, replacing multiplication by n by another isogeny. For practical reasons, it is typically most convenient to use a 2-isogeny, as explained in Silverman [Sil09, Chapter X]. In general, and certainly for the examples we will consider, one typically does not expect to have any rational 2-isogenies. When $E[2]$ is irreducible, one typically follows the procedure in Silverman [Sil09, Exercise 10.9], which we will now review. In the language used in the above proof of the weak Mordell–Weil theorem, it consists of identifying a *minimal* V, the spectrum of the ring of S-integers in an extension of $\mathbf{Q}$ that trivialises a conveniently chosen submodule $M \subset A[n]$, and describing the classes sufficiently explicitly to be able to disqualify many from lying in the image of a global point, by local considerations.

2.3 The method of 2-descent on elliptic curves

Let E be an elliptic curve over $\mathbf{Q}$ such that the $G_{\mathbf{Q}}$-module $E[2]$ is irreducible. Consider a cubic extension $K/\mathbf{Q}$ such that the G_K-module $E[2]$ is reducible. In other words, we take K to be the number field obtained by adjoining the coordinates of a 2-torsion point $P \in E[2]$. Complete this point P to a basis $\{P, Q\}$ of $E[2]$. Then with respect to this basis, the G_K-module $E[2]$ is of the form

$$E[2] \simeq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

By restriction to G_K and projection to the lower right entry, we now obtain a morphism

$$\varphi : \mathrm{H}^1(\mathbf{Q}, E[2]) \longrightarrow \mathrm{H}^1(K, \mu_2) \simeq K^\times/(K^\times)^2 \tag{2.4}$$

This morphism φ has two important properties (see exercises):

- It has kernel $\operatorname{Ker}(\varphi) = 1$.
- It has image $\operatorname{Im}(\varphi) = \operatorname{Ker}\left(K^\times/(K^\times)^2 \xrightarrow{\mathrm{Nm}} \mathbf{Q}^\times/(\mathbf{Q}^\times)^2\right)$.

Already, these two facts allow us to find a bound, purely in terms of number field arithmetic, on the order of the weak Mordell–Weil group $E(\mathbf{Q})/2E(\mathbf{Q})$, since

$$E(\mathbf{Q})/2E(\mathbf{Q}) \leq \operatorname{Im}(\varphi).$$

Indeed, the classes obtained from global points in the image of φ must be squares at all places not contained in the set S, consisting of all places of K lying above the infinite place, the places of bad reduction of E, and the places dividing 2. Together with the above description of $\operatorname{Im}(\varphi)$, this yields a finite computable subgroup of $K^\times/(K^\times)^2$ containing the weak Mordell–Weil group $E(\mathbf{Q})/2E(\mathbf{Q})$.

The second part of the 2-descent then proceeds to eliminate individual classes of this explicitly computed subgroup of $K^\times/(K^\times)^2$, showing they cannot lie in the image of $E(\mathbf{Q})/2E(\mathbf{Q})$ due to a local obstruction. In order to do this, it is necessary to give an explicit description of the map

$$E(\mathbf{Q}) \longrightarrow \mathrm{H}^1(K, \mu_2) \simeq K^\times/(K^\times)^2.$$

Note that this map is constructed by projection to the line spanned by the point Q, and therefore proceeds by taking the principal homogeneous space of $E[2]$ given by the fibre of $[2] : E \longrightarrow E$ at the point Q, and taking the Weil pairing $e_2(-,-)$ with the K-rational point P. By the explicit description of the Weil pairing [Sil09], we see that the image of a point $R \in E(\mathbf{Q})$ coincides with the class of

$$x(R) - x(P) \in K^\times/(K^\times)^2.$$

This explicit description allows us to further restrict the image of rational points in $\mathrm{Im}(\varphi)$, by local considerations. To digest this method, we illustrate it on the same example that appeared in the introduction.

Example

Consider the elliptic curve E defined over $\mathbf{Q}$ by the affine equation

$$E \ : \ y^2 + y = x^3 - x^2 \tag{2.5}$$

which has conductor $N_E = 11$, and we quickly find that the torsion subgroup of $E(\mathbf{Q})$ is isomorphic to $\mathbf{Z}/5\mathbf{Z}$, generated by the rational point $(0,0)$. We will show that the rank of this elliptic curve is zero.

Step 1: The image of φ. The curve has short Weierstraß equation given by $y^2 = x^3 - 432x + 8208$, and the 2-torsion $E[2]$ is irreducible. It acquires a rational point over the number field K defined by the cubic equation on the right hand side. A simple presentation is given by $K = \mathbf{Q}(\alpha)$ where

$$\alpha^3 - \alpha^2 + \alpha + 1 = 0.$$

This is a cubic number field of signature $(r,s) = (1,1)$ and discriminant $\Delta = -2^2 \cdot 11$. Its ring of integers is the monogenic order $\mathcal{O}_K = \mathbf{Z}[\alpha]$ which has trivial class group $\mathrm{Cl}_K = 1$ and rank one unit group

$$\mathcal{O}_K^\times = \langle -1 \rangle \times \langle \alpha \rangle.$$

Let S be the finite set of places of K consisting of all archimedean places, and all places dividing $2N_E = 22$. More precisely, the following places are contained in S:

- There are two archimedean places and $K \otimes_{\mathbf{Q}} \mathbf{R} \simeq \mathbf{C} \times \mathbf{R}$, and the corresponding local elements modulo squares are represented by

$$\begin{array}{rcl} \mathbf{C}^\times/(\mathbf{C}^\times)^2 & = & 1, \\ \mathbf{R}^\times/(\mathbf{R}^\times)^2 & = & \pm 1. \end{array}$$

- There is a unique 2-adic place and $K \otimes_{\mathbf{Q}} \mathbf{Q}_2 \simeq K_{\mathfrak{p}}$ where $(2) = \mathfrak{p}^3$ in $\mathcal{O}_K$ is totally ramified, and $\mathfrak{p} = (\alpha + 1)$. The corresponding local field modulo squares is represented by

$$K_{\mathfrak{p}}^\times/(K_{\mathfrak{p}}^\times)^2 \quad = \quad \langle -1, 5, \alpha, \alpha - 2, \alpha + 1 \rangle \quad \simeq \quad \mathbf{F}_2^5 \, .$$

- There are two 11-adic places and $K \otimes_{\mathbf{Q}} \mathbf{Q}_{11} \simeq K_{\mathfrak{q}_1} \times K_{\mathfrak{q}_2}$ where $(11) = \mathfrak{q}_1\mathfrak{q}_2^2$ in $\mathcal{O}_K$, and we have $\mathfrak{q}_1 = (2\alpha - 1)$ and $\mathfrak{q}_2 = (\alpha^2 + \alpha - 1)$. The local fields modulo squares are represented by

$$\begin{array}{rcll} K_{\mathfrak{q}_1}^\times/(K_{\mathfrak{q}_1}^\times)^2 & = & \langle 11, -1 \rangle & \simeq \ \mathbf{F}_2^2 \\ K_{\mathfrak{q}_2}^\times/(K_{\mathfrak{q}_2}^\times)^2 & = & \langle \alpha^2 + \alpha - 1, \alpha \rangle & \simeq \ \mathbf{F}_2^2 \end{array}$$

Since K has trivial class group, any class in $K^\times/(K^\times)^2$ that is a square locally at all places $v \notin S$ is represented by an element which is, up to a unit in $\mathcal{O}_K^\times$, a product of the generators of $\mathfrak{p}$, $\mathfrak{q}_1$ and $\mathfrak{q}_2$. In other words, an element in the subgroup

$$\mathbf{F}_2^5 \simeq \langle -1, \alpha, \alpha+1, 2\alpha-1, \alpha^2+\alpha-1\rangle \subset K^\times/(K^\times)^2.$$

The image of the weak Mordell–Weil group is contained in the kernel of the norm map to the subgroup $\mathbf{F}_2^3 \simeq \langle -1, 2, 11\rangle \subset \mathbf{Q}^\times/(\mathbf{Q}^\times)^2$. With respect to these chosen bases, we easily compute that the norm map induces a linear transformation $\mathrm{Nm} : \mathbf{F}_2^5 \longrightarrow \mathbf{F}_2^2$ described by the following matrix representation, where the matrix acts on column vectors:

