The average Rank of an
Elliptic Curve

Supervisors:
Prof. Eva Bayer Fluckiger
Swiss Federal Institute of Technology, Lausanne
Prof. Kenneth A. Ribet
University of California, Berkeley.

Vlad Serban
Lausanne - March 10, 2011.
Acknowledgements

First of all, I would like to thank Prof. Eva Bayer for giving me the opportunity to work on this project at UC Berkeley. I also greatly appreciated her counsel throughout this time. Then, I would like to thank Prof. Kenneth Ribet for kindly accepting to guide me through this project and making it an enjoyable and instructive experience for me. Many thanks to both of them for suggesting such an interesting theme! Finally, I would like to extend my gratitude to Jeanine van Order and Dimitar Jetchev for their assistance and helpful comments.
Contents

Acknowledgements 1
1. Introduction 4

Chapter 1. Elliptic curves 5
1. Reduction and Shafarevich’s theorem 5
2. The Mordell-Weil theorem 10
3. Computing $K$-rational points 15

Chapter 2. Abelian varieties 25
1. Preliminaries 25
2. Abelian varieties 28
3. The Faltings height 31
4. The modular height 34
5. Some finiteness results 35

Chapter 3. The average rank of an elliptic curve 37
1. From the 2-Selmer group to binary quartic forms 38
2. Counting integral binary quartic forms with bounded invariants 44
3. The remainder of the proof 49
4. Remarks on the proof 53

Bibliography 57
1. Introduction

As part of his PhD thesis, Manjul Bhargava gave several generalizations of the Gauss composition law for binary quadratic forms and deduced beautiful consequences from this new approach. They appeared in a series of papers ([Bha04a], [Bha04b], [Bha04c] and [Bha08]).

After spending some time studying these results, I tried to understand one of his recent papers ([BS10], in joint work with Arul Shankar). This is an account of the latter.

Their main result is:

**Theorem 1.1.** When averaged over their height, elliptic curves \( E \) defined over \( \mathbb{Q} \) have an average rank of less than 1.5.

Note that before, it wasn’t even known for sure whether the average rank was finite!

This report is structured as follows: the first chapter introduces the standard results and definitions that are required if one wants to talk about the rank of an elliptic curve, mostly based on [Sil09]. In the second chapter, abelian varieties and height functions on them are discussed. This provides a better understanding of elliptic curves and of the heights that are subsequently used to compute their average rank.

A reader familiar with the subject may, however, proceed directly to the final chapter. There, we first establish a correspondence between the 2-Selmer group of an elliptic curve and equivalence classes of integral binary quartic forms. This was already known for a long time, for instance Birch and Swinnerton-Dyer ([BSD63]) used this characterization for computations that led to their famous conjecture. These methods are still used nowadays: see for instance [SC02] or [CFO08].

Then we show how M. Bhargava and A. Shankar count these equivalence classes of forms to give an upper bound for the average rank of an elliptic curve defined over \( \mathbb{Q} \). Finally, the very last section highlights some parts of the proof that weren’t discussed. It also briefly illustrates how the approach that was initiated with M. Bhargava’s thesis factors into the proof of theorem 1.1.
CHAPTER 1

Elliptic curves

In this chapter, we give some results on elliptic curves. In particular, we talk about the Mordell-Weil theorem and define the rank of an elliptic curve. It should be accessible to anyone with basic knowledge of elliptic curves such as covered in the three first chapters of [Sil09]. We follow this book pretty closely, so for convenience most of the notations are also the same.

**Notation.**
- $K$ is a perfect field of characteristic $\text{char} K$.
- $C/K$ denotes a curve defined over $K$ and $C(K)$ denotes the $K$-rational points of $C$.
- For a local field $K$, $R$ denotes the valuation ring, $\mathfrak{M}$ the maximal ideal and $k$ the residue field. We denote the normalized valuation corresponding to a place $v$ by $\text{ord}_v$ and the completion of a valued ring $R$ at a place $v$ $R_v$.
- Similarly, for a number field $K$, $\mathcal{O}$ denotes the ring of integers.
- $\bar{K}$ denotes the algebraic closure of $K$ and $\text{Gal}(L/K)$ denotes the Galois group of an extension $L/K$. The action of Galois is denoted by $\sigma$.
- $K(C)$ denotes the function field of a curve and $\deg \phi$ is the degree of a morphism.
- $\text{Div}(C)$ and $\text{Pic}(C)$ denote the divisor and Picard groups of a curve.

1. Reduction and Shafarevich’s theorem

1.1. Reduction. For this section, let $K$ denote a local field, complete with respect to a normalized discrete valuation $v$. Let $R$ denote the ring of integers of $K$, $\mathfrak{M}$ the maximal ideal of $R$ and let $k = R/\mathfrak{M}$ denote the residue field of $R$. Also, let $\pi$ denote a uniformizer for $R$. Consider an elliptic curve $E$ defined over $K$ and a Weierstrass equation for $E/K$

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$ 

Under the usual change of variables $(x, y) \mapsto (u^{-2} x, u^{-3} y)$, where $u \in K^\times$, the coefficients $a_i$ are mapped to $u^i a_i$. Thus if $u$ contains a large enough power of $\pi$, we get a Weierstrass equation for $E$ with coefficients all in $R$. So the discriminant $\Delta$ also has positive valuation and one can look for an equation with $v(\Delta)$ as small as possible.

**Definition.** Let $E/K$ be an elliptic curve. A minimal equation for $E$ at $v$ is a Weierstrass equation as above, where $v(\Delta)$ is minimized under the condition $a_1, \ldots, a_6 \in R$. We call $v(\Delta)$ the valuation of the minimal discriminant of $E$ at $v$.

**Remark.** Clearly any elliptic curve defined over a local field admits such a minimal equation. Furthermore, a small calculation shows that it is unique up to a change of variables

$$x = u^2 x' + r \text{ and } y = u^3 y' + u^2 s x' + t$$
with \( v(u) = 0 \) and \( r, s, t \in R \).

Now consider the natural reduction map \( R \to k \) and denote it by \( t \to \tilde{t} \). Given a minimal Weierstrass equation for \( E \), we can reduce its coefficients modulo \( \pi \) to obtain a curve \( \tilde{E} \) over \( k \). Let now \( P \in E(K) \). We can find homogeneous coordinates \( (x_0 : y_0 : z_0) \in R \) for \( P \) such that one of them has trivial valuation. Hence \( \tilde{P} \in \tilde{E}(k) \) and we get a reduction map \( E(K) \to \tilde{E}(k) \). We do not know whether \( \tilde{E}(k) \) is non-singular, but we know that its set of non-singular points \( \tilde{E}_{ns}(k) \) forms a group. We then define two subsets of \( E(K) \):

\[
\begin{align*}
E_0(K) &= \{ P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(k) \}; \\
E_1(K) &= \{ P \in E(K) : \tilde{P} = 0 \};
\end{align*}
\]

It follows from the remark above that these sets do not depend on the choice of a minimal Weierstrass equation.

**Proposition 1.1.** There is a short exact sequence of abelian groups

\[
0 \to E_1(K) \to E_0(K) \to \tilde{E}_{ns}(k) \to 0,
\]

where the right-hand map is reduction modulo \( \pi \).

**Proof.** Everything is clear except that the reduction map is a surjective homomorphism. First, observe that the reduction map can be defined on the whole projective space \( \mathbb{P}^2(K) \to \mathbb{P}^2(k) \). Furthermore, lines are mapped to lines. Since group laws on \( E(K) \) as well as \( \tilde{E}_{ns}(k) \) are given by the same process of intersecting lines with the respective curves, this means that the restriction map is a homomorphism. Let now \( \tilde{P} - (\alpha, \beta) \in \tilde{E}_{ns}(k) \) and denote by

\[
f(x, y) - y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0
\]

a minimal Weierstrass equation. Write \( \tilde{f}(x, y) \) for the reduced polynomial. Since \( \tilde{P} \) is non-singular, we can assume for instance \( \frac{df}{dx}(\tilde{P}) \neq 0 \). Choose any \( y_0 \in R \) such that \( \tilde{y}_0 - \beta \). We want to find \( x_0 \in R \) such that \( x_0 - \alpha \) and \( f(x_0, y_0) = 0 \). But since \( \frac{df}{dx}(\alpha, \tilde{y}_0) \neq 0 \), the reduced equation \( f(x, y_0) = 0 \) has \( \alpha \) as a simple root. Thus, by Hensel’s lemma, \( \alpha \) lifts to the desired \( x_0 \in R \).

In the case where \( \tilde{E} \) is non-singular, we see that \( E(K) \) consists of two pieces: \( E_1(K) \) and \( \tilde{E}(k) \). We have a fairly good understanding of the points of an elliptic curve in a residue field (especially a finite field!). The following proposition gives a better description of \( E_1(K) \).

**Proposition 1.2.** Let \( E/K \) be given by a minimal Weierstrass equation, let \( \hat{E}(\mathcal{M}) \) denote the underlying group of the formal group associated to \( E \). Then there is an isomorphism

\[
\hat{E}(\mathcal{M}) \cong E_1(K).
\]

**Proof.** See ([Sil09] 7.3).

We now distinguish 3 types of reduction.

**Definition.** Let \( E/K \) be an elliptic curve and let \( \hat{E} \) be the reduced curve for a minimal Weierstrass equation.

- \( E \) has good (stable) reduction over \( K \) if \( \hat{E} \) is non-singular.
- \( E \) has multiplicative (semi-stable) reduction over \( K \) if \( \hat{E} \) has a node.
- \( E \) has additive (unstable) reduction over \( K \) if \( \hat{E} \) has a cusp.

There is have the following characterisation:
Proposition 1.3. Let $E/K$ be given by a minimal Weierstrass equation
\[ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \]
and write $e = (a_1^2 + 4a_2)^2 - 48a_4 - 24a_1a_3$.

- $E$ has good reduction if and only if $e(\Delta) = 0$.
- $E$ has multiplicative reduction if and only if $e(\Delta) > 0$ and $e(c) = 0$. In this case, $\bar{E}_{ns}(\kappa) \cong \kappa^\times$.
- $E$ has additive reduction if and only if $e(\Delta) > 0$ and $e(c) > 0$. In this case, $\bar{E}_{ns}(\kappa) \cong \kappa^\times$.

The proof of this proposition follows from elementary considerations on Weierstrass equations (see [Sil09] 3.1). The following theorem shows how the reduction type varies under field extensions. In particular, it justifies the stable/semi-stable denomination.

Theorem 1.4 (Semi-stable reduction theorem). Let $E/K$ be an elliptic curve.

- The reduction type does not change under unramified extensions $K'/K$.
- Let $K'/K$ be a finite extension. If $E$ has stable or semi-stable reduction over $K$, then it has the same type of reduction over $K'$.
- There exists a finite extension $K'/K$ such that $E$ has stable or semi-stable reduction over $K'$.

If there exists a finite extension $K'/K$ such that $E$ has good reduction over $K'$, we say that $E$ has potential good reduction. Let us examine an example based on the following criterion.

Proposition 1.5. An elliptic curve $E/K$ has good reduction if and only if the inertia group of $K$ acts trivially on the Tate module $T_l(E)$ for some prime $l \neq \text{char}(K)$.

Example. We want to show that if $K$ is a finite extension of $\mathbb{Q}_p$ and if $E/K$ has complex multiplication, then $E$ has potential good reduction. It is enough to find a prime $l \neq p$ such that the kernel of the action of the inertia group $I_v$ on $T_l(E)$ has finite index. Indeed, then $I_v$ acts on $T_l(E)$ through a finite quotient $I_v/J$. By Galois correspondence, the fixed field $K^{I_v}$ is a finite extension of $K^{nr} - K^{1/l}$ such that $K^{I_v} = K^{nr}$ for some finite extension $K'$ of $K$. The inertia group of $K'$ is then equal to $J$ and thus $E$ has good reduction over $K'$ by the previous criterion. Now if $E$ has complex multiplication over $K$, let $l \neq p$ be any prime. We want to show that the fact that $E$ has more endomorphisms forces the action of $G_{K'/K}$ on $T_l(E)$ to be abelian. Since $\text{char} K = 0$, we know that $\text{End}_K(E)$ is an order in a quadratic imaginary field. Now the Galois representation $V$ given by this action is a 2-dimensional $\mathbb{Q}_l$-vector space. But one also has

\[ V \cong \text{End}_K(E) \otimes \mathbb{Q}_l. \]

So the Galois group acts through $\text{End}_K(E)$-automorphisms on $V$, but this is just $GL_2(\text{End}_K(E) \otimes \mathbb{Q}_l)$ which is abelian. Hence the action of Galois factors through $G_{K^{nr}/K}$. The kernel of the action of $G_{K^{nr}/K}$ on $T_l(E)$ is non-trivial and by local class field theory the inertia group of $K^{ab}/K$ acts through a finite quotient (note that it is isomorphic to the unit group of $K$).
1. Elliptic Curves

1.2. The minimal discriminant. We now shift our attention to the global case: let \( K \) denote a number field, let \( M_K \) denote a complete set of inequivalent (non-archimedean) absolute values on \( K \) and let \( \text{ord}_v \) denote the normalized valuation of \( v \in M_K^0 \). We can look at reduction of an elliptic curve \( E/K \) at a place \( v \) by considering \( E \) as a curve over the completion \( K_v \).

Let \( E/K \) be an elliptic curve and denote by \( \Delta_v \) the discriminant of a minimal Weierstrass equation for \( E \) at \( v \in M_K^0 \).

**Definition.** The minimal discriminant of \( E/K \), denoted \( \mathcal{D}_{E/K} \), is the ideal given by

\[
\mathcal{D}_{E/K} = \prod_{v \in M_K^0} p_v^{\text{ord}_v(\Delta_v)},
\]

where \( p_v \) is the prime ideal associated to \( v \).