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \qquad \text{since} \quad \begin{cases} \mathrm{Nm}(-1) = \mathrm{Nm}(\alpha) = -1 \\ \mathrm{Nm}(\alpha+1) = 2 \\ \mathrm{Nm}(2\alpha-1) = \mathrm{Nm}(\alpha^2+\alpha-1) = -11 \end{cases}$$

We see that the kernel of this matrix is of rank two spanned by the column vectors $(1,1,0,0,0)^\intercal$ and $(0,0,0,1,1)^\intercal$. We may therefore conclude that the image of the global points $E(\mathbf{Q})$ is contained in the rank 2 submodule

$$\langle -\alpha, 3\alpha^2 - 5\alpha - 1\rangle \subset K^\times/(K^\times)^2. \tag{2.6}$$

Step 2: Local obstructions. The upper bound obtained above is not sharp enough to conclude that the rank of E is zero. We will now use the explicit description of the Weil pairing and find local obstructions at primes in S to exclude classes of (2.6) as possible elements of the image of a global point. Consider the short Weierstraß model for E given by

$$E \,:\, y^2 = x^3 - 432x + 8208$$

then $E[2]$ has a unique non-trivial K-rational point

$$P = (x, y) = (-18\alpha^2 + 18\alpha - 12, 0)$$

and the image of a rational point $R = (x, y) \in E(\mathbf{Q})$ is given by the class of the element $x - x(P) \in K^\times/(K^\times)^2$. The subgroup (2.6) has three non-trivial elements, each of which we can consider in turn. For instance, the group $E(\mathbf{Q}_2)/2E(\mathbf{Q}_2)$ is cyclic of order two, generated by the class of

$$(x, y) = (1, \sqrt{7777}) \in E(\mathbf{Q}_2)$$

which maps to the class of

$$13 - 18\alpha + 18\alpha^2 \equiv 3\alpha^2 - 5\alpha - 1 \qquad \bmod (K_\mathfrak{p}^\times)^2.$$

We conclude that in the rank 2 submodule (2.6), the non-trivial classes $-\alpha$ and $-\alpha(3\alpha^2 - 5\alpha - 1)$ are not contained in the image of a global point. A similar argument shows that the remaining non-trivial class has an 11-adic obstruction to coming from a global point. We conclude that $E(\mathbf{Q})/2E(\mathbf{Q}) = 1$ and hence

$$E(\mathbf{Q}) \simeq \mathbf{Z}/5\mathbf{Z}\,.$$

2.4 Modular curves

The elliptic curve whose Mordell–Weil group we just determined is one of special significance. It is a model of the modular curve $X_1(11)$, and the determination of the rational points implies that there are no elliptic

curves over $\mathbf{Q}$ with a rational point of order 11. To explain why, we briefly review some important properties of modular curves, which will be used later.

The (affine) modular curves $Y_0(N)$ and $Y_1(N)$ are moduli spaces for isomorphism classes of elliptic curves E endowed with the following additional structures

$$\begin{array}{lcll} Y_0(N) & : & (E, H) & H \text{ is a cyclic subgroup order } N, \\ Y_1(N) & : & (E, P) & P \text{ is a point order } N. \end{array}$$

They have natural compactifications by a finite set of cusps, indexed by the corresponding level structures on the Tate curve $\mathrm{Tate}(q)/\,\mathbf{Z}(\!(q)\!)$. Concretely, the N-torsion submodule is spanned by elements ζ_N and $q^{1/N}$, and the action of the automorphism group on $E[N]$ is generated by $\zeta_N \mapsto \zeta_N^{-1}$ and $q^{1/N} \mapsto \zeta_N^a q^{\pm 1/N}$. This is explained in detail in [DI995], and perhaps best illustrated on an example.

Example. As in Silverman [Sil09, Exercise VIII.8.12], one shows that any elliptic curve E over a $\mathbf{Q}$-algebra with a rational point P of order 5 can be put in the form

$$E_a : y^2 + (1-a)xy - ay = x^3 - ax^2$$

for some value of a. This curve has discriminant $\Delta = a^5(a^2 - 11a - 1)$. The curve $X_1(5)$ has genus 0 and the cusps are given by the orbits of the points $\zeta_5^a q^{b/5}$ of order 5 under the automorphism group. Concretely, we find the following orbits, grouped by distinct colours.

(a,b)	0	1	2	3	4
0		●	●	●	●
1	●	●	●	●	●
2	●	●	●	●	●
3	●	●	●	●	●
4	●	●	●	●	●

There are hence 4 cusps on $X_1(5)$, of which two (● and ●) are rational over $\mathbf{Q}$, and two (● and ●) are rational over $\mathbf{Q}(\zeta_5)^+ = \mathbf{Q}(\sqrt{5})$, the maximal real subfield of the cyclotomic field $\mathbf{Q}(\zeta_5)$.

Increasing the level structure, one may prove (see exercises) that the modular curve $X_1(11)$ is of genus 1 and has a familiar looking minimal Weierstraß model over $\mathbf{Q}$, given by

$$X_1(11) : y^2 + y = x^3 - x^2.$$

It has precisely 10 cusps, of which 5 are rational over $\mathbf{Q}$ and 5 are rational over $\mathbf{Q}(\zeta_5)^+$. We now see that the example of 2-descent we treated in the previous section has special significance. We proved there that there are 5 rational points on $X_1(11)$, which are all accounted for by the cusps. As a consequence, we see that we proved the following:

Theorem 5. *There is no elliptic curve $E_{/\,\mathbf{Q}}$ with a rational point of order* 11.

Whereas this is but a modest part of the torsion theorem of Mazur, it may make us bold enough to wonder whether these methods may be extended to modular curves $X_1(\ell)$ for $\ell > 11$ prime. This is precisely what Mazur does, though there are clearly many formidable obstacles to overcome. In the next chapter, we will analyse the structures we encountered in the 2-descent, and see whether there may be a better version of the descent argument that is more amenable to generalisation.

3

Modular curves and flat descent

In this chapter, we turn to the systematic study of torsion points of prime order N on elliptic curves $E_{\mathbf{Q}}$, and will discuss some aspects of the groundbreaking work of Mazur [Maz77a, Maz78].

Theorem 6 (Mazur)**.** *Let $E_{\mathbf{Q}}$ be an elliptic curve. The torsion subgroup $E(\mathbf{Q})_{\mathrm{tors}}$ of its Mordell–Weil group is isomorphic to one of the following groups:*

$$E(\mathbf{Q})_{\mathrm{tors}} \simeq \begin{cases} \mathbf{Z}/n\mathbf{Z} & 1 \leq n \leq 10,\ n = 12 \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2n\mathbf{Z} & 1 \leq n \leq 4 \end{cases}$$

The strategy revolves around a study of the rational points on the modular curve $X_1(N)$ by performing a descent on a suitably chosen[1] isogeny factor A of its Jacobian $J_1(N)$. In a general descent procedure, as reflected in the example in the previous chapter, we discern two key steps:

- Imposing only unramifiedness conditions outside a finite set of bad primes S gives an a priori bound on the Selmer group, which can be represented by explicit classes.
- This bound is sharpened using explicit equations for twists in the Weil–Châtelet group, where classes are excluded from the image of global points using local obstructions at places in S.

An appealing feature of modular Jacobians is that they frequently have a rational point of large order, and they have good reduction outside of N. This makes the a priori bound arising in the first step quite good, though ultimately not good enough. Needless to say, methods involving the Weil–Châtelet group and explicit equations for twists are not suited to further sharpen this bound. This is already the case for modest values of N, and certainly for general N.

To obtain sharper bounds, one may spread out the geometry over $\mathrm{Spec}(\mathbf{Z})$, and work with respect to the more sophisticated *flat* topology. Concretely, Mazur shows the existence of propitious quotients A whose p-torsion is *admissible* for some $p \nmid N$, a stringent condition that assures the Jordan–Hölder factors to be $\mathbf{Z}/p\mathbf{Z}$ or μ_p. The descent formalism applied to the Néron model $\mathscr{A}_{\mathbf{Z}}$ then leads to a short exact sequence

$$1 \longrightarrow A(\mathbf{Q})/pA(\mathbf{Q}) \longrightarrow \mathrm{H}^1_{\mathrm{fl}}(\mathrm{Spec}(\mathbf{Z}), \mathscr{A}[p]) \longrightarrow \mathrm{H}^1_{\mathrm{fl}}(\mathrm{Spec}(\mathbf{Z}), \mathscr{A})[p] \longrightarrow 1$$

The admissibility of the Galois module in the middle term allows Mazur to sufficiently control the corresponding pieces of the cohomology, frequently using Kummer theory through the fact that

$$1 \longrightarrow \mu_n \longrightarrow \mathbf{G}_m \xrightarrow{\cdot^n} \mathbf{G}_m \longrightarrow 1$$

is an exact sequence of sheaves on the flat site (it is not generally right exact in the étale site).