We want to know under which conditions there exists an equation that is simultaneously minimal for all \( v \in M_K^0 \). Consider any Weierstrass equation for \( E \) with discriminant \( \Delta \). A change of coordinates such that the equation is minimal at a place \( v \) multiplies the discriminant by some 12-th power: \( \Delta = u_v^{12} \Delta_v \) for \( u \in K^\times \). This prompts the definition of the following ideal

\[
\mathfrak{a}_\Delta = \prod_{v \in M_K^0} p_v^{-\text{ord}_v(\Delta_v)},
\]

such that we can rewrite

\[
\mathcal{D} = (\Delta)\mathfrak{a}_\Delta^{12}.
\]

**Lemma 1.6.** The ideal class of \( \mathfrak{a}_\Delta \) in \( K \) is independent of \( \Delta \).

**Proof.** Take another equation for \( E/K \) with discriminant \( \Delta' \). Then write \( \Delta = u^{12} \Delta' \) such that

\[
(\Delta')\mathfrak{a}_\Delta^{12} = \mathcal{D}_{E/K} - (\Delta')[(u)\mathfrak{a}_\Delta]^{12}.
\]

Thus \( \mathfrak{a}_\Delta = (u)\mathfrak{a}_\Delta \). \( \square \)

**Definition.** We write \( \bar{\mathfrak{a}}_{E/K} \) for the ideal class of any \( \mathfrak{a}_\Delta \) and call it the Weierstrass class of \( E/K \).

**Definition.** A global minimal Weierstrass equation for \( E/K \) is a Weierstrass equation with coefficients in the ring of integers \( \mathcal{O}_K \) such that the discriminant verifies

\[
\mathcal{D}_{E/K} = (\Delta).
\]

**Proposition 1.7.** A global minimal Weierstrass equation exists if and only if \( \bar{\mathfrak{a}}_{E/K} \) is the trivial class.

**Proof.** See ([Sil09] 8.8). \( \square \)

In particular, this is true if \( K \) has class number 1.

**Example.** There are already counterexamples for quadratic fields: consider \( \mathbb{Q}(\sqrt{-10}) \). It is known to have class number 2, the class group being generated by \( \mathfrak{p} = (5, \sqrt{-10}) \). Also, consider the elliptic curve given by

\[
E : y^2 = x^3 + 125.
\]

The equation has discriminant \( \Delta = -2^4 3^3 5^6 \). One sufficient condition for minimality at a prime \( v \) is that \( v(\Delta) < 12 \) (by looking at changes of coordinates). Thus the equation is surely minimal for all primes but \( p \), which lies over 5. The change of coordinates

\[
x = (\sqrt{-10})^2 x', \quad y = (\sqrt{-10})^3 y'
\]

would give an equation with discriminant \( \Delta' = u^{12} \Delta_v \).
Reduction and Shafarevich’s Theorem gives a minimal equation with good reduction at \( p \)

\[
(y')^2 - (x')^3 - 2^{-3},
\]

since the discriminant becomes \( \Delta' = 2^{-2}3^3 \). This shows that

\[
\mathcal{D}_{E/K} = (2^43^3)
\]

and thus \( \bar{a}_{E/K} = (p) \).

1.3. Shafarevich’s theorem for elliptic curves. We prove the following theorem:

**Theorem 1.8** (Shafarevich’s theorem). Let \( S \subset M_K \) be a finite set of places containing the archimedean ones. Then up to isomorphism over \( K \), there are only finitely many elliptic curves \( E/K \) having good reduction at all primes outside of \( S \).

Let \( R_S \) denote the ring of \( S \)-integers \( \{ a \in K : v(a) \geq 0 \text{ for } v \in M_K, v \notin S \} \). We use the following result:

**Lemma 1.9.** Let \( S \subset M_K \) be a finite set containing the archimedean places and all places dividing \( 2,3 \). Assume also that \( R_S \) is a principal ideal domain. Then every elliptic curve \( E/K \) admits a Weierstrass equation

\[
y^2 - x^3 + Ax + B
\]

with \( A,B \in R_S \) and with discriminant satisfying

\[
\mathcal{D}_{E/K} R_S - \Delta R_S.
\]

**Proof.** We start with any Weierstrass equation for \( E/K \) of the form

\[
y^2 - x^3 + Ax + B.
\]

Recall that under this form, \( \Delta = -16(4A^3 + 27B^2) \). For each place not in \( S \), choose \( u \in K^\times \) such that the substitution

\[
x = u^2x' \quad \text{and} \quad y = u^3y'
\]

gives a minimal equation at \( v \) and \( v(\mathcal{D}_{E/K}) = v(\Delta) - 12v(u) \) for all such \( v \). Because \( R_S \) is a principal ideal domain, we can find \( u \in K^\times \) such that \( v(u) = v(u_v) \), and this for all \( v \in M_K, v \notin S \). Thus make the substitution

\[
x = u^2x' \quad \text{and} \quad y = u^3y'
\]

to obtain

\[
E : y^2 - x^3 + u^{-1}Ax + u^{-6}B.
\]

The coefficients are in \( R_S \) because the various minimal equations had coefficients with positive valuations. Furthermore, \( v(\mathcal{D}_{E/K}) = v(\Delta') \) for all \( v \in M_K, v \notin S \), and so we have found the right equation. □

**Lemma 1.10.** Let \( E/K \) be an elliptic curve. With the assumptions of the previous lemma,

\[
\{ P \in E(K) : x(P) \in R_S \}
\]

is a finite set, where \( x(P) \) denotes the Weierstrass coordinate function.

**Proof.** This is a consequence of Siegel’s theorem. For details, see ([Sil09] 9.3). □
Proof of the theorem. We may enlarge $S$ without loss of generality. Therefore, assume $S$ contains all primes of $K$ lying over 2, 3 and enlarge $S$ until $R_S$ is a principal ideal domain. We can now use lemma 1.9 to give us an equation

$$E : y^2 = x^3 + Ax + B,$$

with $A, B \in R_S$ and discriminant satisfying $\Delta R_S = \mathcal{D}_{E/K} R_S$. This procedure for any sequence of elliptic curves $E_i/K$ gives $A_i, B_i \in R_S$ and discriminants $\Delta_i \in R_S^\times$. Look at the (finitely many!) subsequences that have same residue class in $R_S^\times/(R_S^\times)^{12}$. A subsequence of discriminants then looks like $\Delta_i = C(D_1)^{12}$ for a constant $C$ and $D_1 \in R_S^\times$. Since the discriminants verify $\Delta_i = -16(4A_i^3 + 27B_i^2)$, we see that the point $(-12A_i/D_1^3, 72B_i/D_1^6)$ lies on the elliptic curve $Y^2 = X^3 + 27C$. Furthermore, the point lies in $R_S$, whence by lemma 1.10 there are only finitely many possibilities for $A_i/D_1^3$ and $B_i/D_1^6$. Finally, if $E_i$ and $E_j$ are such that

$$A_i/D_1^3 - A_j/D_1^3 \text{ and } B_i/D_1^6 - B_j/D_1^6,$$

the two curves are $K$-isomorphic via the change of coordinates

$$x = (D_i/D_j)^2 x', \quad y = (D_i/D_j)^3 y'.$$

We conclude with one of the (many) applications of this theorem.

**Corollary 1.11.** Let $E$ be an elliptic curve defined over $K$. There are only finitely many elliptic curves which are $K$-isogeneous to $E$.

**Proof.** Assume there is a non-zero isogeny $\phi : E \to E'$ defined over $K$. Let also $m$ be prime to $\text{char}(k)$ and $\deg \phi$. Then the induced map on torsion points $E[m] \to E'[m]$ is an isomorphism of $G_{K/K}$-modules and their Tate modules $T_m(E)$ are also isomorphic as $G_{K/K}$-modules. This means by proposition 1.5 that both curves have good reduction at exactly the same non-archimedean places. The result now follows from Shafarevich’s theorem. \(\square\)

2. **The Mordell-Weil theorem**

Let $E$ be an elliptic curve defined over $K$ be a number field, we want to prove that $E(K)$ is finitely generated. This result is known as the Mordell-Weil theorem. We first prove the weak Mordell-Weil theorem, namely that for any integer $m \geq 2$, $E(K)/mE(K)$ is a finite group.

2.1. **The Kummer pairing.** Let $m \geq 2$ be an integer. There is a short exact sequence of $G_{K/K}$-modules

$$0 \to E[m] \to E(K) \xrightarrow{[m]} E(K) \to 0.$$  

Cohomology with coefficients in $G_{K/K}$ yields a long exact sequence

$$0 \to E(K)[m] \to E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta} H^1(G_{K/K}, E[m]) \to H^1(G_{K/K}, E(K)) \to \cdots$$

from which we get a short exact sequence called the Kummer sequence for $E/K$

$$0 \to E(K)/mE(K) \xrightarrow{\delta} H^1(G_{K/K}, E[m]) \to H^1(G_{K/K}, E(K)) \xrightarrow{[m]} 0.$$
Then define $\delta(P)$ to be the class of
\[
c : G_{K/K} \to E[m] \\
\sigma \mapsto Q^\sigma - Q
\]
in $H^1(G_{K/K}, E[m])$. A standard diagram chase then shows that this homomorphism is well defined. Furthermore, the kernel is exactly $mE(K)$. Assume now that all the $m$-torsion points are in $E(K)$. Then the action of $G_{K/K}$ on $E[m]$ is trivial and therefore
\[
H^1(G_{K/K}, E[m]) = \text{Hom}(G_{K/K}, E[m]).
\]

**Definition.** Assume $E[m] \subset E(K)$. The connecting homomorphism $\delta$ defines a pairing
\[
\kappa(\cdot, \cdot) : E(K) \times G_{K/K} \to E[m],
\]
where
\[
\kappa(P, \sigma) = \delta(P)(\sigma).
\]
By definition, the pairing is well-defined, bilinear and its kernel on the left is $mE(K)$. What does the kernel on the right look like?

**Proposition 2.1.** The kernel on the right is $G_{K/L}$, where $L$ is the compositum of all fields $K(Q)$ where $Q$ verifies $[m]Q \in E(K)$.

**Proof.** One inclusion is obvious. Suppose now $\sigma \in G_{K/K}$ and $\kappa(P, \sigma) = 0$ for all $P \in E(K)$. Then for every $Q \in E(K)$ such that $[m]Q \in E(K)$,
\[
Q^\sigma - Q - \kappa([m]Q, \sigma) = 0.
\]
So $\sigma$ fixes any such $Q$, therefore it fixes the compositum of all fields of the form $K(Q)$, which is $L$. Thus $\sigma \in G_{K/L}$.

**Corollary 2.2.** Under the assumption $E[m] \subset E(K)$ and with the notations above, the Kummer pairing induces a perfect bilinear pairing
\[
E(K)/mE(K) \times G_{L/K} \to E[m].
\]
In particular, if the extension $L/K$ is finite, $E(K)/mE(K)$ is a finite group.

**Proof.** This follows immediately from our previous considerations, the fact that $L/K$ is Galois and that the order of $E[m]$ is $m^2$.

**2.2. The weak Mordell-Weil theorem.** To apply the results of the previous section we need to show that we can assume $E[m] \subset E(K)$ without loss of generality. Since $E[m]$ has a finite number of points, the following lemma shows that we can enlarge the base field $K$ enough so that the inclusion holds.

**Lemma 2.3.** Let $L/K$ be a finite Galois extension. If $E(L)/mE(L)$ is finite, then so is $E(K)/mE(K)$.

**Proof.** Let $L/K$ be finite Galois, the following diagram commutes (by naturality), where the lower row is the inflation-restriction exact sequence.

\[
\begin{array}{cccccc}
0 & \rightarrow & \phi & \rightarrow & E(K)/mE(K) & \rightarrow & E(L)/mE(L) \\
& & \downarrow & & \downarrow & & \\
0 & \rightarrow & H^1(G_{L/K}, E[m]) & \rightarrow & H^1(G_{K/K}, E[m]) & \rightarrow & H^1(G_{L/L}, E[m])
\end{array}
\]

Because the two vertical arrows $E(K)/mE(K) \rightarrow H^1(G_{K/K}, E[m])$ and $E(L)/mE(L) \rightarrow H^1(G_{L/L}, E[m])$ are injective (Kummer sequence), by the Snake
lemma $\phi$ injects into the finite group $H^1(G_{L/K}, E[m])$. Thus $\phi$ is finite and so is $E(K)/mE(K)$. 

By corollary 2.2, we have reduced the problem to showing that $L = K[[m]^{-1}E(K)]$ is a finite extension of $K$. The following proposition is very useful for dealing with torsion points:

**Proposition 2.4.** Let $E/K_v$ be an elliptic curve defined over a local field and $m$ prime to char$(k_v)$. If $E$ has good reduction at $v$, then the reduction map

$$E(K_v)[m] \hookrightarrow \tilde{E}(k_v)$$

is injective.

**Proof.** Recall from proposition 1.1 that if $\tilde{E}$ is non-singular, there is an exact sequence

$$0 \to E_1(K_v) \to E(K_v) \to \tilde{E}(k_v) \to 0.$$  

Thus, to show that $E(K_v)[m] \hookrightarrow \tilde{E}(k_v)$, it is enough to see that $E_1(K_v)$ has no $m$-torsion. But we have seen that $E_1(K_v)$ is isomorphic to a formal group $\hat{E}(\mathcal{M})$, and the conclusion follows from a general result on the torsion of formal groups (see [Sil09] 4.3).

We get a better description of $L$:

**Corollary 2.5.** Let $L = K[[m]^{-1}E(K)]$. Let $S \subset M_K$ be a set of places that contains the non-archimedean places where $E$ has bad reduction or $m$ is not a unit, as well as the archimedean places. Then $L/K$ is unramified outside of $S$.

**Proof.** Let $v \in M_K, v \notin S$. Recall that $L$ is the compositum of fields $K(Q)$, where $[m]Q \in E(K)$. It is enough to show that $K(Q)/K$ is unramified at $v$. Let $v' \in M_{K(Q)}$ be a place above $v$. Let $\sigma \in I_{v'/v}$ be in the inertia group of $K(Q)/K$. We have to show that $\sigma$ acts trivially on $Q$. By proposition 2.4, it is enough to show that $Q^v = Q$ is in the kernel of the reduction map

$$E(K(Q))[m] \to \tilde{E}_{v'}(k_{v'})$$

where $k_{v'}$ denotes the residue field of $K(Q)$ at $v'$. But by definition $[m](Q^v - Q) - ([m]Q - [m]Q - [m]Q = 0$ so $Q^v - Q \in E(K(Q))[m]$. Furthermore, since inertia acts trivially on $k_{v'}$, $Q^v - Q$ maps to 0 via the reduction map.

We can now prove the theorem.