[1] It is the so-called "Eisenstein quotient", whose construction is a key part of the work of Mazur [Maz78].

Goal. It would be impossible to do justice to the beautiful arguments of Mazur [Maz77a] in a mere three hours of lectures. We have therefore settled for the much more modest goal of treating the cases of 11-torsion and 13-torsion, highlighting those aspects that represent important steps in the proof of the general case. These notes may therefore be viewed as an introduction to the subject, and the interested student is referred to a more complete set of lectures by Snowden [Sno13].

3.1 The flat topology

The arguments of Mazur take place in the *flat topology*. Anyone who wants to understand the fine print of these techniques should consult Milne [Mil80]. In these notes, we will take a pedestrian approach to the inherent technicalities, and content ourselves with using the formal cohomological framework, along with one or two black boxes. Treating the cohomological formalism as a given allows one to already appreciate some of the beautiful ideas in the general case.

Motivation. In the previous chapter, we showed that there are no elliptic curves over $\mathbf{Q}$ with a rational point of order 11, using an explicit 2-descent. But how does this approach generalise to find rational points on $X_1(\ell)$ for primes $\ell > 11$? A careful examination of the structures we encountered in the 2-descent makes us desire for an alternative approach that has the following features:

- The 2-descent involved some cubic extension over which we cannot expect good control in general. The general descent argument should involve structures that have 'meaning', in the sense of the moduli problem, so as to generalise to other modular curves.
- The descent argument should yield sharp bounds so as to avoid having to write down explicit equations for twists. Clearly, this will not be a fruitful approach for primes $\ell > 11$, so we will most likely need to engage with what happens at the finite set of bad primes S.

The ideas of Mazur achieve these goals in the following way. The first point is addressed by performing a descent with respect to a canonical class of rational points, which in the case of $X_1(11)$ is accounted for by the rational 5-torsion. The second point is resolved by working with flat cohomology groups, making the cohomological framework interact with the finite set of bad places S. In these notes, we will avoid the additional technical complications that arise at primes of bad reduction, settling for the primes dividing the order of the isogeny. This will be sufficient for the specific examples that we treat here.

The flat topology. Mazur replaces the étale topology by the finer *flat topology* which is better equipped for dealing with group schemes of order p in characteristic p. The flat topology is a Grothendieck topology, where the coverings of a scheme S are given by families of morphisms

$$\{\varphi_i : T_i \longrightarrow S\}$$

where each morphism φ is flat and locally of finite presentation, and their images cover S in the sense that $S = \bigcup_i \varphi_i(T_i)$. This notion of coverings satisfied the axioms of a Grothendieck topology [Mil80, Chapter II.1] and very important theorem of Grothendieck [Mil80, Theorem I.2.17] implies that whenever G is a commutative group scheme over S then the functor defined by

$$T \mapsto \mathrm{Hom}_S(T, G)$$

is a sheaf of abelian groups with respect to the flat topology defined above. This theorem is central for the practical usefulness of the flat site, and it gives a mechanism whereby short exact sequences of commutative group schemes give rise to long exact sequences in flat cohomology via the cohomological framework developed by Grothendieck, see [Mil80, Chapter III].

Kummer theory. We mention one key fact about the flat topology that is used in the descent arguments on the Jacobians of $X_1(11)$ and $X_1(13)$ below. We often need to control cohomology with values in μ_p when analysing the torsion of modular Jacobians. To do this, we may use that the Kummer sequence

$$1 \longrightarrow \mu_n \longrightarrow \mathbf{G}_m \xrightarrow{\cdot^n} \mathbf{G}_m \longrightarrow 1$$

of abelian group schemes over any base scheme S is *exact* in the flat topology. To see why it is surjective, let U be any S-scheme with a global section $u \in \mathrm{Hom}_S(U, G) = \Gamma(U, \mathcal{O}_U^\times)$. Choose an affine Zariski covering of U by open sets $\mathrm{Spec}(A_i)$, and let $u_i \in A_i^\times$ be the restriction of u to this open subset. For each such open set, there is a covering in the flat topology given by

$$\mathrm{Spec}\, A_i[T]/(T^n - u_i) \longrightarrow \mathrm{Spec}\, A_i \tag{3.1}$$

and note that the restriction (= pullback) of u_i to this covering is in the image of the n-th power map, since it is the n-th power of the unit T. This shows that the Kummer sequence is indeed right exact.

Remark. Note that the Kummer sequence is not generally exact in the étale topology. The problem with the above argument is that the covering (3.1) is not a covering in the étale topology. When n is invertible on S, Hensel's lemma for the polynomial $T^n - u_i$ does imply that the covering (3.1) is étale, and therefore the Kummer sequence is exact in such cases. Note that we already used this fact in our discussion of the weak Mordell–Weil theorem, and it was precisely our desire to use this fact that caused us to add the primes dividing n to the finite set S of bad places. Perhaps this strengthens our faith that we may include these bad places, at the cost of working with the formalism of flat cohomology.

An important consequence of the exactness of the Kummer sequence, which we will use several times in the arguments to follow, is that when the base scheme is the spectrum of the ring $\mathcal{O}_S$ of S-integers in a number field K, its first flat cohomology group with coefficients in μ_p can be computed in terms of arithmetic invariants of the ring, as follows:

Lemma 1. *Suppose S is a finite set of primes in a number field K, and n is any integer. Then we have a short exact sequence*

$$1 \longrightarrow \mathcal{O}[1/S]^\times/(\mathcal{O}[1/S]^\times)^n \longrightarrow \mathrm{H}^1_{\mathrm{fl}}(\mathcal{O}[1/S], \mu_n) \longrightarrow \mathrm{Cl}(\mathcal{O}[1/S])[n] \longrightarrow 1.$$

Proof. By the exactness of the Kummer sequence in the flat topology, we obtain a long exact sequence in flat cohomology from which we extract the five-term sequence

$$\mathrm{H}^0_{\mathrm{fl}}(\mathcal{O}[1/S], \mathbf{G}_m) \xrightarrow{(-)^n} \mathrm{H}^0_{\mathrm{fl}}(\mathcal{O}[1/S], \mathbf{G}_m) \longrightarrow \mathrm{H}^1_{\mathrm{fl}}(\mathcal{O}[1/S], \mu_n) \longrightarrow \mathrm{H}^1_{\mathrm{fl}}(\mathcal{O}[1/S], \mathbf{G}_m) \xrightarrow{(-)^n} \mathrm{H}^1_{\mathrm{fl}}(\mathcal{O}[1/S], \mathbf{G}_m)$$

The lemma now follows from the observations that

$$\begin{array}{rcl} \mathrm{H}^0_{\mathrm{fl}}(\mathcal{O}[1/S], \mathbf{G}_m) & = & \mathcal{O}[1/S]^\times \\ \mathrm{H}^1_{\mathrm{fl}}(\mathcal{O}[1/S], \mathbf{G}_m) & = & \mathrm{H}^1_{\text{ét}}(\mathcal{O}[1/S], \mathbf{G}_m) \quad = \quad \mathrm{Pic}(\mathcal{O}[1/S]) \end{array}$$

where the latter equalities follow from the fact that flat cohomology agrees with étale cohomology when valued in the sheaf $\mathbf{G}_m$, and they both compute the Picard group of the base [Mil80, Theorem III.4.9]. The Picard group of a number ring is its class group, consisting of invertible fractional ideals modulo principal ones. This proves the lemma. □

3.2 Torsion points of order 11

We will now treat the example $X_1(11)$ once again, using a descent by 5-isogeny. As overkill as this may be in this example, we use it as an excuse to explore some of the fundamental ideas in Mazur–Tate [MT73], and ultimately Mazur [Maz72, Maz77a, Maz78]. We begin with some preliminary facts about the modular curves $X_0(11)$ and $X_1(11)$ that may be calculated easily, and which will be used in our descent arguments below. Both are elliptic curves defined over $\mathbf{Q}$, and we may find their minimal Weierstraß models:

$$\begin{array}{rcccl} X_0(11) & : & y^2+y & = & x^3-x^2-10x-20 \\ X_1(11) & : & y^2+y & = & x^3-x^2 \end{array} \tag{3.2}$$

The curve $X_0(11)$ has two cusps 0 and ∞, which are both rational. The curve $X_1(11)$ has ten cusps, of which five are rational, and five are defined over $\mathbf{Q}(\zeta_{11})^+$. The primes 5 and 11 play a central role in our descent argument, coming from the torsion and bad reduction respectively, which we investigate now.