**Proof of the weak Mordell-Weil theorem.** We have to prove that $L = K[[m]^{-1}E(K)]$ is a finite extension of $K$. Remark that since $G_{L/K}$ injects into $\text{Hom}(E(K), E[m])$, $L$ is an abelian extension of $K$. Furthermore, $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ has exponent $m$ and thus so does $G_{L/K}$. Kummer theory characterises abelian extensions of exponent $m$, but we first have to adjoin the $m$-th roots of unity to $K$. This is possible, since we have seen that it is enough to show the proposition for a finite extension of $K$. We now show that a maximal abelian extension $M$ of exponent $m$ unramified outside of $S$ as in corollary 2.5 is necessarily finite. Since then $L \subset M$, this concludes the proof. For this purpose, we can without loss of generality increase $S$ since this only increases $M$. Let now $S$ be large enough so that $v(m) = 0$ if $v \notin S$ and that the ring of $S$-integers $R_S$ is a principal ideal domain. Kummer theory says that $M$ is obtained by adjoining $m$-th roots from $K$. Thus $M$ is the biggest subfield of

$$K(\sqrt[m]{a} : a \in K)$$
unramified outside $S$. We have to reduce the set of adjoined roots to make it finite. First of all, remark that it is enough to adjoin roots of each class modulo $(K^\times)^m$.

Secondly, let $v \in M_K, v \notin S$. Then $K_v(\sqrt[m]{a})/K_v$ is unramified if and only if $\text{ord}_v(a) = 0(m)$. Indeed, if $a$ contains no $m$-th powers, the extension is unramified if and only if $v(am) = 0$ (by looking at the discriminant of the extension). Since $v(m) = 0$ by assumption, this is equivalent to $v(a) = 0$. So it is clear that the condition for $a$ in general is $\text{ord}_v(a) = 0(m)$. This leaves:

$$M = K(\sqrt[1/a]{a} : a \in T_S),$$

where $$T_S = \{a \in K^\times/(K^\times)^m : \text{ord}_v(a) = 0(m) \text{ for all } v \notin S\}.$$ To see that $T_S$ is finite, observe that the map

$$R_S^\times \twoheadrightarrow T_S$$

is surjective. Indeed, if $a \in K^\times$, the ideal $aR_S$ is a $m$-th power of an ideal of $R_S$ because $\text{ord}_v(a)$ is a multiple of $m$ and the valuations not in $S$ correspond to the primes in $R_S$. Finally, since $R_S$ is a principal ideal domain, we can write $aR_S = b^mR_S$ for some $b \in K^\times$. Hence there exists $u \in R_S^\times$ that verifies $a = ub^m$, so $u$ maps to $a$. In fact we have shown more, namely that

$$R_S^\times/(R_S^\times)^m \twoheadrightarrow T_S$$

is surjective. By Dirichlet’s unit theorem, $R_S^\times$ is finitely generated. But if $R_S^\times/(R_S^\times)^m$ isn’t finite, this cannot be true (just look at the classification of finitely generated abelian groups). We conclude that $R_S^\times/(R_S^\times)^m$ and $T_S$ are finite. □

2.3. Proof of the Mordell-Weil theorem. The proof that the Mordell-Weil theorem follows from the weak version is a classical one. We just give a brief sketch here. The key is the following result.

**Proposition 2.6.** Let $A$ be an abelian group. Suppose there is a function

$$h : A \rightarrow \mathbb{R}$$

with the following properties:

1. Let $Q \in A$. There is a constant $C_1(Q)$ so that for all $P \in A$,

$$h(P + Q) \leq 2h(P) + C_1(Q).$$

2. There is an integer $m \geq 2$ and a constant $C_2$ so that for all $P \in A$,

$$h(mP) \geq m^2h(P) - C_2.$$

3. For any constant $C_3$,

$$\{P \in A : h(P) \leq C_3\}$$

is a finite set.

Then if for the integer $m$ in (2), $A/mA$ is a finite group, the abelian group $A$ is finitely generated.

The proof can be consulted in ([Sil09] 8.3).
Remark. In particular, the proof shows that a finite set of generators for $A$ is given by
$\{Q_1, \ldots, Q_r\} \cup \{Q \in A : h(Q) \leq 1 + (C_1 + C_2)/2\}$,
where $Q_1, \ldots, Q_r$ are the elements of $A/mA$ and $C_i$ is the maximum of the constants $C_i(-Q_i), 1 \leq i \leq r$. This means in our context that in order to compute $E(K)$, we only need to be able to compute the constants $C_1(Q), C_2$ and the finite set $\{P \in A : h(P) \leq C_3\}$ as well as the finite group $E(K)/mE(K)$ for some $m \geq 2$.

To finalize the proof of the Mordell-Weil theorem, one proceeds as follows:

- One defines a height function on projective space (in this case, one uses the logarithmic height)
  \[ h : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{R}. \]
  We will discuss such a height function in the next chapter.

- Let $E/K$ be an elliptic curve. A non-constant function $f \in K(E)$ gives a surjective morphism
  \[ F : E \to \mathbb{P}^1 \]
  \[ P \mapsto (f(P) : 1) \text{ if } f \text{ is smooth at } P \]
  If $P$ is a pole, we map it to the point at infinity. Then define the height of $E$ relatively to $f$ to be
  \[ h_f(P) = h(F(P)). \]

- Show that for any even, non-constant function $f \in K(E)$, the 3 required properties in 2.6 for $h_f$ hold with $m = 2$, thereby proving the theorem. For this step, the reader may consult \cite{Sil09} 8.6.

Moreover, the constants that arise while performing the last step are effectively computable. This means that, from a computational standpoint, we only have to be able to compute $E(K)/mE(K)$.

### 2.4. Torsion points and rank of an elliptic curve.

Let $K$ be a number field. We have established that
\[ E(K) \cong E_{\text{tors}}(K) \times \mathbb{Z}^r, \]
where the torsion subgroup $E_{\text{tors}}(K)$ is a finite group. The number $r$ is called the rank of an elliptic curve. We give here a few results and conjectures that describe these two objects. Let us first discuss torsion points. Often the quickest way to find the torsion subgroup in practice is to use proposition 2.4 for several places $v$.

We illustrate this procedure over $\mathbb{Q}$:

**Example.** Let $E/\mathbb{Q}$ be the elliptic curve given by
\[ y^2 = x^3 + x. \]
Its discriminant is $\Delta = -64$. So $\tilde{E}$ is non-singular for any prime $p \neq 2$. We now compute $E(\mathbb{F}_p)$ for small primes. If one of these groups is trivial for instance, we know that torsion injects into it, so $E$ would have no rational torsion. We get
\[ E(\mathbb{F}_3) = \{O, (0, 0), (2, 1), (2, 2)\} \text{ and } \]
\[ E(\mathbb{F}_5) = \{O, (0, 0), (2, 0), (3, 0)\}. \]
The geometric description of the group law on $E$ shows that a point has order two if and only if its $y$-coordinate is zero. Thus as groups, $E(\mathbb{F}_3) \cong \mathbb{Z}/4\mathbb{Z}$ and $E(\mathbb{F}_5) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This shows that only the 2-torsion can be non-trivial, since no other torsion group could possibly inject into $E(\mathbb{F}_5)$. But this amounts to finding
Computing \(K\)-rational points

Let \(K\) be a number field and \(E/K\) an elliptic curve. To compute \(E(K)\), we only need to know generators for \(E(K)/mE(K)\), for some \(m \geq 2\). Unfortunately, this is not always possible. To see why this might be, let us re-examine the proof of the Weak Mordell-Weil theorem (section 2.2). We again make the assumption \(E[m] \subseteq E(K)\). Recall that there is a homomorphism

\[ E(K)/mE(K) \to \text{Hom}(G_{K/K}, E[m]). \]

Via the Weyl pairing \(E[m] \times E[m] \to \mu_m\), this defines a pairing

\[ E(K)/mE(K) \times E[m] \to \text{Hom}(G_{K/K}, \mu_m). \]

Moreover, by Hilbert’s theorem 90, there is an isomorphism

\[ K^*/K^{*m} \cong \text{Hom}(G_{K/K}, \mu_m). \]
So finally we get a pairing
\[ \kappa : E(K)/mE(K) \times E[m] \to K^*/K^{\times m} \]
that is non-degenerate on the left. Furthermore, if \( S \) is a set of places as in the proof of 2.2, the image of the pairing lies in a finite subgroup \( K(S,m) \) of \( K^*/K^{\times m} \). Once we fix two generators for the finite group \( E[m] \), one can explicit the pairing.

The problem then amounts to checking for all elements of \( K^p S, m \) whether they can come from an actual rational point of \( E \). This in turn is the same as finding a rational point on a curve. These types of curves are described in the next section.

One is then inclined to check for rational points of these curves over some completion \( K_v \) (for instance using Hensel’s lemma). However, there are curves that have points in every completion, but not in \( K \). We define a group that measures this failure of the Hasse principle. Finally, all of this is made more explicit with some examples in the last section.

### 3.1. Twists and homogeneous spaces.

For this section, \( K \) is an arbitrary perfect field. Let \( C/K \) be a smooth projective curve. Write \( \text{Isom}(C) \) for the isomorphism group of \( C \).

**Definition.** A twist of \( C/K \) is a smooth curve \( C'/K \) which is isomorphic to \( C \) over \( \overline{K} \). The set \( \text{Twist}(C/K) \) is defined as the set of twists modulo \( K \)-isomorphism.

We now interpret a twist in terms of cohomology. Let \( C'/K \) be a twist of \( C \) and let \( \phi : C' \to C \) be an isomorphism. Define a map
\[ G_{K/K} \to \text{Isom}(C) \]
\[ \sigma \mapsto \xi_\sigma = \phi \sigma \phi^{-1} \]
For \( \tau \in G_{K/K} \), we have
\[ \xi_{\sigma \tau} = \phi^{\sigma \tau} \phi^{-1} = (\phi^\sigma \phi^{-1})^\tau (\phi^\sigma \phi^{-1}) = (\xi_\sigma)^\tau. \]
This shows that \( \xi \) is a 1-cocycle.

**Proposition 3.1.** The cohomology class of \( \xi \) in \( H^1(G_{K/K}, \text{Isom}(C)) \) depends only on the \( K \)-isomorphism class of \( C' \). Hence there is a well-defined map
\[ \text{Twist}(C/K) \to H^1(G_{K/K}, \text{Isom}(C)). \]

**Proof.** Let \( C''/K \) be another twist of \( C \), together with a \( K \)-isomorphism \( \theta : C'' \to C' \) and a \( K \)-isomorphism \( \psi : C'' \to C \). We have to show that the cocycles \( \phi^\sigma \phi^{-1} \) and \( \psi^\sigma \psi^{-1} \) are in the same cohomology class. They differ by a coboundary if there exists \( \alpha \in \text{Isom}(C) \) such that
\[ \alpha^\sigma (\phi^\sigma \phi^{-1}) \alpha^{-1} - \psi^\sigma \psi^{-1}. \]
But \( \alpha = \phi \theta \phi^{-1} \) verifies this equality:
\[ \alpha^\sigma (\phi^\sigma \phi^{-1}) \alpha^{-1} - \phi^\sigma \theta^\sigma \psi^{-1}(\phi \theta \psi^{-1})^{-1} \]
\[ = \phi^\sigma \theta^\sigma \phi^{-1} \psi^{-1} - \phi^\sigma \phi^{-1}. \]

\[ \square \]

**Proposition 3.2.** The map
\[ \text{Twist}(C/K) \to H^1(G_{K/K}, \text{Isom}(C)) \]
is a bijection.
PROOF. First we prove injectivity. Let $\phi : C' \to C$ and $\psi : C'' \to C$ be $K$-isomorphisms and suppose they map to the same cocycle. We have to show there is a $K$-isomorphism $\theta : C' \to C''$. We know that there exists $\alpha \in \text{Isom}(C)$ such that $\alpha^\sigma(\phi^\sigma \phi^{-1})\alpha^{-1} = \psi^\sigma \psi^{-1}$.

So we naturally set $\theta = \psi^{-1} \alpha \phi$. It remains to check that for any $\sigma \in G_{K/K}$, $\theta^\sigma = \theta$.

But

\[
\theta^\sigma = (\psi^\sigma)^{-1} \alpha^\sigma \phi^\sigma \\
- (\psi^\sigma)^{-1} \psi^\sigma \psi^{-1} \alpha \phi \\
- \psi^{-1} \alpha \phi = \theta.
\]

We now prove surjectivity. Let $\xi : G_{K/K} \to \text{Isom}(C)$ be a cocycle, we have to exhibit a curve $C'/K$ and an isomorphism $\phi : C' \to C$ with $\xi_\sigma = \phi^\sigma \phi^{-1}$. The idea is to use the equivalence of categories between smooth curves and function fields to define the twist on $\bar{K}(C)$: Recall that $\xi_\sigma : C \to C$ induces a map $\xi_\sigma^* : K(C) \to \bar{K}(C)$. Then take any field $\bar{K}(C)_{\xi}$ together with a $K$-isomorphism $I : \bar{K}(C) \to \bar{K}(C)_{\xi}$ and let the action of $G_{K/K}$ be "twisted" by $\xi$, meaning that:

\[
I(f)^\sigma = I(\xi^* f^\sigma)
\]

for all $\sigma \in G_{K/K}$. Let

\[
\mathcal{F} = \bar{K}(C)_{\xi}^{G_{K/K}}
\]

denote the fixed field. We show that this is the function field of a smooth curve defined over $K$. So we have to show that $\mathcal{F}$ has transcendence degree 1 over $K$ and that $\mathcal{F} \cap \bar{K} = K$. The first result comes from the fact that the $\bar{K}$-vector space $\bar{K}(C)_{\xi}$ has a basis of $G_{K/K}$-invariant vectors, so $\mathcal{F}$ generates $\bar{K}(C)_{\xi}$ as a $K$-vector space and thus $\bar{K} \mathcal{F} = \bar{K}(C)_{\xi}$.

Therefore $\mathcal{F}$ has the same transcendence degree over $K$ as $\bar{K}(C)_{\xi}$. The second result is clear. We assert that the curve $C'/K$ corresponding to the fixed field $\mathcal{F}$ has the desired properties. By definition of $C'$, we have $\bar{K}(C') \cong \bar{K}(C)_{\xi}$ and so $C'$ is a twist of $C$. Let $\phi : C' \to C$ be the $\bar{K}$-isomorphism corresponding to the isomorphism $I = \phi^*$ on function fields. Then for $\sigma \in G_{K/K}$, for all $f \in K(C)$

\[
(\phi^\sigma)^* f^\sigma = (\phi^* f)^\sigma = \phi^* \xi^* f^\sigma = (\xi_\sigma \phi)^* f^\sigma.
\]

So $(\phi^\sigma)^* = (\xi_\sigma \phi)^*$. This means that for the corresponding morphisms of curves, $\phi^\sigma = \xi_\sigma \phi$. So indeed $\phi$ maps to the cocycle $\xi_\sigma$. □

In general, the set $\text{Twist}(C/K)$ is not a group because $\text{Isom}(C)$ is not abelian. The trick is to find a $G_{K/K}$-invariant abelian subgroup of $\text{Isom}(C)$, thus yielding a group structure on some subset of $\text{Twist}(C/K)$. It would be useful to characterize $H^1(G_{K/K}, E)$ for $E/K$ an elliptic curve, so we want to find the corresponding twists.

DEFINITION. Let $E$ be an elliptic curve defined over $K$. A homogeneous space for $E/K$ is a smooth curve $C/K$ together with a morphism $\mu : C \times E \to C$ defined over $K$ such that

1. $\mu(p, O) = p$ for all $p \in C$.
2. $\mu(\mu(p, P), Q) = \mu(p, P + Q)$ for $p \in C$ and $P, Q \in E$.
3. for all $p, q \in C$, there is a unique $P \in E$, denoted $p - q$, satisfying $\mu(p, P) = q$. 

3. COMPUTING $K$-RATIONAL POINTS

17
In other words, $E$ acts on $C$ through $\mu$ and we will denote this action by a + sign.

One may check easily that the new laws $+,-$ have all the right properties.

**Proposition 3.3.** Let $C/K$ be a homogeneous space for $E$ and choose a base-point $p_0 \in C$. Then the map

$\theta : E \to C$

$P \mapsto p_0 + P$

is an isomorphism defined over $K(p_0)$.

**Proof.** By definition of homogeneous spaces, $\theta$ is an isomorphism. Furthermore, if $\sigma \in G_{K/K}$ fixes $p_0$,

$\theta(P)^\sigma - (p_0 + P)^\sigma - p_0 + P^\sigma - \theta(P^\sigma)$.

□

Among others, this shows that a homogeneous space is a twist of $E$.

**Definition.** The Weil-Chatelet group of $E$ over $K$, denoted $WC(E/K)$, consists of the equivalence classes of homogeneous spaces $C/K$, where we identify $C/K$ with $C'/K$ if there is a $K$-isomorphism $\theta : C \to C'$ compatible with the action of $E$:

$\theta(p + P) = \theta(p) + P$ for $p \in C, P \in E$.

There is, as promised, the following result:

**Theorem 3.4.** Let $E$ be an elliptic curve defined over $K$. There is a bijection

$WC(E/K) \to H^1(G_{K/K}, E)$

defined on equivalence classes by

$[C/K] \mapsto [\sigma \mapsto p_0^\sigma - p_0]$

for any choice of $p_0 \in C$.

**Proof.** See ([Sil09] 10.3).

□

Thus, the Weil-Chatelet group indeed inherits a group structure such that this bijection becomes an isomorphism. We call the equivalence class of $E$ in $WC(E/K)$ the trivial class. In particular, the isomorphism above actually makes this class into the identity with respect to the inherited group structure. The arithmetic importance of this group is then shown by the following proposition.

**Proposition 3.5.** Let $C/K$ be a homogeneous space for $E/K$. Then $C$ is trivial in the Weil-Chatelet group if and only if $C(K) \neq \emptyset$.

**Proof.** If $C$ is trivial, then there is an isomorphism $\theta : E \to C$ defined over $K$. Therefore $\theta(O) \in C(K)$. Conversely, assume that $p_0 \in C(K)$. Then we have shown that the map $\theta : E \to C$ defined by

$\theta(P) - p_0 + P$

is an isomorphism defined over $K(p_0) - K$. Finally, we check that

$\theta(P + Q) - p_0 + (P + Q) - (p_0 + P) + Q = \theta(P) + Q$.

□

We conclude this section with a result that states that the Jacobian of a homogeneous space is isomorphic to $E$ over $K$ (see the next chapter for the Jacobian of a curve).
Theorem 3.6. Let $C/K$ be a homogeneous space for an elliptic curve $E/K$. For any point $p_0 \in C$, the map 
\[ \text{Div}^0(C) \to E \]
\[ \sum n_i(p_i) \mapsto \sum [n_i(p_i - p_0)] \]
induces an isomorphism of $G_{K/K}$-modules 
\[ \text{Pic}^0(C) \cong E. \]

3.2. The Selmer and Tate-Shafarevich groups. We define these groups in general for a non-zero isogeny $\phi : E \to E'$, where $E$ and $E'$ are elliptic curves defined over $K$. The case that is of particular interest to us is if $E' = E$ and $\phi = [m]$ for some $m \geq 2$. In the same way as we obtained the Kummer sequence, one gets the following short exact sequence:
\[ 0 \to E'(K)/\phi(E(K)) \to H^1(G_{K/K}, E[\phi]) \to H^1(G_{K/K}, E)[\phi] \to 0. \]

We want to measure the failure of the Hasse principle. Therefore, for each place $v \in M_K$, we consider the action of the decomposition group $G_v \subset G_{K/K}$ on $E(K_v)$, where $K_v$ as usual denotes the completion of $K$ at $v$. This enables us to take $G_v$-cohomology groups and get exact sequences for all $v \in M_K$:
\[ 0 \to E'(K_v)/\phi(E(K_v)) \to H^1(G_v, E[\phi]) \to H^1(G_v, E)[\phi] \to 0. \]

Then fix an extension of $v$ to $\bar{K}$ for each place $v \in M_K$. The inclusion $E(\bar{K}) \subset E(K_v)$ is then canonical, as is $G_v \subset G_{E/\bar{K}}$. They induce natural restriction maps on cohomology, such that the following diagram commutes for all $v \in M_K$:
\[
\begin{array}{ccc}
0 & \to & E'(K)/\phi(E(K)) \\
\downarrow & & \downarrow \\
0 & \to & E'(K_v)/\phi(E(K_v)) \\
\delta & \to & H^1(G_{K/K}, E[\phi]) \\
\downarrow & & \downarrow \\
0 & \to & H^1(G_{K/K}, E)[\phi] \\
\end{array}
\]

By the universal property of the product, we can capture all this information in a single diagram. Also, use theorem 3.4 to rewrite the last column in terms of homogeneous spaces.
\[
\begin{array}{ccc}
0 & \to & E'(K)/\phi(E(K)) \\
\downarrow & & \downarrow \\
0 & \to & E'(K_v)/\phi(E(K_v)) \\
\delta & \to & H^1(G_v, E[\phi]) \\
\downarrow & & \downarrow \\
0 & \to & H^1(G_v, E)[\phi] \\
\end{array}
\]

We can now define a group that measures how many non-trivial homogeneous spaces are everywhere trivial locally. In view of proposition 3.5, this group documents the failure of the Hasse principle for genus 1 curves.

Definition. The Tate-Shafarevich group of an elliptic curve $E/K$ is defined by
\[ \Sha(E/K) = \ker\left[ WC(E/K) \to \prod_{v \in M_K} WC(E/K_v) \right]. \]

Similarly, we set:

Definition. The $\phi$-Selmer group of $E/K$ is defined by
\[ S^\phi(E/K) = \ker\left[ H^1(G_{K/K}, E[\phi]) \to \prod_{v \in M_K} WC(E/K_v) \right]. \]

We get the following result.
Proposition 3.7. Let $E/K$ be an elliptic curve, $m \geq 2$ an integer. There is an exact sequence

$$0 \to E(K)/mE(K) \to S^m(E/K) \to \text{IM}(E/K)[m] \to 0.$$  

Proof. This follows from applying the snake lemma to the following commutative diagram (with exact rows):

$$
\begin{array}{cccccc}
0 & \to & E(K)/mE(K) & \to & H^1(G_{K/K}, E[m]) & \to \text{WC}(E/K)[m] & \to 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & 0 & \to & \prod \text{WC}(E/K_v) & \to \prod \text{WC}(E/K_v) & \to 0.
\end{array}
$$

Corollary 3.8. The Selmer group $S^m(E/K)$ is finite.

Proof. This proof involves essentially the same tools as the proof of the Weak Mordell-Weil theorem. The reader may consult ([Si09] 10.4) for details. □

3.3. Examples of 2-descent over $\mathbb{Q}$. First, we explicit a method for performing two-descent. It can be found in ([Si09] 10.1). Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation

$$y^2 = (x - e_1)(x - e_2)(x - e_3),$$

with $e_i \in \mathbb{Q}$, $1 \leq i \leq 3$. Let $S \subset M_\mathbb{Q}$ be a set of primes containing $|\ |$, $p - 2$ and the primes at which $E$ has bad reduction. Then set

$$\mathbb{Q}(S, 2) = \{b \in \mathbb{Q}^\times/\mathbb{Q}^\times 2 : \text{ord}_p(b) = 0(2) \text{ for all } p \notin S\}.$$

There is an injective homomorphism

$$E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$$

given by

$$P = (x, y) \mapsto \begin{cases} (x - e_1, x - e_2) & x \neq e_1, e_2 \\
((e_1 - e_3)/(e_1 - e_2), e_1 - e_2) & x = e_1 \\
(e_2 - e_1, (e_2 - e_3)/(e_2 - e_1)) & x = e_2 \\
(1, 1) & P = O.\end{cases}$$

If $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ is not in the image of $E(\mathbb{Q})[2]$, then it is in the image of a point $P \in E(\mathbb{Q})/2E(\mathbb{Q})$ if and only if the equations

$$b_1z_1^2 - b_2z_2^2 - e_2 - e_1$$

$$b_1z_1^2 - b_2z_3^2 - e_3 - e_1$$

have a solution $(z_1, z_2, z_3) \in \mathbb{Q}^\times \times \mathbb{Q}^\times \times \mathbb{Q}$. If this is the case, one may take $P = (b_1z_1^2 + e_1, b_1b_2z_1z_2z_3)$. Let us illustrate this with an example.

Example. Consider the elliptic curve

$$E : y^2 = x^3 - x - x(x + 1)(x - 1)$$

over $\mathbb{Q}$. We want to find $E(\mathbb{Q})$. The discriminant is $\Delta = 2^6$. We have $E[2] \subset E_{\text{tors}}(\mathbb{Q})$, and the torsion points are

$$O, (0, 0), (1, 0) \text{ and } (-1, 0).$$

Also, $E$ has good reduction modulo 3 and a small calculation shows that $\#\hat{E}(F_3) = 4$. Hence $E_{\text{tors}}(\mathbb{Q}) = E[2]$. Let now $S = \{2, |\ |\}$. With the notations above, a complete set of representatives for $\mathbb{Q}(S, 2)$ is given by

$$\{\pm 1, \pm 2\}.$$
The torsion points map as follows:

\[ O \mapsto (1, 1) \quad (0, 0) \mapsto (-1, 1) \quad (1, 0) \mapsto (1, 2) \quad (-1, 0) \mapsto (-1, 2). \]

For the remaining 12 pairs \((b_1, b_2)\), we have to check for solutions of the system

\begin{align*}
(1) & \quad b_1z_1^2 - b_2z_2^2 - 1 \\
(2) & \quad b_1z_1^2 - b_1b_2z_3^2 - 1.
\end{align*}

- One immediately sees that if \(b_1, b_2 < 0\) the second equation has no real solutions. Also, if \(b_1 > 0\) and \(b_2 < 0\), the first equation has no real solutions. We have eliminated all but 4 points: \((2, 1), (2, 2), (-2, 1), (-2, 2)\).
- One can use that the map \(E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)\) is a homomorphism. Since \((2, 2) - (2, 1)(1, 2) - (-1, 2)(-2, 1) - (-1, 1)(-2, 2)\)

the points map to each other if multiplied by images of torsion points so it is enough to check if one of them has a rational solution.

- So we see that the problem amounts to checking if the space defined by the equations (say)

\begin{align*}
(3) & \quad 2z_1^2 - z_2^2 - 1 \\
(4) & \quad 2z_1^2 - 2z_3^2 - 1.
\end{align*}

has a rational point.

Note that this example was very simple and that the amount of computation necessary for this method increases drastically with the number of bad primes! Fortunately, there are more refined methods.

We now give an example of a curve for which the Hasse principle fails.

**Example.** Consider the curve over \(\mathbb{Q}\) given by

\[ C : 3X^3 + 4Y^3 + 5Z^3 = 0. \]

Let us first show that it has a point over every completion \(\mathbb{Q}_p\). We use the following version of Hensel’s lemma: Let \(R\) be a complete ring with respect to a discrete valuation \(v\). If \(f(T) \in R[T]\) and \(a_0 \in R\) satisfy

\[ v(f(a_0)) > 2v(f'(a_0)) \]

then the sequence \(\{a_n\} \in R\) defined by

\[ a_{n+1} - a_n = f(a_n)/f'(a_n) \]

converges to an element \(a \in R\) such that \(f(a) = 0\) and

\[ v(a - a_0) \geq v(f(a_0)/f'(a_0)^2) > 0. \]

There is the following corollary: if \(F(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]\) is a polynomial and there exists a point \((a_1, \ldots, a_n) \in R^n\) such that

\[ v(F(a_1, \ldots, a_n)) > 2v((\partial F/\partial X_i)(a_1, \ldots, a_n)) \]

for some \(1 \leq i \leq N\), then \(F\) has a root in \(R^N\). Indeed, let \(F \in R[X_1, \ldots, X_n]\) with

\[ v(F(a_1, \ldots, a_n)) > 2v((\partial F/\partial X_i)(a_1, \ldots, a_n)) \]

for some \(a\). Setting \(f(x) = F(a_1, \ldots, a_{k-1}, x, \ldots, a_n)\) we see that \(f\) verifies the conditions of the lemma and thus there exists \(b \in R\) such that \(F(a_1, \ldots, b, \ldots, a_n) = 0\).