Torsion. We begin with an analysis of the Galois properties of the 5-torsion on both of these elliptic curves. Using the explicit Weierstraß equations above, we easily check that

$$\begin{array}{rcccl} X_0(11)(\mathbf{Q})_{\mathrm{tors}} & = & \{0,(5,5),(5,-6),(16,60),(16,-61)\} & \simeq & \mathbf{Z}/5\mathbf{Z} \\ X_1(11)(\mathbf{Q})_{\mathrm{tors}} & = & \{0,(0,0),(0,-1),(1,0),(1,-1)\} & \simeq & \mathbf{Z}/5\mathbf{Z} \end{array}$$

This means we have an injection of the Galois module $\mathbf{Z}/5\,\mathbf{Z}$ into both $X_0(11)[5]$ and $X_1(11)[5]$. The self-duality of the 5-torsion furnished by the Weil pairing shows that the quotient is in both cases isomorphic to μ_5. The classes defined by $X_0[5]$ and $X_1[5]$ in the space of extensions

$$\big[X_0(11)[5]\big],\ \big[X_1(11)[5]\big] \ \in\ \mathrm{Ext}^1(\mu_5, \mathbf{Z}/5\mathbf{Z})$$

can be represented by choosing an $\mathbf{F}_5$-basis for either of these Galois modules whose first element is a rational point. This yields a matrix representation of $G_{\mathbf{Q}}$, and denoting $\chi_5 : G_{\mathbf{Q}} \to \mathbf{F}_5^\times$ for the cyclotomic character defined by the action on the primitive 5-th roots of unity, it is of the form

$$\begin{pmatrix} 1 & * \\ 0 & \chi_5 \end{pmatrix}$$

The nature of the extension class is precisely the nature of the upper triangular part of this matrix, which defines a 1-cocycle of $G_{\mathbf{Q}}$ with values in μ_5^{-1}. Let $L/\mathbf{Q}$ be the field obtained by adjoining all 5-torsion, then we have

$$\mathrm{Gal}(L/\mathbf{Q}) \simeq \mathrm{Gal}(L/\mathbf{Q}(\zeta_5)) \rtimes \mathrm{Gal}(\mathbf{Q}(\zeta_5)/\mathbf{Q}).$$

We see that $\mathrm{Gal}(L/\mathbf{Q}(\zeta_5))$ must be a subgroup of $\mathbf{F}_5$ and $\mathrm{Gal}(\mathbf{Q}(\zeta_5)/\mathbf{Q})$ acts by conjugation through the character χ_5^{-1}. Determining the extension L therefore determines completely the structure of the extension class. Using the Weierstraß equations above, we can easily compute (though please don't do this by hand!) the 5-division polynomials and arrive at the conclusion that

$$\begin{array}{rcll} \mathbf{Q}(X_0(11)[5]) & = & \mathbf{Q}(\zeta_5) & \\ \mathbf{Q}(X_1(11)[5]) & = & \mathbf{Q}(\zeta_5,\alpha), & \text{where } \alpha^5-2\alpha^4+6\alpha^3+2\alpha^2+4\alpha+1 \end{array}$$

so that in particular, the extension defined by $X_0[5] \simeq \mathbf{Z}/5\mathbf{Z} \times \mu_5$ is split, whereas the extension defined by $X_1[5]$ is non-split, and described by the number field above. The pair of isogenies defined by the forgetful map on level structures and its dual have the following kernels

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbf{Z}/5\mathbf{Z} & \longrightarrow & X_1(11) & \longrightarrow & X_0(11) & \longrightarrow & 1 \\ 1 & \longrightarrow & \mu_5 & \longrightarrow & X_0(11) & \longrightarrow & X_1(11) & \longrightarrow & 1 \end{array}$$

Néron models. We will denote the Néron models of $X_0(11)$ and $X_1(11)$ over $\mathbf{Z}$ by $\mathscr{X}_0(11)$ and $\mathscr{X}_1(11)$ respectively. For notational simplicity, we often just write $\mathscr{X}_0$ and $\mathscr{X}_1$, and likewise for their generic fibres. The only prime of bad reduction is 11, where we may use Tate's algorithm to find that the reduction is semistable and has Kodaira types I_5 and I_1 respectively. We may therefore visualise the Néron models over $\mathbf{Z}_{11}$ as in the following picture.

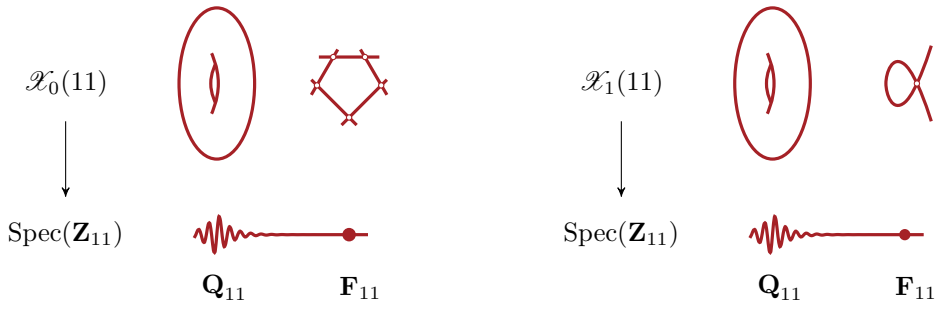


Figure 3.1: The Néron models $\mathscr{X}_0(11)$ and $\mathscr{X}_1(11)$ over $\mathrm{Spec}(\mathbf{Z}_{11})$.

Over $\mathrm{Spec}(\mathbf{Z}[1/11])$ the Néron models are abelian varieties, and the pair of dual 5-isogenies between $X_0(11)$ and $X_1(11)$ extends to an isogeny between the Néron models, whose kernels are therefore finite flat group schemes over $\mathbf{Z}[1/11]$. Their generic fibres (over $\mathbf{Q}$) are isomorphic to the generic fibres of the constant group scheme $\underline{\mathbf{Z}/5\mathbf{Z}}$ and μ_5 respectively. By the classification theorem of Oort–Tate [TO70] this means that the kernels must also be isomorphic to them over $\mathbf{Z}[1/11]$. In other words, over $\mathrm{Spec}(\mathbf{Z}[1/11])$ we have short exact sequences of group schemes

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \underline{\mathbf{Z}/5\mathbf{Z}} & \longrightarrow & \mathscr{X}_1(11) & \longrightarrow & \mathscr{X}_0(11) & \longrightarrow & 1 \\ 1 & \longrightarrow & \mu_5 & \longrightarrow & \mathscr{X}_0(11) & \longrightarrow & \mathscr{X}_1(11) & \longrightarrow & 1. \end{array}$$

Descent by 5-isogeny

The curve $X_1(11)$ comes equipped with a 5-torsion point, which defines the isogeny

$$\phi : X_1(11) \longrightarrow X_0(11)$$

corresponding to the forgetful map on moduli problems that sends the rigidification of the point P of order 5 to the subgroup $\langle P \rangle$ of order 5. This 5-torsion point is 'meaningful', in the sense that it is generated by a cusp and similar torsion will be available on other modular curves, so it feels very natural to make use of it. Here, we will show how to perform a 5-descent to determine the Mordell–Weil group of $X_1(11)$, showing there are no elliptic curves over $\mathbf{Q}$ with a rational point of order 11 (again).