Now for instance \(\partial F/\partial X(X, Y, Z) = 9X^2\) where \(F\) is the homogeneous polynomial giving the curve. Let \(p\) be a prime, and \(k\) an integer large enough so that
C is everywhere locally trivial (of course
Thus a ∈ ℤ_p^3 is the point we were looking for and we apply the corollary to see that
C is everywhere locally trivial (of course C also has a point in ℤ). Let us show that
there is no rational point in C. The curve is a homogeneous space for the elliptic
curve
\[ E : y^3 + y^3 + 60z^3 - 0. \]
Moreover, if C has a rational point, then E has a non-trivial rational point (see [Cas91] 18). It remains to show that E(ℤ) is trivial. For this purpose, it is enough to show that E(ℤ)/2E(ℤ) and E_{tors}(ℤ) are trivial. To see this, we write E under
the form
\[ y^2 - x^3 - 2^3 \cdot 3^5 \cdot 5^2. \]
Let p ≠ 2, 3, 5, whence the reduced curve \( \tilde{E} \) is nonsingular. Also, denote \( \tilde{D} = 2^3 \cdot 3^5 \cdot 5^2 \) mod p. We then get
\[ \hat{E}(ℤ_p) = 1 + p + \sum_{x ∈ ℤ_p} \left( \frac{x^3 - \tilde{D}}{p} \right), \]
using the Legendre symbol. Furthermore, if p = 2(3), the map \( x → x^3 \) is an automorphism of ℤ_p^3, whereby the sum of the Legendre symbols is trivial. So in this case
\[ \hat{E}(ℤ_p) = 1 + p. \]
By looking at the first eligible primes 11 and 17, we get that the order of E_{tors}(ℤ)
divides 6. Moreover, \( 2^3 \cdot 3^5 \cdot 5^2 \) is neither a square nor a cube, so there is no rational 2 or 3-torsion. Hence E_{tors}(ℤ) is trivial. Finally, the proof that E(ℤ)/2E(ℤ)
is trivial is given in ([Cas91] 15).

To conclude, let us give an example where the rank is still unknown.

**Example.** Consider the elliptic curve
\[ E : y^2 = x^3 + px, \]
with p = 5(8). The rank of this elliptic curve is at most 1. A similar calculation as in the previous example shows us that the order of E_{tors}(ℤ) divides 4. Then, because p is not a perfect square, we see that E[2] ⊄ E(ℤ). Also, E(ℤ) has no point of order 4: The only point of order 2 in E(ℤ) is (0, 0) and (0, 0) ⊄ 2E(ℤ). This follows immediately from the duplication formula in ([Sil99] 3.2). So the only remaining possibility is:
\[ E_{tors}(ℤ) = ℤ/2ℤ. \]
Now define an elliptic curve \( E' : y^2 = x^3 - 4px \). Also, let \( \phi : E → E' \) be the isogeny of degree 2 with kernel E_{tors}(ℤ) and denote by \( \hat{\phi} : E' → E \) the dual isogeny. Descent via 2-isogeny (see [Sil99] 10.6.2b) gives
\[ S^\phi(E/ℤ) ≅ ℤ/2ℤ × ℤ/2ℤ, \]
\[ S^{\hat{\phi}}(E'/ℤ) ≅ ℤ/2ℤ. \]
We write \( r_2(A) = s \) if A is an abelian 2-group of order 2^s. Then since
E_{tors}(ℤ) = ℤ/2ℤ, the rank of E is equal to \( r_2(E(ℤ)/2E(ℤ)) - 1 \). There are exact sequences
\[ 0 → E(ℤ)/\phi E'(ℤ) → S^\phi(E/ℤ) → III(E/ℤ)[\hat{\phi}] → 0, \]
\[ 0 → E'(ℤ)/\hat{\phi} E(ℤ) → S^{\hat{\phi}}(E'/ℤ) → III(E'/ℤ)[\phi] → 0. \]
Furthermore, since $\hat{\phi} \circ \phi = [2]$, there is also the exact sequence (from cohomology)\[
0 \to \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q})[2])} \to \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \to \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \to \frac{E(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \to 0.
\]
We piece all these results together and obtain that the rank of $E$ is equal to:\[
2 + r_2(S^0(E/\mathbb{Q})) + r_2(S^0(E'/\mathbb{Q})) - r_2(E'(\mathbb{Q})[\hat{\phi}] / \phi(E(\mathbb{Q})[2])) - r_2(\mathbb{III}(E/\mathbb{Q})[\phi]) - r_2(\mathbb{III}(E'/\mathbb{Q})[\phi]) + 1
- 2 - r_2(E'(\mathbb{Q})[\hat{\phi}] / \phi(E(\mathbb{Q})[2])) - r_2(\mathbb{III}(E/\mathbb{Q})[\phi]) - r_2(\mathbb{III}(E'/\mathbb{Q})[\hat{\phi}]).
\]
Observe that because $E(\mathbb{Q})[2] \in \ker \phi$, one has $r_2(E'(\mathbb{Q})[\hat{\phi}] / \phi(E(\mathbb{Q})[2])) = 1$. Finally, by looking at the 2-ranks in the short exact sequence\[
0 \to \mathbb{III}(E/\mathbb{Q})[\phi] \to \mathbb{III}(E/\mathbb{Q})[2] \to \mathbb{III}(E/\mathbb{Q})[\hat{\phi}] \to 0
\]
we end up with: \[
\text{rank of } E = 1 - r_2(\mathbb{III}(E/\mathbb{Q})[2]).
\]
Determining if the rank of this curve is 0 or 1 is still an open problem, although it is conjectured that the rank is 1. This is related to the congruent number problem and would for instance follow from the Birch-Swinnerton-Dyer conjecture (by looking at the functional equation). See for example [Ste75]. In addition to that, Cassels showed in [Cas62] that there is an alternating, bilinear pairing \[
\mathbb{III}(E/\mathbb{Q}) \times \mathbb{III}(E/\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z},
\]
which kernel the group of divisible elements of $\mathbb{III}(E/\mathbb{Q})$. So if we assume that $\mathbb{III}(E/\mathbb{Q})$ is finite, we get a non-degenerate, bilinear pairing into $\mathbb{Q}/\mathbb{Z}$. But it is also alternating, so the order of $\mathbb{III}(E/\mathbb{Q})$ has to be a perfect square! In particular, $\mathbb{III}(E/\mathbb{Q})[2]$ has order $2^{2k}$ which eliminates the possibility of rank zero.
CHAPTER 2

Abelian varieties

In this chapter, we want to look at higher dimensional analogues of elliptic curves: abelian varieties. In particular, in the same way as height functions are required to deduce the Mordell-Weil theorem from its weak version, heights on abelian varieties play an important role in various finiteness results, some of which we state at the end of the chapter. Throughout this chapter, \( \text{Spec}(A) \) denotes the affine scheme associated to a commutative ring \( A \). We denote a ringed space by \((X, \mathcal{O}_X)\), where \( \mathcal{O}_X \) is the sheaf; the stalk at \( x \in X \) is denoted by \( \mathcal{O}_{X,x} \).

1. Preliminaries

We start with some useful results and definitions.

1.1. Base extension and fibres. Although we will only deal with algebraic varieties, it is useful to give general definitions for schemes. For proofs, see ([Iit82] 1.19-1.22)

**Definition.** Let \( S \) be a scheme. A scheme over \( S \) (or \( S \)-scheme) is a pair \((X, \phi)\), where \( X \) is a scheme and \( \phi : X \to S \) is a morphism. If \((Y, \psi)\) is another scheme over \( S \), a morphism of schemes \( f : X \to Y \) is a morphism of \( S \)-schemes \( f : (X, \phi) \to (Y, \psi) \) if \( \psi \circ f = \phi \).

**Theorem 1.1.** The schemes over \( S \) form a category. Furthermore, the product exists in this category.

We will denote the product of two \( S \)-schemes \( X \) and \( Y \) by \( X \times_S Y \).

**Definition.** Let \( X \) be a scheme over a field \( k \). For any extension of fields \( K/k \), let \( X(K) \) denote the set of \( k \)-morphisms \( \text{Hom}_k(\text{Spec} K, X) \). An element of \( X(K) \) is called a \( K \)-valued point of \( X \).

**Definition.** Let \( X \) and \( Y \) be schemes over \( S \). The product \( X \times_S Y \) comes with a projection \( s : X \times_S Y \to Y \) which makes it into a \( Y \)-scheme. We call it the extension of the base scheme from \( S \) to \( Y \) and denote it \( X_Y \).

Let \( f : X \to Y \) be a morphism and \( y \in Y \). Let \( U \cong \text{Spec}(A) \) be an affine neighborhood of \( y \). Then if \( \mathfrak{p} \) is the prime ideal of \( A \) corresponding to \( y \), there is an isomorphism

\[
\mathcal{O}_{Y,y} \cong A_{\mathfrak{p}},
\]

where \( A_{\mathfrak{p}} \) denotes the localization at \( \mathfrak{p} \). Write \( k(y) \) for the residue field \( A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \). Then the natural homomorphism \( A \to A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \) yields \( i_y : \text{Spec} k(y) \to U \subseteq Y \). This morphism does not depend on the choice of \( U \). Moreover, \( i_y((0)) = y \) so we can identify \( y \) and \( \text{Spec} k(y) \). Now extend the base scheme of \( X \) from \( Y \) to \( \text{Spec} k(y) \) such that the following diagram (with the obvious projections) commutes.

\[
\begin{array}{ccc}
X_y & \xrightarrow{i_y} & X \\
\downarrow & & \downarrow f \\
y & \xrightarrow{i_Y} & Y
\end{array}
\]
Definition. The Spec $k(y)$-scheme $X \times_Y \text{Spec } k(y)$, denoted $X_y$, is called the fiber of the morphism $f$ over $y$.

The following result justifies this denomination:

**Proposition 1.2.** The underlying topological space of $X_y$ is homeomorphic to $f^{-1}(y)$.

Remark. In particular, we will use these definitions for algebraic varieties over a field $K$, which are separated schemes of finite type over $K$, reduced over the algebraic closure $\overline{K}$. Now an affine algebraic variety over a field $K$ is just Spec $A$ for some finitely generated $K$-algebra $A$ such that $A\otimes_K \overline{K}$ is reduced. An algebraic variety over $\overline{K}$ is then a ringed space $(V, \mathcal{O}_V)$ such that there exists an open covering $V = \bigcup U_i$ where $(U_i, \mathcal{O}_V|U_i)$ is an affine algebraic variety over $K$ and is separated (as a scheme). We keep the same notations as for schemes, namely if $V$ is a variety over $K$ and $L/K$ an extension of fields, we write $V(L)$ for the set of points in $L$ and $V_L$ for the variety over $L$ obtained by extension of scalars.

Definition. Let $V$ be an algebraic variety over an algebraic closure $\overline{K}$ of the field $K$. A model of $V$ over $K$ is an algebraic variety $V'$ over $K$ such that there an isomorphism

$$\phi : V \to V'_K.$$ 

### 1.2. Coherent and invertible sheaves

The primary reference here is ([Har77], 2). We first discuss sheaves of modules.

**Definition.** Let $(X, \mathcal{O}_X)$ be a ringed space. A sheaf of $\mathcal{O}_X$-modules (or simply $\mathcal{O}_X$-module) is a sheaf $\mathcal{F}$ on $X$ such that for each open set $U \subseteq X$, the group $\mathcal{F}(U)$ is an $\mathcal{O}_X(U)$-module, and for each inclusion of open sets $V \subseteq U$, the restriction homomorphism $\mathcal{F}(U) \to \mathcal{F}(V)$ is compatible with the module structure.

**Definition.** A morphism $\mathcal{F} \to \mathcal{G}$ of sheaves of $\mathcal{O}_X$-modules is a morphism of sheaves such that the map $\mathcal{F}(U) \to \mathcal{G}(U)$ is a homomorphism of $\mathcal{O}_X(U)$-modules for any open subset $U \subseteq X$.

Note that any kernel, cokernel and image of a morphism of $\mathcal{O}_X$-modules is an $\mathcal{O}_X$-module as well as any direct sum, product or limit of $\mathcal{O}_X$-modules.

**Definition.** Let $\mathcal{F}$ and $\mathcal{G}$ be two $\mathcal{O}_X$-modules. Define their tensor product $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$ to be the sheaf associated to the presheaf

$$U \mapsto \mathcal{F}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{G}(U).$$

**Definition.** An $\mathcal{O}_X$-module $\mathcal{F}$ is free if it is isomorphic to a direct sum of copies of $\mathcal{O}_X$. It is locally free if $X$ can be covered by open sets $U$ for which $\mathcal{F}|_U$ is a free $\mathcal{O}_X|_U$-module. The rank of $\mathcal{F}$ on an open set is defined as the number of copies of the structure sheaf needed.

Remark. If $X$ is connected, the rank of a locally free sheaf is the same everywhere.

**Definition.** An invertible sheaf is a locally free sheaf of rank 1.

Let $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ be a morphism of ringed spaces. Let $\mathcal{F}$ be an $\mathcal{O}_X$-module. Then $f_* \mathcal{F}$ as an $f_* \mathcal{O}_X$-module inherits a natural structure of $\mathcal{O}_Y$-module via the morphism of sheaves of rings $f^* : \mathcal{O}_Y \to f_* \mathcal{O}_X$. It is called the direct image of $\mathcal{F}$ by $f$. Similarly, let $\mathcal{G}$ be a sheaf of $\mathcal{O}_Y$-modules such that $f^{-1} \mathcal{G}$ is an $f^{-1} \mathcal{O}_Y$-module. There is a morphism of sheaves of rings $f^{-1} \mathcal{O}_Y \to \mathcal{O}_X$ such that $f^{-1} \mathcal{O}_Y$ is an $\mathcal{O}_X$-module. Thus define the inverse image of $\mathcal{G}$ by $f$ to be the $\mathcal{O}_X$-module

$$f^* \mathcal{F} = f^{-1} \mathcal{G} \otimes_{f^{-1} \mathcal{O}_Y} \mathcal{O}_X.$$
1. PRELIMINARIES

PROPOSITION 1.3. The pair \( f_* \) and \( f^* \) are adjoint functors such that there is a natural isomorphism of groups

\[
\text{Hom}_{\mathcal{O}_X}(f^* \mathscr{F}, \mathscr{G}) \cong \text{Hom}_{\mathcal{O}_Y}(\mathscr{F}, f_* \mathscr{G}).
\]

Let \( A \) be a ring and \( M \) be an \( A \)-module. We construct a sheaf on \( \text{Spec} \ A \) associated to \( M \) and denote it by \( \tilde{M} \). Let \( M_p \) denote the localization of \( M \) at a prime ideal \( p \) of \( A \). Define \( \tilde{M}_p \) to be the set of functions \( s: U \to \prod_{p \in U} M_p \) such that for \( p \in U \), \( s \) is locally a fraction \( m/f \) with \( m \in M \) and \( f \in A \) and \( s(p) \in M_p \). The obvious restriction maps then make \( \tilde{M} \) into a sheaf. The sheaf \( \tilde{M} \) has the following properties:

**PROPOSITION 1.4.**

1. \( \tilde{M} \) is an \( \mathcal{O}_{\text{Spec} \ A} \)-module;
2. for each \( p \in \text{Spec} \ A \), the stalk of the sheaf \( \tilde{M} \) at \( p \) is isomorphic to the localization \( M_p \);
3. the global section \( \Gamma(\text{Spec} \ A, \tilde{M}) \) equals \( M \).

This construction is functorial and preserves small products and coproducts. Moreover, the functor \( M \mapsto \tilde{M} \) from the category of \( A \)-modules to the category of \( \mathcal{O}_{\text{Spec} \ A} \)-modules is exact and fully faithful. We can now define:

**DEFINITION.** Let \( (X, \mathcal{O}_X) \) be a scheme. A sheaf of \( \mathcal{O}_X \)-modules \( \mathscr{F} \) is quasi-coherent if there is a cover \( X = \bigcup_i \text{Spec} \ A_i \) by open affine subsets such that for each \( i \) there exists an \( A_i \)-module \( M_i \) with \( \mathscr{F}|_{U_i} \cong M_i \). In addition to that, each \( M_i \) can be taken to be a finitely generated \( A_i \)-module, we say that \( \mathscr{F} \) is coherent.

Coherence is a local property. An example of coherent modules are locally free modules of finite rank. We conclude with the following result on coherent sheaves:

**PROPOSITION 1.5.** Let \( f: X \to Y \) be a morphism of schemes. If \( X \) and \( Y \) are noetherian and if \( \mathscr{G} \) is coherent, then \( f^* \mathscr{G} \) is coherent.

1.3. The Picard group of a variety. Let \( X \) be a scheme. First, observe that if \( \mathscr{F} \) and \( \mathscr{G} \) are two \( \mathcal{O}_X \)-modules, we get a presheaf

\[
U \mapsto \text{Hom}_{\mathcal{O}_X}(\mathscr{F}|_U, \mathscr{G}|_U)
\]

which is in fact a sheaf, denoted \( \text{Hom}(\mathscr{F}, \mathscr{G}) \). Let now \( V \) be a variety. The tensor product of two invertible sheaves is again an invertible sheaf and we get a group structure on the set of isomorphism classes of invertible sheaves. The group law is given by the tensor product:

\[
[\mathcal{L}][\mathcal{L}'] := [\mathcal{L} \otimes_{\mathcal{O}_V} \mathcal{L}']
\]

and clearly \( \mathcal{O}_V \) is the identity element. Now define the sheaf

\[
\mathcal{L}^\wedge \coloneqq \text{Hom}(\mathcal{L}, \mathcal{O}_V).
\]

Let \( U \) be an open set such that \( \mathcal{L} \) is free of rank one, then \( \mathcal{L}^\wedge \) is by definition of \( \text{Hom} \) free of rank one on \( U \). Hence \( \mathcal{L}^\wedge \) is an invertible sheaf. Finally, the map

\[
\mathcal{L}^\wedge \otimes \mathcal{L} \to \mathcal{O}_V
\]

\[
(f, x) \mapsto f(x)
\]

is an isomorphism over any open subset \( U \) by definition of the dual \( \mathcal{O}_X(U) \)-module. Thus the map is an isomorphism and we obtain a group. It is called the Picard group of \( V \), denoted \( \text{Pic}(V) \) and we write \( \mathcal{L}^{-1} \) for \( \mathcal{L}^\wedge \).
1.4. The sheaf of differentials. We give here a short outline on sheaves of differentials for varieties. For a more detailed and general description for schemes, we refer the reader to ([Har77] 2.8). Let \( K \) be an arbitrary field, \( A \) a \( K \)-algebra and let \( M \) be an \( A \)-module.

**Definition.** A \( K \)-derivation is a map \( D : A \rightarrow M \) such that

1. \( D(c) = 0 \) for all \( c \in K \);
2. \( D(f + g) = D(f) + D(g) \);
3. \( D(fg) = D(f)g + fD(g) \) (Leibniz’s rule).

A pair \((\Omega_A^{A/K}, d)\) consisting of an \( A \)-module \( \Omega_A^{A/K} \) and a \( K \)-derivation \( d : A \rightarrow \Omega_A^{A/K} \) is called the module of differential one-forms for \( A \) over \( K \) if the following universal property holds: for any \( K \)-derivation \( D : A \rightarrow M \), there is a unique \( K \)-linear map \( \alpha : \Omega_A^{A/K} \rightarrow M \) such that the following diagram commutes.

\[
\begin{array}{ccc}
A & \xrightarrow{d} & \Omega_A^{A/K} \\
\downarrow{D} & & \downarrow{\beta} \\
M & & \\
\end{array}
\]

**Example.** Let \( A = K[X_1, \ldots, X_n] \). The \( \Omega_A^{A/K} \) is the free \( A \)-module with basis \( dX_1, \ldots, dX_n \) and 

\[
df = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i} dX_i.
\]

For varieties, we have the following result:

**Theorem 1.6.** Let \( V \) be a variety. For each \( n \geq 0 \), there is a sheaf of \( \mathcal{O}_V \)-modules \( \Omega_{V/K}^n \) such that 

\[
\Omega_{V/K}^n(U) = \bigwedge^n \Omega_A^{A/K}
\]

whenever \( U \) is an open affine of \( V \) isomorphic to \( \text{Spec } A \).

And finally, since abelian varieties are non-singular, the following result is useful.

**Proposition 1.7.** If \( V \) is nonsingular, then \( \Omega_{V/K}^1 \) is a locally free sheaf of rank \( \dim(V) \).

2. Abelian varieties

We now give a couple of useful definitions on abelian varieties. For more details, we refer the reader to ([Mil08]).

2.1. Basic definitions.

**Definition.** A group variety over a field \( K \) is an algebraic variety \( V \) over \( K \) together with regular maps

\[
m : V \times_K V \rightarrow V \text{(multiplication)}
\]

\[
\text{inv} : V \rightarrow V \text{(inverse)}
\]

and an element \( e \in V(K) \) such that the structure on \( V(K) \) defined by \( m \) and \( \text{inv} \) is a group with identity element \( e \).
Definition. Let $V$ be a group variety over $K$. For a point $a \in V(K)$ we define the right translation by $a$ to be the composite

$$V \xrightarrow{\cdot a} V \xrightarrow{x \mapsto x} V.$$ 

It is an isomorphism $V \xrightarrow{\cdot a} V$.

**Proposition 2.1.** Group varieties are smooth.

**Proof.** Over an algebraically closed field, this is straightforward, since any variety has a nonsingular dense open subvariety. Its translatees are still smooth, but they cover $V$. Finally a variety $V$ over $K$ is nonsingular if and only if $V_K$ is nonsingular. □

Definition. A complete connected group variety is called an abelian variety.

The geometric notion of connectedness of a variety is that it is connected over $\bar{K}$. Fortunately, one can show that a connected group variety is also geometrically connected. We can classify regular maps on abelian varieties:

**Proposition 2.2.** Every regular map $\alpha : A \to B$ of abelian varieties is a composition of a homomorphism with a translation.

**Corollary 2.3.** The group law on an abelian variety is commutative.

**Proof.** Observe the following: a group is abelian if and only if mapping an element to its inverse defines a homomorphism. Now the same mapping on an abelian variety is clearly regular. Furthermore it maps $0$ to itself, so it cannot be a homomorphism composed with a non-trivial translation. □

We now define isogenies. Recall that for elliptic curves, a non-constant isogeny is surjective and its kernel is a finite subgroup.

**Definition.** Let $\alpha : A \to B$ be a homomorphism of abelian varieties. The kernel of $\alpha$ is the fibre of $\alpha$ over $0$.

**Remark.** In general, note that $\ker \alpha$ is not an algebraic variety. However, it is if $K$ has characteristic $0$.

**Definition.** A homomorphism $\alpha : A \to B$ of abelian varieties is called an isogeny if $\alpha$ is surjective and its kernel has dimension $0$.

**Definition.** The degree of an isogeny $\alpha : A \to B$ is its degree as a regular map $[K(A) : \alpha^* K(B)]$.

As an example, the following theorem generalizes a familiar result for elliptic curves: Let $[m]$ denote the multiplication-by-$m$ map on an abelian variety $A$:

$$a \mapsto ma - a + a + \ldots + a (m \text{ terms}).$$

**Theorem 2.4.** Let $A$ be an abelian variety of dimension $g$, $m \in \mathbb{N}_0$. Then the multiplication-by-$m$ map $[m] : A \to A$ is an isogeny of degree $n^{2g}$.

Recall that for elliptic curves, there is a canonical isomorphism

$$E \to \text{Pic}^0(E)$$

$$P \mapsto [P] - [0].$$

There are two ways in which abelian varieties generalize this fact. One will be discussed in the next section, the other one deserves a mention here. Let $k$ be algebraically closed. Consider a curve $C/k$ and choose a base-point $Q \in C(k)$. 
Then there is an abelian variety, called the Jacobian variety of $C$ and a canonical regular map $\phi : C \to J$, such that $\phi(Q) = 0$ and

$$\text{Div}^0(C) \to J(k)$$

$$\sum_i n_i(P_i) \mapsto \sum_i n_i(\phi(P_i))$$

restricts to an isomorphism $\text{Pic}^0(C) \to J(k)$. Moreover, the dimension of the Jacobian equals the genus of the curve.

### 2.2. The dual abelian variety and polarizations.

For an elliptic curve, there is an isomorphism $E \cong \text{Pic}^0(E)$. Let $A$ be an abelian variety over $K$, we define a dual abelian variety $A^\vee$ such that $\text{Pic}^0(A) \cong A^\vee(K)$ and $\text{Pic}^0(A^\vee) \cong A(K)$. So let us first define $\text{Pic}^0$ of an abelian variety. We assume the following theorem:

**Theorem 2.5** (Theorem of the Square). Let $A$ be an abelian variety, $a, b \in A$, and let $t_a$ denote the translation map. For any invertible sheaf $L$ on $A$, there is an isomorphism

$$t^*_{a+b}L \otimes L \cong t^*_aL \otimes t^*_bL.$$

**Proof.** See ([CS86] 5.6). \qed

We can now map $A$ to the Picard group:

**Corollary 2.6.** The map

$$\lambda_L : A \to \text{Pic}(A)$$

$$a \mapsto t^*_aL \otimes L^{-1}$$

is a group homomorphism.

**Proof.** Just tensor the equality $t^*_{a+b}L \otimes L \cong t^*_aL \otimes t^*_bL$ with $L^{-2}$ to obtain

$$t^*_{a+b}L \otimes L^{-1} \cong (t^*_aL \otimes L^{-1}) \otimes (t^*_bL \otimes L^{-1}).$$ \qed

We want an invertible sheaf to lie in $\text{Pic}^0$ if this homomorphism becomes trivial over an algebraic closure:

**Definition.** Define $\text{Pic}^0(A)$ to be the subgroup of $\text{Pic}(A)$ satisfying for all $a \in A(K)$

$$t^*_aL \cong L \text{ on } A_K.$$

**Definition.** Let $K$ be a field. The dual abelian variety of an abelian variety $A/K$ is a pair $(A^\vee, \mathcal{P})$, where $A^\vee$ is an abelian variety over $K$ and $\mathcal{P}$ is an invertible sheaf on $A \times_K A^\vee$ such that the following two conditions hold:

1. $\mathcal{P}|_{A \times \{b\}} \in \text{Pic}^0(A_b)$ for all $b \in A^\vee$;
2. $\mathcal{P}|_{\{0\} \times A^\vee}$ is trivial,

where $A_b$ denotes the fibre for the projection morphism $A \times A^\vee \to A^\vee$. Furthermore, we require that the pair satisfies the following universal property: for any other pair $(T, \mathcal{L})$ such that

1. $\mathcal{L}|_{A \times \{t\}} \in \text{Pic}^0(A_t)$ for all $t \in T$ and
2. $\mathcal{L}|_{\{0\} \times T}$ is trivial,

there is a unique regular map $\alpha : T \to A^\vee$ such that $(1 \times \alpha)^*\mathcal{P} \cong \mathcal{L}$. 

3. THE FALTINGS HEIGHT

We assume the existence of such a pair here. Note that by definition, the pair \((A^\wedge, \mathcal{P})\) is uniquely determined up to isomorphism. The sheaf \(\mathcal{P}\) is called the \textit{Poincare sheaf}. We can rewrite the universal property in terms of \(\text{Hom}(T, A^\wedge) \cong \{\text{iso. classes of invertible sheaves on } A \times T \text{ satisfying (1) and (2)}\}\).

Now let \(T = \text{Spec}(K)\) such that the left-hand side is exactly \(A^\wedge(K)\). Moreover, the right-hand side is \(\text{Pic}^0(A)\) and so we see that indeed the dual abelian variety parametrizes \(\text{Pic}^0\).

Remark. The dual abelian variety has the nice property \(A^{\wedge \wedge} = A\). See for example ([Mum08] 3.13).

It follows from our previous considerations that for an elliptic curve \(E^\wedge = E\). However, in general, \(A\) and \(A^\wedge\) are isogenous, but not isomorphic. This leads us to define polarizations of abelian varieties.

Definition. A \textit{polarization} \(\lambda\) on an abelian variety \(A\) defined over \(K\) is an isogeny \(\lambda: A \to A^\wedge\) such that over \(A\bar{K}\), there is an invertible sheaf \(\mathcal{L}\) that verifies \(\lambda*\mathcal{L} = \lambda_{\bar{K}}\) (with the notations of corollary 2.6). Furthermore, we require the sheaf \(\mathcal{L}\) to be ample.