Note that by the defining properties of Néron models, we have $\mathscr{X}_0(\mathbf{Z}[1/11]) = X_0(\mathbf{Q})$ and $\mathscr{X}_1(\mathbf{Z}[1/11]) = X_1(\mathbf{Q})$. Therefore, considering the isogeny ϕ and the associated long exact sequence in cohomology over $\mathbf{Z}[1/11]$, extract the injection

$$X_0(11)(\mathbf{Q})/\phi(X_1(11)(\mathbf{Q})) \hookrightarrow \mathrm{H}^1_{\text{ét}}(\mathrm{Spec}(\mathbf{Z}[1/11]), \mathbf{Z}/5\mathbf{Z}) \simeq \mathbf{F}_5,$$

where the target is isomorphic to $\mathbf{F}_5$ because there is a unique cyclic degree 5 extension of $\mathbf{Q}$ unramified outside 11, namely $\mathbf{Q}(\zeta_{11})^+$. Since we can produce 5 elements in the image, this injection must in fact be

an isomorphism. We therefore find that $X_0(11)(\mathbf{Q})/\phi(X_1(11)(\mathbf{Q})) \simeq \mathbf{Z}/5\mathbf{Z}$ without ever having to write down explicit elements of the Weil–Châtelet group, if such a thing would be possible in the first place.

To deal with the dual isogeny $\hat{\phi} : X_0(11) \longrightarrow X_1(11)$, we face more serious difficulties. Indeed, this time the kernel over $\mathbf{Z}[1/11]$ is μ_5, and we face the étale cohomology group $\mathrm{H}^1_{\text{ét}}(\mathrm{Spec}(\mathbf{Z}[1/11], \mathbf{Z}/5\mathbf{Z})$. This is awkward, since μ_5 is not smooth over $\mathbf{Z}[1/11]$ due to its problematic fibre over the prime ideal (5). To gain control over this group, we note instead that the short exact sequence

$$1 \longrightarrow \mu_5 \longrightarrow \mathscr{X}_0(11) \longrightarrow \mathscr{X}_1(11) \longrightarrow 1$$

defines a perfectly valid sequence of sheaves on the flat site of $\mathrm{Spec}(\mathbf{Z}[1/11])$. The flat site is well-equipped for controlling the cohomology of μ_5, since the Kummer sequence

$$1 \longrightarrow \mu_5 \longrightarrow \mathbf{G}_m \longrightarrow \mathbf{G}_m \longrightarrow 1$$

is an exact sequence of flat sheaves (it is **not** exact on the étale site!). Therefore the long exact sequence, where $\mathrm{H}^1_{\text{fl}}(\mathrm{Spec}(\mathbf{Z}[1/11]), \mathbf{G}_m) = \mathrm{Pic}(\mathrm{Spec}(\mathbf{Z}[1/11])) = 0$, gives us an isomorphism

$$\mathrm{H}^1_{\text{fl}}\big(\mathrm{Spec}(\mathbf{Z}[1/11]), \mu_5\big) \simeq \mathbf{F}_5\,.$$

Wonderful! However, we need one last ingredient, since we are trying to show that $X_1(\mathbf{Q})/\hat{\phi}(X_0(\mathbf{Q}))$ is trivial. This ingredient will come from controlling the image at the final frontier: The prime 11. Indeed, the descent sequence gives us the following commutative diagram

$$\begin{array}{ccccccc}
X_0(\mathbf{Q}) & \longrightarrow & X_1(\mathbf{Q}) & \longrightarrow & \mathrm{H}^1_{\text{fl}}\big(\mathrm{Spec}(\mathbf{Z}[1/11]), \mu_5\big) & \simeq & \mathbf{F}_5 \\
\downarrow & & \downarrow & & \downarrow (**) & & \\
X_0(\mathbf{Q}_{11}) & \xrightarrow{(*)} & X_1(\mathbf{Q}_{11}) & \longrightarrow & \mathrm{H}^1_{\text{fl}}\big(\mathrm{Spec}(\mathbf{Q}_{11}), \mu_5\big) & \simeq & \mathbf{F}_5^2
\end{array}$$

The triviality of the group $X_1(\mathbf{Q})/\hat{\phi}(X_0(\mathbf{Q}))$ would finally follow, if we could show that the map $(*)$ is surjective, and the map $(**)$ is injective. Let us check these in turn.

- Let us check first that $(*)$ is surjective. If we denote M_0 and M_1 to be the kernels of the reduction maps of $\mathscr{X}_0(\mathbf{Z}_{11})$ and $\mathscr{X}_1(\mathbf{Z}_{11})$ modulo 11, then the map $(*)$ fits into the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M_0 & \longrightarrow & \mathscr{X}_0(\mathbf{Z}_{11}) & \longrightarrow & \mathscr{X}_0(\mathbf{F}_{11}) & \longrightarrow & 0 \\
 & & \downarrow \hat{\phi} & & \downarrow (*) & & \downarrow \hat{\phi} & & \\
0 & \longrightarrow & M_1 & \longrightarrow & \mathscr{X}_1(\mathbf{Z}_{11}) & \longrightarrow & \mathscr{X}_1(\mathbf{F}_{11}) & \longrightarrow & 0
\end{array}$$

  Note that to prove that $(*)$ is surjective, it suffices to show that its left and right flanking maps in this commutative diagram are surjective, by the snake lemma. For the left map, we note that $[5] = \phi \circ \hat{\phi}$ is an isomorphism on the pro-11 group M_1, and therefore so is $\hat{\phi}$. For the right map, surjectivity can be checked directly, by observing that it factors through the induced map on minimal Weierstraß models, which can be computed explicitly and shown to have trivial kernel, hence trivial cokernel since the special fibres are both cyclic groups of order 10.

- Finally, we note that the map $(**)$ is identified via the long exact sequence of flat cohomology associated to the Kummer exact sequence with the natural map

$$\pm 11^{\mathbf{Z}} / \pm 11^{5\,\mathbf{Z}} \longrightarrow \mathbf{Q}_{11}^{\times} / (\mathbf{Q}_{11}^{\times})^5.$$

This map is clearly injective, since 11 is not a fifth power in $\mathbf{Q}_{11}^{\times}$.

3.3 Torsion points of order 13

For the modular curve $X_1(11)$ we now proved twice that the set of rational point consist entirely of the 5 rational cusps. The second proof is more amenable to generalisation, though clearly there are many obstacles to overcome. To get us a little closer to the general argument, we will use similar techniques to prove the following theorem, due to Mazur–Tate [MT73].

Theorem 7. *There are no elliptic curves $E_{/\mathbf{Q}}$ with a rational point of order 13.*

To prove this theorem, we will exploit the existence of a rational point of order 19 on the Jacobian $A := J_1(13)$. This was originally found by Ogg [Ogg71] and the announcement of this result was the impetus for the work of Mazur–Tate [MT73], who say the following:

> The possibility that this could be done occurred to us when Ogg passed through our town and mentioned that he had discovered a point of order 19 on the 2-dimensional abelian variety *J*. It seemed (to us and to Swinnerton-Dyer) that if such an abelian variety *J*, which has bad reduction at only one prime, and has a sizeable number of endomorphisms, has a point of order 19, it is not entitled to have any other points.

The modular curve $X_1(13)$

We begin by discussing a number of facts about the arithmetic and geometry of the modular curve $X_1(13)$ and its Jacobian $A := J_1(13)$, for later use in the argument. The curve $X_1(13)$ has genus 2 and a model over $\mathbf{Q}$ given by

$$X_1(13) : y^2 + (x^3 + x + 1)y = x^5 + x^4.$$

It has a total of 12 cusps, six of which are rational over $\mathbf{Q}$, and six of which are defined over $\mathbf{Q}(\zeta_{13})^+$, the maximal real subfield of the cyclotomic field $\mathbf{Q}(\zeta_{13})^+$. The curve has many automorphisms, for instance those induced by the following maps on elliptic curves

$$\begin{array}{lcccll} \gamma_m & : & (E,P) & \longmapsto & (E, mP) & \text{where } m \in (\mathbf{Z}/13\mathbf{Z})^{\times}/\{\pm 1\} \\ \tau_\zeta & : & (E,P) & \longmapsto & (E/\langle P\rangle, Q) & \text{where } \zeta \in \mu_{13}\backslash\{1\} \text{ and } \langle P, \widetilde{Q}\rangle_{\text{Weil}} = \zeta. \end{array}$$