For more on ample sheaves, we refer the reader to ([Iit82] 2.20). In this context, one can think of an ample sheaf as an invertible sheaf with non-trivial global section and such that only a finite set of points \(a \in A(K)\) verify \(t_a^*\mathcal{L} \cong \mathcal{L}\).

Definition. A \textit{polarized abelian variety} is a pair \((A, \lambda)\), where \(A\) is an abelian variety and \(\lambda\) a polarization.

A morphism of polarized abelian varieties is then a morphism of abelian varieties that commutes with the polarizations. For some purposes it is preferable to consider polarized abelian varieties if one seeks higher degree analogues of elliptic curves. For instance, polarized abelian varieties clearly have less automorphisms and recall that the automorphism group of an elliptic curve is small (it has order dividing 24).

2.3. Families of abelian varieties.

Definition. Let \(S\) be a variety over \(K\). A \textit{family of abelian varieties over} \(S\) is a proper smooth map \(\pi: A \to S\) together with a law of composition

\[ A \times_s A \to A \]

such that each fibre is an abelian variety.

We need this definition later, but give no further results. However, note that indeed many results on abelian varieties extend to families of abelian varieties. For instance, a family of abelian varieties is also commutative.

3. The Faltings height

Faltings attaches a canonical height to an abelian variety \(A\) over a number field \(K\).

3.1. The height of an elliptic curve over \(\mathbb{Q}\). Let us first consider the case that is of a particular interest to us, namely the height of an elliptic curve defined over \(\mathbb{Q}\). For an elliptic curve \(E\) over \(\mathbb{C}\) the most intuitive way to assign it a real number that measures its size would be to view the curve as \(\mathbb{C}/\Lambda\) and take the reciprocal of the area of a fundamental domain for \(\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2\). However, this is not canonical, since the real number

\[ H(E) = |\omega_1 \wedge \omega_2|^{-1} \]
depends on the choice of an isomorphism $\mathbb{C}/\Lambda \rightarrow E(\mathbb{C})$. In fact, we have the following result.

**Proposition 3.1.** Let $E$ be an elliptic curve over $\mathbb{C}$. The following are equivalent:

1. the choice of an isomorphism $\mathbb{C}/\Lambda \rightarrow E(\mathbb{C})$;
2. the choice of a non-zero holomorphic differential on $E$;
3. the choice of an equation
   
   \[ Y^2 - 4X^3 - BX - C \]

for $E$.

**Proof.**

- (1) $\rightarrow$ (3) Given a lattice $\Lambda$, there is a Weierstrass function $P(z)$ together with numbers $B, C$ for which the map
  
  $\mathbb{C}/\Lambda \rightarrow \mathbb{P}^2$
  
  $z \mapsto (P(z) : P'(z) : 1)$

is an isomorphism between $E$ and the projective curve given by $Y^2 - 4X^3 - BX - C$.

- (3) $\rightarrow$ (2) Just put $\omega = dX/Y$.

- (2) $\rightarrow$ (1) Let $\omega$ be a differential on $E$ and consider the map $P \mapsto \int_0^P \omega : E(\mathbb{C}) \rightarrow \mathbb{C}$. This integral depends on the choice of a path and because $\omega$ is holomorphic, it only depends on the homotopy class of the path. Now if $\gamma_1$ and $\gamma_2$ are generators for $H_1(E, \mathbb{Z})$, two such paths will differ by a loop $l_\gamma + n\gamma_2$. Thus, if we set $\omega_i - \int_{\gamma_i} \omega$, we obtain a well-defined map $E(\mathbb{C}) \rightarrow \mathbb{C}/\Lambda, \Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. It is an isomorphism.

Now if we have chosen a pair $(E, \omega)$ over $\mathbb{C}$, we can set $H(E, \omega)^{-1}$ to be the volume of a fundamental domain for the corresponding lattice. Moreover, if the elliptic curve is given over $\mathbb{Q}$, we can choose an equation $Y^2 - 4X^3 - BX - C$ with rational coefficients and take the differential to be $\omega = dX/Y$. This procedure gives a well-defined height up to multiplication by a nonzero rational number. But we can do better then that: we know there is a minimal equation

\[ Y^2 + a_1XY + a_3Y - X^3 + a_2X^2 + a_4X + a_6, \ a_i \in \mathbb{Z} \]

and the Weierstrass differential

\[ \omega = \frac{dX}{2Y + a_1X + a_3} \]

is well-defined up to sign. Which means that the height function corresponding to this differential is uniquely determined. Unfortunately, this already fails to work if instead of $\mathbb{Q}$ we consider a number field with class number $h_K > 1$, because the existence of a global minimal equation is no longer guaranteed.

**3.2. The height of a normed module.** Let $K$ be a number field, let $R$ denote the ring of integers in $K$. Recall that if $M$ is a projective $R$-module of rank 1, the choice of an isomorphism $M \otimes_R K \cong K$ identifies $M$ with a fractional ideal in $K$. Now suppose we are given norms on $M \otimes_R K_v$ for each $v \mid \infty$. We can then define a height on $M$ relative to these norms:

\[ H(M) = \frac{[M : mR]}{\prod_{v \mid \infty} \prod\{m\}} \]
3. THE FALTINGS HEIGHT

where \( m \) is any nonzero element of \( M \) and \( \epsilon_v = 1 \) or 2 depending on whether the valuation is real or complex. We have to show that this height is well-defined.

**Lemma 3.2.** The definition is independent of the choice of \( m \).

**Proof.** Let \( M_v = R_v \otimes_K M \). It is a projective module of rank 1 over \( R_v \) and since \( R_v \) is principal \( M_v \) is free of rank 1. Thus, we can write \( M_v = m_v R_v \). With these notations, the local indexes are easy to compute:

\[
[M_v : m R_v] = [m_v R_v : m R_v] = |a_v|_v,
\]

where \( a \) is the unique element of \( K_v \) such that \( a_v m = m_v \). By the chinese remainder theorem,

\[
\mathbb{M}_v = \mathbb{M}_v R_v \cong \bigoplus_{v \mid \infty} \mathbb{M}_v/m R_v
\]

and we get a better description of the height (with the previous notations):

\[
H(M) = \frac{1}{\left[ \prod_{v \mid \infty} |a_v|_v \right] \prod_{v \mid \infty} |m|_v^{\epsilon_v}}.
\]

Since we use normalized absolute values, the product formula holds \( \prod |a_v|_v = 1 \) and it follows that the height does not change if we replace \( m \) by \( am, a \in R \). This concludes the proof since \( M \) is of rank 1 over \( R_v \).

The advantage is that this height can be made absolute in the following sense:

**Proposition 3.3.** Let \( \mathbb{K} \) be a number field and define

\[
h(M) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \log H(M).
\]

Then for any finite extension \( L \) of \( \mathbb{K} \), if \( R_L \) denotes the ring of integers of \( L \)

\[
h(R_L \otimes_R M) = h(M).
\]

3.3. The Faltings height of an abelian variety. Let \( A \) be an abelian variety of dimension \( g \) over a number field \( \mathbb{K} \), \( \mathbb{R} \) the ring of integers in \( \mathbb{K} \). We want to attach a normed module to this variety in a canonical way, if possible. We assume the following result about the existence of the Neron model.

**Proposition 3.4.** There is a canonical extension of \( A \) to a smooth group variety \( \mathcal{A} \) over \( \text{Spec} \mathbb{R} \). Furthermore, the sheaf of relative differential \( g \)-forms on \( \mathcal{A} \)

\[\Omega^g_{\mathcal{A}/\mathbb{R}}\]

is a locally free sheaf of \( \mathcal{O}_{\mathcal{A}} \)-modules of rank 1.

Define \( s : \text{Spec} \mathbb{R} \to \mathcal{A} \) to be the section whose image in each fibre is the zero element. Finally, define

\[M = s^* \Omega^g_{\mathcal{A}/\mathbb{R}}.\]

It is a locally free sheaf of rank 1 on \( \text{Spec} \mathbb{R} \), so it can be viewed as a projective \( \mathbb{R} \)-module of rank 1. Let \( v \) be an infinite prime of \( \mathbb{K} \). It remains to define an appropriate norm on \( M \otimes_{\mathbb{R}} K_v \). We assume the following equality, which is discussed in ([Mil08] 4.6):

\[M \otimes_{\mathbb{R}} K_v = \Gamma(A, \Omega_{A/K_v}) \text{ such that } M \otimes_{\mathbb{R}} K_v = \Gamma(A_{K_v}, \Omega_{A_{K_v}/K_v}).\]

Now the algebraic closure of \( K_v \) is contained in \( \mathbb{C} \) and we can define \n
\[|a|_v = \left( \left( \frac{i}{2} \right)^g \int_{A(\mathbb{C})} \omega \wedge \omega \right)^{1/2}\]

which is easily seen to make \( M \) into a normed \( \mathbb{R} \)-module. Thus, we can define the Faltings height of \( A \) to be

\[H(A) = H(M).\]
Using the description of lemma 3.2, we can make this height more explicit: let a holomorphic differential $g$-form $\omega$ be the element $m \in M$. Again, assume the existence of a Neron differential $g$-form $\omega_v$ for $A/K_v$. Then

$$H(A) = \frac{1}{\prod_{v < \infty} |a_v|_v \prod_{v < \infty} \left( (\frac{1}{2})^g \int_{A(C)} \omega \wedge \omega \right)^{1/2}},$$

where $a_v$ denotes the element $a \in K_v$ such that $\omega = a \omega_v$.

Let us re-examine what happens if $A$ is an elliptic curve. In this case, the Weierstrass minimal equation is unique and provides the canonical model for an infinite prime $v$. Thus $\omega_v$ is just the differential corresponding to the Weierstrass minimal equation. Let now $L/K$ be an extension of number fields. This yields an abelian variety $A_L$ over $L$. If we define

$$h(A) = \frac{1}{[K : \mathbb{Q}]} \log H(A)$$

do we also have $h(A_L) = h(A)$? In general this is not true, since the Neron minimal model might change. However, this is true if $A$ has semistable reduction everywhere, in which case we call $h(A)$ the **stable Faltings height** and denote it $h_F(A)$.

4. The modular height

4.1. Heights on projective space. Let $K$ be a number field. Let $P = (x_0 : \ldots : x_n) \in \mathbb{P}^n(K)$. We want to assign to this point a real number $H(P)$ such that, among others, the following property holds:

**Proposition 4.1.** For any $C \in \mathbb{R}$, there are only finitely many points in $\mathbb{P}^n(K)$ with $H(P) < C$.

We will define this height function, but not prove any propositions. The whole discussion (and the proofs) can be found in ([Sil09] 8.5). Let $v$ be a place of $K$ and denote by $n_v$ the local degree at $v$

$$n_v = [K_v : \mathbb{Q}].$$

Also, let $\mathcal{M}_K$ denote the standard set of inequivalent absolute values on $K$, namely those that restrict to a non-archimedean absolute value on $\mathbb{Q}$ or to the usual absolute value on $\mathbb{Q}$.

**Definition.** Let $P = (x_0 : \ldots : x_n) \in \mathbb{P}^n(K)$, the height of $P$ is defined by

$$H(P) = \prod_{v \in \mathcal{M}_K} \max(|x_0|_v, \ldots, |x_n|_v)^{n_v}.$$ 

A trivial calculation using the product formula shows that the height is independent of the choice of homogeneous coordinates for $P$, and thus well-defined. Furthermore, the following result holds:

**Lemma 4.2.** Let $L/K$ be a finite extension. Then

$$h_L(P) = H_K(P)^{[L : K]},$$

with the obvious notations.

Thus we get a new height invariant under finite field extensions

$$h(P) := \frac{1}{[K : \mathbb{Q}]} \log H(P).$$

Of course, this function has very similar properties, in particular the finiteness result of proposition 4.1 also holds (for a proof, see theorem 5.11 of [Sil09]). Now if $V$ is an algebraic variety, an embedding $\alpha : V \hookrightarrow \mathbb{P}^n$ defines a height function on $V$ and injectiveness guarantees that yet again proposition 4.1 holds.
4.2. The Siegel modular variety. For the sake of completeness, we define the Siegel modular variety, but omit any proofs, which are beyond the scope of this report. Let $L$ be a field and let $\mathcal{M}_{g,d}(L)$ denote the set of isomorphism classes of pairs $(A, \lambda)$, where $A$ is an abelian variety over $L$ of dimension $g$ and $\lambda$ is a polarization of $A$ of degree $d$.

**Theorem 4.3.** There exists a unique algebraic variety $M_{g,d}$ over $\mathbb{C}$ and a bijection

$$j : \mathcal{M}_{g,d}(\mathbb{C}) \to M_{g,d}(\mathbb{C})$$

such that:

1. For every point $P \in M_{g,d}$, there is an open neighbourhood $U$ of $P$ and a family $\mathcal{A}$ of polarized abelian varieties over $U$ such that for all $Q \in M_{g,d}$, the fibre $A_Q$ represents $j^{-1}(Q)$.
2. For any variety $T$ over $\mathbb{C}$ and any family of polarized abelian varieties over $T$ of dimension $g$ and degree $d$, the map $T \to M_{g,d}$, $t \mapsto j(A_t)$ is regular.

This variety is called the Siegel modular variety. Now the automorphisms of $\mathbb{C}$ act on $M_{g,d}$ over $\mathbb{C}$. They also act on any model over $\mathbb{Q}$ of a variety $V$ over $\mathbb{C}$. The following holds:

**Proposition 4.4.** There exists a unique model of $M_{g,d}$ over $\mathbb{Q}$ such that the bijection $j$ commutes with the two actions described above.