Here, the notation $\widetilde{Q}$ is used for any point on E whose image on $E/\langle P\rangle$ is equal to Q. Note that the condition on the Weil pairing determines $\widetilde{Q}$ up to multiples of P, which makes its image well-defined. We see that the the elements γ_m form a group Γ which is isomorphic to $(\mathbf{Z}/13\mathbf{Z})^{\times}/\{\pm 1\}$ and is generated by the element γ_2 of order 6. The elements τ_ζ are involutions, and we check that

$$\left\{ \begin{array}{rcccl} \tau_\zeta \gamma_m \tau_\zeta & = & \gamma_m^{-1} & = & \gamma_{m^{-1}} \\ \gamma_m \tau_\zeta & = & \tau_{\zeta^m} & & \end{array} \right.$$

so that we exhibited a group of automorphisms

$$\Delta := \Gamma \rtimes C_2 \;\leq\; \mathrm{Aut}_{\overline{\mathbf{Q}}}\, X_1(13)$$

which is dihedral of order 12. In fact, this is the entire automorphism group, though we shall not use this fact. Note that the subgroup of automorphisms Γ is defined over $\mathbf{Q}$, whereas the involutions τ_ζ are defined over $\mathbf{Q}(\zeta_{13})^+$. Explicitly, by the equivariance of the Weil pairing, the action of an element of the Galois group $g \in G_{\mathbf{Q}}$ satisfies

$$\tau_\zeta^g = \tau_{\zeta^g} = \gamma_g \tau_\zeta,$$

where γ_g is the image of g under $G_{\mathbf{Q}} \longrightarrow \mathrm{Gal}(\mathbf{Q}(\zeta_{13})^+/\,\mathbf{Q}) \simeq (\mathbf{Z}\,/13\mathbf{Z})^\times/\{\pm 1\}$.

The structure of the 19-torsion

The argument of Mazur–Tate centers around the structure of the Galois module of 19-torsion points $V := J_1(13)[19]$ on the Jacobian of $X_1(13)$, for which henceforth we shall use the shorthand $A := J_1(13)$. The work of Ogg shows the following

- If we embed the curve $X_1(13)$ using the Abel–Jacobi map attached to the cusp ∞ (or, really, any of the 6 rational cusps) then the 6 rational cusps generate a cyclic subgroup of order 19.
- This accounts for all the torsion in the Jacobian, and

$$X_1(13)(\mathbf{Q}) \cap A(\mathbf{Q})_{\mathrm{tors}} = \{6 \text{ rational cusps}\}.$$

The method that Ogg uses is very interesting in its own right, but a thorough discussion of it would lead us too far. We content ourselves with mentioning that the subgroup of cuspidal divisors is always torsion by a celebrated theorem of Manin–Drinfeld, and that explicit relations between cusps may be found using the theory of *Siegel units*, which are rational functions coming from the theory of modular forms with explicit cuspidal divisors. We will take these facts for granted here, pretending (if you will) that Ogg likewise passed through our town and thoroughly convinced us of the veracity of these facts.

For the descent argument, it will be important to understand more precisely the structure of the Galois module of 19-torsion $V := A[19]$. Note that the ring $\mathrm{End}_{\mathbf{Q}}\, A$ of rational endomorphism contains the quadratic order $\mathbf{Z}[\gamma_2] \simeq \mathbf{Z}[\zeta_6]$ of Eisenstein integers, which has unique factorisation. We have a factorisation $19 = \pi\overline{\pi}$ and may consider the submodules

$$\begin{cases} V_\pi &:= \mathrm{Ker}\,(\pi\,:\,A \longrightarrow A)\,, \\ V_{\overline{\pi}} &:= \mathrm{Ker}\,(\overline{\pi}\,:\,A \longrightarrow A)\,. \end{cases}$$

Since π and $\overline{\pi}$ are coprime, we must have a rational decomposition

$$V = A[\pi\overline{\pi}] = V_\pi \,\oplus\, V_{\overline{\pi}},$$

where both factors are stable under the actions of the Galois group and Γ alike, whereas they are interchanged by any of the involutions τ_ζ. The subgroup $\mathbf{Z}\,/19\mathbf{Z}$ generated by the rational point is stable under the group Γ (for instance, since Γ preserves the set of rational cusps on $X_1(13)$, which generate the rational torsion of A), and therefore it must be contained either in the kernel of π or $\overline{\pi}$. Let us assume, at the cost of interchanging our notation if necessary, that $\mathbf{Z}\,/19\mathbf{Z} \subset V_{\overline{\pi}}$. Finally, define the line

$$\mathscr{L} := \tau_\zeta(\mathbf{Z}\,/19\mathbf{Z})$$

to be the image of the subgroup generated by the rational point of order 19 under the involution τ_ζ. Then $\mathscr{L}$ is contained in V_π and independent of the choice of primitive root of unity $\zeta \in \mu_{13}$ since the involutions attached to two different choice are related by an element of Γ, which preserves the subgroup $\mathbf{Z}\,/19\mathbf{Z}$. Now note that the action of Γ on V_π may be diagonalised into two eigenlines on which the action of the generator

γ_2 is by multiplication by distinct conjugate sixth roots of unity in $\mathbf{F}_{19}^{\times}$. Since the Weil pairing is invariant under simultaneous action of Γ on both arguments, we see that V_π and $V_{\overline{\pi}}$ are self-orthogonal with respect to the Weil pairing, and therefore they are dual to each other. Therefore, the Weil pairing with the rational point of order 19 gives a quotient $V_\pi \to \mu_{19}$. Since the Galois action on this quotient is disjoint from that on $\mathscr{L}$, we must have a short exact sequence

$$1 \longrightarrow \mathscr{L} \longrightarrow V_\pi \longrightarrow \mu_{19} \longrightarrow 1$$

We note for future reference that the Galois module $\mathscr{L}$ becomes trivial over the extension $\mathbf{Q}(\zeta_{13})^+$.

The 19-descent

We are now ready to perform a 19-descent on A. More specifically, the descent will be with respect to the rational isogeny $\pi : A \to A$ of degree 19^2, and follows the same formalism that we employed on the modular curve $X_1(11)$ with respect to the pair of dual 5 isogenies we obtained from the natural forgetful map $X_1(11) \to X_0(11)$.

We begin with an observation: The ring $\mathbf{Z}[\zeta_6] \subset \mathrm{End}_{\mathbf{Q}}\, A$ is a principal ideal domain. Since the Mordell–Weil group is a finitely generated $\mathbf{Z}[\zeta_6]$-module, it suffices to show that $A(\mathbf{Q})/\pi A(\mathbf{Q}) = 0$ to conclude that the rank is zero. To achieve this, consider the Néron model $\mathcal{A}$ of A, then we have a short exact sequence

$$0 \longrightarrow \mathcal{A}[\pi] \longrightarrow \mathcal{A} \xrightarrow{\pi} \mathcal{A} \longrightarrow 0 \qquad \text{over } \mathbf{Z}[1/13].$$

The long exact sequence in flat cohomology over both $\mathbf{Z}[1/13]$ and $\mathbf{Q}_{13}$ then gives rise to a commutative diagram with exact rows, reminiscent of our arguments in the case of 11-torsion, which in this case reads

$$\begin{array}{ccccc} A(\mathbf{Q}) & \longrightarrow & A(\mathbf{Q}) & \longrightarrow & \mathrm{H}^1_{\mathrm{fl}}\big(\mathbf{Z}[1/13], \mathcal{A}[\pi]\big) \\ \downarrow & & \downarrow & & \downarrow (**) \\ A(\mathbf{Q}_{13}) & \xrightarrow{(*)} & A(\mathbf{Q}_{13}) & \longrightarrow & \mathrm{H}^1_{\mathrm{fl}}\big(\mathbf{Q}_{13}, \mathcal{A}[\pi]\big) \end{array}$$

As before, we will argue that $(*)$ is surjective, and $(**)$ is injective, using very similar arguments.

- The surjectivity of $(*)$ follows by a very similar argument. Namely, we use the commutative diagram whose rows are the short exact sequences that furnish the filtration on the local points of the Néron model, given by

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & \mathcal{A}(\mathbf{Z}_{13}) & \longrightarrow & \mathcal{A}(\mathbf{F}_{13}) & \longrightarrow & 0 \\ & & \downarrow \pi & & \downarrow (*) & & \downarrow \pi & & \\ 0 & \longrightarrow & M & \longrightarrow & \mathcal{A}(\mathbf{Z}_{13}) & \longrightarrow & \mathcal{A}(\mathbf{F}_{13}) & \longrightarrow & 0 \end{array}$$

  The map induced on M is a factor of multiplication by 19, which must therefore be an isomorphism on the pro-13 group M. To show that the map $\pi : \mathcal{A}(\mathbf{F}_{13}) \to \mathcal{A}(\mathbf{F}_{13})$ is surjective, it suffices to show that it is injective, since it is an endomorphism of a finite module. By the snake lemma, it therefore suffices that the map $(*)$ itself, namely $\pi : \mathcal{A}(\mathbf{Z}_{13}) \to \mathcal{A}(\mathbf{Z}_{13})$, is *injective*. This is true, since the kernel of this morphism is precisely

$$\mathrm{Ker}\,(A(\mathbf{Q}_{13}) \longrightarrow A(\mathbf{Q}_{13})) = V_\pi^{D_{13}}$$

where $D_{13} \leq G_{\mathbf{Q}}$ is a decomposition group above the prime 13. This is shown because taking D_{13}-invariants yields a short exact sequence of modules

$$1 \longrightarrow \mathscr{L}^{D_{13}} \longrightarrow V_\pi^{D_{13}} \longrightarrow \mu_{19}^{D_{13}}$$

and we can argue that both flanking terms must vanish. Indeed, for $\mathscr{L}^{D_{13}}$ we note that it cannot be isomorphic to $\mathbf{F}_{19}$ since this would imply (by the fact that $\mathscr{L}$ is constant over this extension) that 13 splits completely in $\mathbf{Q}(\zeta_{13})$. Similarly, 13 does not split completely in $\mathbf{Q}(\zeta_{19})$, so that μ_{19} has trivial D_{13}-invariants.

- The injectivity of $(**)$ is slightly more involved, and exploits the filtration of V_π. The module $\mathscr{L}$ can be thought of as a finite flat subgroup of A. We denote its Zariski closure in $\mathcal{A}$ by $\overline{\mathscr{L}}$, whence we obtain a filtration

$$1 \longrightarrow \overline{\mathscr{L}} \longrightarrow \mathcal{A}[\pi] \longrightarrow \mu_{19} \longrightarrow 1 \qquad \text{over } \mathbf{Z}[1/13].$$

To see that the quotient is still isomorphic to μ_{19}, we note that it is determined by its generic fibre (which is μ_{19}) by the classification of Oort–Tate [TO70], and likewise we may conclude from this result that $\overline{\mathscr{L}}$ is constant over $\mathbf{Z}[1/13, \zeta_{13} + \zeta_{13}^{-1}]$. By the Hochschild–Serre spectral sequence, there is an isomorphism

$$\mathrm{H}^1_{\mathrm{fl}}(\mathbf{Z}[1/13], \overline{\mathscr{L}}) = \mathrm{H}^1_{\mathrm{fl}}(\mathbf{Z}[1/13, \zeta_{13}], \mathbf{Z}/19\mathbf{Z})^{(\mathbf{Z}/13\mathbf{Z})^\times}$$

where the right hand side is seen to be trivial, since $\mathbf{Q}(\zeta_{13})$ has no $\mathbf{Z}/19\mathbf{Z}$-extensions that are unramified outside 13. We conclude that there is a commutative diagram

$$\begin{array}{ccc} 1 \longrightarrow \mathrm{H}^1_{\mathrm{fl}}(\mathbf{Z}[1/13], \mathcal{A}[\pi]) & \longrightarrow & \mathrm{H}^1_{\mathrm{fl}}(\mathbf{Z}[1/13], \mu_{19}) \\ \big\downarrow (**) & & \big\downarrow \\ \mathrm{H}^1_{\mathrm{fl}}(\mathbf{Q}_{13}, \mathcal{A}[\pi]) & \longrightarrow & \mathrm{H}^1_{\mathrm{fl}}(\mathbf{Q}_{13}, \mu_{19}) \end{array}$$

whose upper horizontal arrow is an *injection*. To show that $(**)$ is injective, it is therefore enough to show that the right vertical arrow is injective. This follows by essentially the same argument we saw before. Namely, this map has a very concrete description by Kummer theory, namely as the natural map induced by inclusion:

$$\pm 13^{\mathbf{Z}} / \pm 13^{19\,\mathbf{Z}} \longrightarrow \mathbf{Q}_{13}^\times / (\mathbf{Q}_{13}^\times)^{19}.$$

This map is clearly injective, since 13 is not a nineteenth power in $\mathbf{Q}_{13}^\times$.

3.4 Mazur's theorem on torsion

The general theorem of Mazur [Maz78] extends these arguments considerably. Most notably, we can of course not expect the rank of the modular Jacobians $J_1(\ell)$ to be zero when ℓ is a large prime. For instance, $J_0(37)$ is a factor of $J_1(37)$ and it is isogenous to a product of two elliptic curves, one of which has rank 1. Therefore, the best one can hope to find in general is a quotient of genus zero. Mazur finds the so-called *Eisenstein quotient*

$$J_0(\ell) \longrightarrow J_{\mathrm{eis}}$$

which is small enough to have rank zero, but large enough to remember enough about the curve $X_0(\ell)$.

More precisely, for a scheme S we say that a morphism of S-schemes $f : X \longrightarrow Y$ is a formal immersion at $x \in X(S)$ if the induced map on complete local rings

$$f^* : \widehat{\mathcal{O}}_{Y,f(x)} \longrightarrow \widehat{\mathcal{O}}_{X,x}$$

is surjective. Mazur shows that the only rational points on $X_1(\ell)$ are cusps, as long as one finds a rank zero quotient $J_0(p) \longrightarrow A$ for which the map $X_0(p) \longrightarrow A$ induced by the Abel–Jacobi map defined by the cusp ∞ is a formal immersion at ∞. Mazur shows that the Eisenstein quotient $A = J_{\text{eis}}$ satisfies these properties. The hardest part is to show that it has rank zero, which proceeds using a descent argument similar to what we encountered in our small examples, using the *Shimura subgroup* of $J_0(\ell)$, which is the kernel of the map to the Jacobian of $J_1(\ell)$ and is of order

$$n = \text{Numerator}\left(\frac{p-1}{12}\right).$$

It is cyclic of order n and is generated by the rational point $(0) - (\infty)$. This subgroup survives in the Eisenstein quotient, and Mazur performs an n-descent to show the rank is zero. The general arguments are substantially more sophisticated than they were in our small examples, but after our brief foray into small special cases, our hope is that the reader will feel more confident taking on the original paper of Mazur [Maz78].

Merel's theorem on torsion

A natural question to ask is whether the methods of Mazur extend to number fields of higher degree. This was explored by Kamienny and Mazur [Kam92b, Kam92a, KM95], see also Edixhoven [Edi95]. The results remained in first instance limited to particular fields, such as $K/\mathbf{Q}$ quadratic. Finally, it was proved by Merel [Mer96] that the torsion is uniformly bounded in the strongest possible sense:

Theorem 8 (Merel)**.** *The size of the torsion subgroup $E(K)_{\text{tors}}$ is bounded by a constant depending only on the degree of K over $\mathbf{Q}$.*

The key innovation of Merel was to pass to a different quotient of the Jacobian, namely the winding quotient. The intricate flat descent arguments of Mazur are here replaced by the works of Gross–Zagier [GZ85, GZ86] and Kolyvagin [Kol89] which establish a sufficiently large part of the Birch–Swinnerton-Dyer conjecture to show that the rank of the winding quotient is zero. It should be pointed out however that the Eisenstein quotient has by no means left the stage, and there has been renewed recent interest in Eisenstein quotients, see for instance [WWE20, Lec21].

4

Exercises

1. Show that $X_1(11)$ has 5 rational cusps, and is an elliptic curve with minimal Weierstraß equation

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

2. Let E be an elliptic curve over $\mathbf{Q}$ such that the $G_{\mathbf{Q}}$-module $E[2]$ is irreducible. Consider the morphism

$$\varphi \ : \ \mathrm{H}^1(\mathbf{Q}, E[2]) \longrightarrow \mathrm{H}^1(K, \mu_2) \simeq K^\times/(K^\times)^2$$

constructed in (2.4). Show that φ is injective, and has image equal to

$$\mathrm{Im}(\varphi) = \mathrm{Ker}\left(K^\times/(K^\times)^2 \xrightarrow{\mathrm{Nm}} \mathbf{Q}^\times/(\mathbf{Q}^\times)^2\right)$$

Hint: Show that the map φ arises in the long exact sequence in cohomology associated to an appropriately defined short exact sequence of $G_{\mathbf{Q}}$-modules of the form

$$1 \longrightarrow E[2] \longrightarrow \mathrm{Ind}_K^{\mathbf{Q}}(\mu_2) \longrightarrow \mu_2 \longrightarrow 1.$$

3. Determine the Mordell–Weil group of the curve

$$E_N \ : \ y(N - y) = x^3 - x.$$

for the case $N = 6$ appearing in the work of Diophantus. Show that the rank is at least two for all but finitely many integer values of N, and find examples where it is larger than two.

4. Prove that when p is an odd prime, we have that

- the curve $X_0(p)$ has two cusps, both of which are rational,
- the curve $X_1(p)$ has $p - 1$ cusps, of which

$$\begin{array}{l}(p-1)/2 \text{ are rational,}\\ (p-1)/2 \text{ form a full Galois orbit over } \mathbf{Q}(\zeta_p)^+.\end{array}$$

- the curve $X(p)$ has $(p^2 - 1)/2$ cusps, rational over $\mathbf{Q}(\zeta_p)$.

5. Determine all rational solutions to

$$E \ : \ y^2 + xy + y = x^3 - x^2 - x - 14.$$

Bonus: Find all rational elliptic curves with a rational subgroup of order 17.

6. Prove that there are no elliptic curves over $\mathbf{Q}$ with a rational point of order 17.

Hint: First deduce it from the previous exercise. Then prove it using a descent on $X_1(17)$ in the style of Mazur–Tate. You may use that $J_1(17)$ has a rational point of order 73.

Bibliography

[BDM+19] J. Balakrishnan, N. Dogra, S. Müller, J. Tuitman, and J. Vonk. Explicit Chabauty–Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3):885–944, 2019. ↑11, 12.

[BDM+21] J. Balakrishnan, N. Dogra, S. Müller, J. Tuitman, and J. Vonk. Quadratic Chabauty for modular curves. *arXiv:2101.01862*, 2021. ↑11, 12.

[BP11] Y. Bilu and P. Parent. Serre's uniformity problem in the split Cartan case. *Ann. of Math. (2)*, 173(1):569–584, 2011. ↑11.

[BPR13] Y. Bilu, P. Parent, and M. Rebolledo. Rational points on $x_0^+(p^r)$. *Ann. Inst. Fourier*, 63(3):957–984, 2013. ↑11.

[dF59] P. de Fermat. Letter to Pierre de Carcavi. 14 August 1659. ↑5.

[DI995] *Modular Curves and Modular Forms*. Amer. Math. Soc., 1995. ↑18.

[Dio93] Diophantus. *Diophanti Alexandrini Opera omnia: cum Graecis commentariis*, volume 1. Lipsiae : In aedibus B.G. Teubneri, 1893. ↑3.

[DioAD] Diophantus. *Arithmetika*. Alexandria, 3rd Century AD. ↑3.

[DKSS21] M. Derickx, S. Kamienny, W. Stein, and M. Stoll. Torsion points on elliptic curves over number fields of small degree. *arXiv:1707.00364*, 2021. ↑10.

[DN19] M. Derickx and F. Najman. Torsion of elliptic curves over cyclic cubic fields. *Math. Comp.*, 88:2443–2459, 2019. ↑10.

[Edi95] B. Edixhoven. Rational torsion points of elliptic curves over number fields (after Kamienny and Mazur). *Astérisque*, 227:209–227, 1995. ↑10, 29.

[Fer70] S. Fermat. *Diophanti Alexandrini Arithmeticorum Libri Sex: cum commentariis C.G. Bacheti et observationibus D.P. de Fermat.* 1670. ↑5, 6.

[GZ85] B. Gross and D. Zagier. On singular moduli. *J. Reine Angew. Math.*, 355:191–220, 1985. ↑10, 29.

[GZ86] B. Gross and D. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986. ↑10, 29.

[Hee52] K. Heegner. Diophantische Analysis und Modulfunktionen. *Math. Z.*, 59:227–253, 1952. ↑11.

[JKL11] D. Jeon, C. H. Kim, and Y. Lee. Families of elliptic curves over cubic number fields with prescribed torsion subgroups. *Math. Comp.*, 80:579–591, 2011. ↑10.

[Kam92a] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(221–229), 1992. ↑10, 29.

[Kam92b] S. Kamienny. Torsion points on elliptic curves over fields of higher degree. *Int. Math. Res. Not.*, (6):129–133, 1992. ↑10, 29.

[Kim05] M. Kim. The motivic fundamental group of $\mathbf{P}^1\backslash\{0,1,\infty\}$ and the theorem of Siegel. *Invent. Math.*, 161:629–656, 2005. ↑12.

[Kim09] M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. RIMS*, 45:89–133, 2009. ↑12.

[Kim10] M. Kim. Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.*, 23(3):725–747, 2010. ↑12.

[KM88] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.*, 109:125–149, 1988. ↑10.

[KM95] S. Kamienny and B. Mazur. Rational torsion of prime order in elliptic curves over number fields. *Astérisque*, 228(3):81–100, 1995. ↑10, 29.

[Kol89] V. Kolyvagin. Finiteness of e(q) and x(e,q) for a class of Weil curves. *Math. USSR-Izv.*, 32(3):523–541, 1989. ↑10, 29.

[Lec21] E. Lecouturier. Higher Eisenstein elements, higher Eichler formulas and rank of Hecke algebras. *Invent. Math.*, 223:485–595, 2021. ↑10, 29.

[Lig77] G. Ligozat. Courbes modulaires de niveau 11. In J.-P. Serre and D. Zagier, editors, *Modular functions in one variable V*, volume 601 of *Lecture Notes in Math.* Springer-Verlag, Berlin, 1977. ↑12.

[Man69] Yu. I. Manin. The p-torsion of elliptic curves is uniformly bounded. *Izv. Akad. Nauk. CCCP*, 33:459–465, 1969. ↑9.

[Maz72] B. Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18:183–266, 1972. ↑22.

[Maz77a] B. Mazur. Modular curves and the Eisenstein ideal. *IHÉS Publ. Math.*, 47:33–186, 1977. ↑3, 9, 11, 19, 20, 22.

[Maz77b] B. Mazur. Rational points on modular curves. In *Modular functions in one variable V*, volume 601 of *Lecture Notes in Math.*, pages 107–148. Springer-Verlag, 1977. ↑9, 12.

[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978. ↑9, 11, 19, 22, 28, 29.

[Mer96] Loï c Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996. ↑10, 29.

[Mil80] J. Milne. *Étale cohomology*. Princeton University Press, 1980. ↑12, 14, 20, 21.

[Mil06] J.S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006. ↑14.

[Mor22] L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Cambridge Phil. Soc.*, 21:179–192, 1922. ↑5, 8, 9.

[MT73] B. Mazur and J. Tate. Points of order 13 on elliptic curves. *Invent. Math.*, 22:41–49, 1973. ↑22, 25.

[Ogg71] A. Ogg. Rational points on finite order on elliptic curves. *Invent. Math.*, 12:105–111, 1971. ↑25.

[Poi01] H. Poincaré. Sur les propriétés arithmétiques des courbes algébriques. *Journal de mathématiques pures et appliqueés, 5e série*, 7:161–234, 1901. ↑5.

[Ser68] J.-P. Serre. *Abelian ℓ-adic representations and elliptic curves*. Benjamin, New York, 1968. ↑9, 10.

[Ser72] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972. ↑3, 10, 11.

[Ser97] J.-P. Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. ↑12.

[Sil09] J. Silverman. *The arithmetic of elliptic curves, 2nd edition*, volume 106 of *GTM*. Springer-Verlag, 2009. ↑8, 9, 12, 13, 14, 15, 16, 18.

[Sno13] A. Snowden. Course on Mazur's theorem. http://www-personal.umich.edu/ asnowden/teaching/2013/679/, 2013. ↑20.

[Sta66] H. M. Stark. On complex quadratic fields with class number equal to one. *Trans. Amer. Math. Soc.*, 122:112–119, 1966. ↑11.

[TO70] J. Tate and F. Oort. Group schemes of prime order. *Ann. Sci. ENS*, 3(1):1–21, 1970. ↑23, 28.

[Wei29] A. Weil. L'arithmétique sur les courbes algébriques. *Acta Mathematica*, 52(1):281–315, 1929. ↑8.

[WWE20] P. Wake and C. Wang-Erickson. The rank of Mazur's Eisenstein ideal. *Duke Math. J.*, 169(1):31–115, 2020. ↑10, 29.