4.3. The modular height. The Siegel modular variety described above has a canonical embedding into projective space and so there is a height function $h$ on $M_{g,d}(K)$ for any number field $K$. We define the modular height of a polarized abelian variety $(A, \lambda)$ over $K$ by

$$h_M(A, \lambda) = h(j(A, \lambda)).$$

Let us now examine elliptic curves over $\mathbb{Q}$. In this case, $\mathcal{M}_{1,1}(\mathbb{C})$ is the set of isomorphism classes of elliptic curves over $\mathbb{C}$. The map $j$ is precisely given by the $j$-invariant of the elliptic curve and so $M_{1,1} = \mathbb{A}^1$. Furthermore, the model of $M_{1,1}$ over $\mathbb{Q}$ is still $\mathbb{A}^1$. Indeed, $j$ commutes with the action of an automorphism $\sigma$ of $\mathbb{C}$: if $E$ has equation

$$Y^2 - X^3 + AX + B,$$

then $\sigma E$ has equation

$$Y^2 - X^3 + \sigma AX + \sigma B$$

and so $j(\sigma E) = \sigma j(E)$. Now write $j(E) = \frac{m}{n}$, where $m$ and $n$ are relatively prime integers. We view $j(E)$ as a point $(m : n) \in \mathbb{P}^1$ and since they are relatively prime, the only absolute value that contributes is the archimedean one. Indeed, for any non-archimedean absolute value, both integers have absolute value $\leq 1$ and at least one has absolute value $1$. Hence

$$h_M(E) = \log \max\{|m|, |n|\}.$$

5. Some finiteness results

We have defined two quite different heights on an abelian variety. There is a beautiful (but alas, hard to prove) result that relates these two heights:

**Theorem 5.1.** Let $K$ be a number field. For every polarized abelian variety $(A, \lambda)$,

$$h_F(A) = h_F(A, \lambda) + O(\log h_M(A, \lambda)).$$
This has some immediate consequences. Since we have seen that the set
\[ \{ P \in M_{g,d}(K) \mid H(P) < C \} \]
is finite, one can prove using theorem 5.1:

**Corollary 5.2.** Let \( K \) be a number field and let \( g, C \) be integers. Up to isomorphism, there are only finitely many abelian varieties \( A \) over \( K \) of dimension \( g \) with semistable reduction everywhere and
\[ h_F(A) < C. \]

**Proof.** We refer the reader to [Mil08] for a detailed explanation of semistable reduction and the proof of this corollary.

We conclude by stating two finiteness results that Faltings published in his famous paper [Fal83].

**Theorem 5.3** (Shafarevich conjecture). Let \( K \) be a number field and \( S \) a finite set of primes of \( K \). For given \( g \) and \( d \), there are only finitely many isomorphism classes of polarized abelian varieties over \( K \) with dimension \( g \), degree of polarization \( d \) and good reduction outside of \( S \).

We have proven this result for elliptic curves (theorem 1.8 and corollary). In this more general setting, the impressive result is that the Shafarevich conjecture implies the Mordell conjecture:

**Theorem 5.4** (Mordell’s conjecture). If \( C \) is a projective nonsingular curve of genus \( g \geq 2 \) over a number field \( K \), then \( C(K) \) is finite.
CHAPTER 3

The average rank of an elliptic curve

Our goal in this final chapter is to retrace the proof given in ([BS10]) of the following fact:

**Theorem 0.5.** When averaged over their height, the average rank of elliptic curves $E$ defined over $\mathbb{Q}$ is less than $1.5$.

More precisely, if $H(E)$ denotes the height of an elliptic curve $E$, we want to see that

$$\lim_{X \to \infty} \frac{\sum_{H(E) < X} \text{rank}(E)}{\sum_{H(E) < X}} = 1.5.$$ 

Any elliptic curve $E$ over $\mathbb{Q}$ can be written as

$$E : y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{Z}$. Under this form, the discriminant is

$$\Delta = -16(4A^3 + 27B^2).$$

Over $\mathbb{Q}$, we know that there is a global minimal Weierstrass equation. Considering that the only change of variables preserving this form is

$$x = u^2 x' \quad \text{and} \quad y = u^3 y',$$

for some $u \in \mathbb{Q}^*$, (and that the discriminant then becomes $\Delta' = u^{-12}\Delta$) we see that the equation above is unique if we require that for all primes $p$ one of the two conditions $p \nmid B$ or $p \nmid A$ is false. We denote this equation $E_{A,B}$ and its discriminant $\Delta_{A,B}$. As height of an elliptic curve, we use

$$H(E_{A,B}) = \max\{4|A|^3, 27B^2\}.$$ 

In the previous chapter, we saw that modular height and Faltings height only differ by a constant. Moreover, recall that the modular height is given by the j-invariant. But for an equation of the form $E_{A,B}$, the invariant is

$$J(E_{A,B}) = \frac{1728A^3}{4A^3 + 27B^2}.$$ 

So we can use $H(E_{A,B})$ instead. For instance, if $H(E_{A,B}) < C$, then the modular height $H(E) < 432C$. In fact, we prove the following:

**Theorem 0.6.** When all elliptic curves $E/\mathbb{Q}$ are ordered by height, the average size of the 2-Selmer group $S^2(E/\mathbb{Q})$ is 3.

This implies theorem 0.5. Indeed, there is the short exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to S^2(E/\mathbb{Q}) \to \text{III}(E/\mathbb{Q})[2] \to 0,$$

where $TS(E)$ denotes the Tate-Shafarevich group. We have seen that the 2-Selmer group is finite and thus has order $2^s$ for some integer $s$ since the two other terms in the sequence are 2-groups. Set $r_2(A) = s$ for an abelian 2-group $A$ of order $2^s$. Then $E(\mathbb{Q})/2E(\mathbb{Q})$ has a copy of $\mathbb{Z}/2\mathbb{Z}$ for each copy of $\mathbb{Z}$ in $E(\mathbb{Q})$. So $r_2(E(\mathbb{Q})/2E(\mathbb{Q})) = r(E(\mathbb{Q})) + r_2(E(\mathbb{Q})[2])$. This yields the following equality of positive integers:

$$r_2(S^2(E/\mathbb{Q})) = r(E(\mathbb{Q})) + r_2(E(\mathbb{Q})[2]) + r_2(\text{III}(E/\mathbb{Q})[2]).$$
Hence, if on average we bound the term on the left by 1.5, the 3 terms on the right are automatically bounded by 1.5.

Remark. What would one expect these ranks to be on average? First of all, it is an old conjecture that roughly half of the elliptic curves have rank 0 and half half rank 1 so on average the rank \( E(\mathbb{Q}) \) is 1/2. As for rational 2-torsion, a cubic equation \( x^3 + Ax + B = 0 \) is on average not expected to have a rational solution, so one expects this rank to be 0 on average. This result will in fact follow from lemma 3.2. Finally, heuristics suggest that most of elliptic curves do not have elements of order two in their Tate-Shafarevich group. Assuming that the \( \mathcal{X}(E/\mathbb{Q}) \) is finite, Delaunay ([Del01]) showed that one expects 58% of curves of rank 0 and 31% of curves of rank 1 to verify \( 2 | \mathcal{X}(E/\mathbb{Q}) \). So if all the conjectures above hold, an ideal result would be \( r \) on average. However, Bhargava and Shankar’s result remains very impressive, since the best known bound until then was 25/14, and assumed the Riemann hypothesis and the Birch-Swinnerton-Dyer conjecture.

We now turn to the proof of theorem 0.6. First, we show how to associate an integral binary quartic form to an element in the 2-Selmer group. Then in the next section, we count \( Gl_2(\mathbb{Z}) \)-equivalence classes of such forms. To count the forms relevant for us, a sieve has to be performed, which is done in the third section.

1. From the 2-Selmer group to binary quartic forms

In this section, we show how counting elements in the 2-Selmer group reduces to counting equivalence classes of binary quartic forms. The reference for this section is [BSD63].

1.1. The Selmer group and 2-coverings.

Definition. Let \( E/\mathbb{Q} \) be an elliptic curve. A 2-covering of \( E \) is a genus one curve \( C \) together with morphisms \( \phi : C \rightarrow E \) and \( \theta : C \rightarrow E \), where \( \phi \) is an isomorphism (over \( \overline{\mathbb{Q}} \)) and \( \theta \) is a morphism of degree 4 defined over \( \mathbb{Q} \) such that the following diagram commutes.

\[
\begin{array}{c}
E \\
\phi \downarrow \downarrow \theta \\
C \\
\end{array}
\]

We identify two 2-coverings \( C \) and \( C' \) if there exists a 2-torsion point \( P \in E \) and an isomorphism \( \psi : C \rightarrow C' \) over \( \mathbb{Q} \) such that the diagram

\[
\begin{array}{c}
E \\
\phi \\
C \\
\end{array} \quad \begin{array}{c}
\phi' \\
\psi \\
C' \\
\end{array}
\]

commutes.

Definition. We say that a 2-covering \( C \) is soluble if \( C(\mathbb{Q}) \neq \emptyset \) and locally soluble if it possesses a point in every completion \( \mathbb{Q}_p \) and in \( \mathbb{R} \).

Now such a curve \( C \) has a rational point \( Q \) if and only if \( \theta(Q) \in E(\mathbb{Q}) \). Moreover, if \( \theta(Q) \in 2E(\mathbb{Q}) \), we get that \( \phi(Q) \) is a rational point. It follows that \( \phi \) is defined over \( \mathbb{Q} \) and we get the trivial covering (the equivalence class of \( E \)). There is in fact an isomorphism of groups

\[ \{ \text{eq. classes of soluble 2-coverings} \} \cong E(\mathbb{Q})/2E(\mathbb{Q}). \]
But \(\phi\) defined. Take \(\psi\) so that 
\[
\ker \phi = \psi \phi \psi^{-1} \quad \text{and also}
\]
where \(P\) and is also a morphism. Define a map:

\[
\begin{align*}
\homogeneous \text{ space. The subtraction map is given by} \\
E \text{group law on} \quad (this is clear from the fact that} \\
C \text{using the addition law on} \\
2 \\
\text{of} \\
\text{Twist} \\
\text{Thus via the bijection above, we get a group structure on the corresponding subset} \\
\text{is an isomorphism of groups. Since} \ E[2]\text{ is abelian and} \ G_{\mathbb{Q}/\mathbb{Q}}\text{-invariant,} \\
T_2 \text{ is too. Thus via the bijection above, we get a group structure on the corresponding subset} \\
T_{\text{Twist}}(\mathbb{E}/\mathbb{Q}) \text{. We show that these are our} \\
2 \text{-coverings. Let} \ (C, \theta, \phi) \text{ be such a} \\
2 \text{-covering. Define a map} \\
\mu : C \times E \to C \\
(p, P) \mapsto \phi^{-1}(\phi(p) + P) \\
\text{using the addition law on} \ E \text{. This map gives a simply transitive action of} \ E \text{ on} \\
C \text{(this is clear from the fact that} \ \phi \text{ is an isomorphism and that we use the actual} \\
\text{group law on} \ E \text{)}. It is also clear that} \ \mu \text{ is a morphism. Thus a} \\
2 \text{-covering is a} \\
\text{homogeneous space. The subtraction map is given by} \\
\nu : C \times C \to E \quad (q, p) \mapsto \phi(q) - \phi(p) \\
\text{and is also a morphism. Define a map:} \\
\}
\text{classes of 2-coverings} \to H^1(G_{\mathbb{Q}/\mathbb{Q}}, E[2]) \\
(C, \theta, \phi) \mapsto \{\sigma \mapsto \phi(P)^{\sigma} - \phi(P)\}, \\
\text{where} \ P \in \ker \theta \text{. Observe that} \\
[2](\phi(P)^{\sigma} - \phi(P)) = [2]\phi(P)^{\sigma} - [2]\phi(P) \\
- \theta(P)^{\sigma} - \theta(P) \\
- O \\
\text{and also} \\
\phi(P)^{\sigma \tau} - \phi(P) - (\phi(P)^{\sigma \tau} - \phi(P)^{\tau} + \phi(P)^{\tau} - \phi(P) \\
\text{so that} \ \sigma \mapsto \phi(P)^{\sigma} - \phi(P) \text{ is indeed a cocycle. Let us show that the map is well-} \\
\text{defined. Take} \ \psi : C \to C' \text{ to be the isomorphism defined over} \ \mathbb{Q} \text{ that gives the} \\
equivalence and \ P' \in \ker \theta' \text{. Then for some} \ Q \in \ E[2]: \\
\phi(P)^{\sigma} - \phi(P) - \phi \psi(P)^{\sigma} - Q - \phi \psi(P) + Q \\
- \phi \psi(P)^{\sigma} - \psi \phi(P) \\
- (\phi'(P')^{\sigma} - \phi'(P')) + [\phi'(\psi(P))^{\sigma} - \phi'(P')^{\sigma} - (\phi'(\psi(P)) - \phi'(P'))] \\
- (\phi'(P')^{\sigma} - \phi'(P')) + [(\phi'(\psi(P)) - \phi'(P'))^{\sigma} - (\phi'(\psi(P)) - \phi'(P'))]. \\
\text{But} \\
[2](\phi'(\psi(P)) - \phi'(P')) - \theta \psi(P) - \theta'(P') = 0
so the two cocycles differ by the coboundary generated by $\phi'(\psi(P)) - \phi'(P') \in E[2]$. We now prove injectivity. Assume $C$ and $C'$ map to cocycles that differ by $T^\sigma - T$ for some $T \in E[2]$: 

(6) \[ \phi(P)^\sigma - \phi(P) - (\phi'(P')^\sigma - \phi'(P')) + T^\sigma - T. \]

Then define

\[ \psi : C \rightarrow C', \]

\[ Q \mapsto \phi'^{-1}(\phi(Q) - \phi(P) + \phi'(P') + T). \]

The following diagram commutes

\[
\begin{array}{ccc}
E & \xrightarrow{\phi} & E \\
\downarrow{\phi(P)^\sigma - \phi(P) - (\phi'(P')^\sigma - \phi'(P')) + T^\sigma - T} & & \downarrow{\phi'} \\
C & \xrightarrow{\psi} & C'
\end{array}
\]

where $(-\phi(P) + \phi'(P') + T) \in E[2]$. Finally, it follows from equation 6 that $\psi$ is defined over $\mathbb{Q}$. Thus $C$ and $C'$ are in the same equivalence class! To prove surjectivity, let $\xi$ be a cocycle. From surjectivity in proposition 3.2 of chapter 1, we get a curve $C/\mathbb{Q}$, together with an isomorphism $\phi : C \rightarrow E$ over $\overline{\mathbb{Q}}$ such that

$\phi^\sigma \phi'^{-1} - \tau_{\xi_\sigma}$

is the translation by a 2-torsion point. It remains to see that the composition $[2]\phi$ is defined over the rationals. But this follows from

$([2]\phi)^\sigma - [2]\phi^\sigma - [2]\tau_{\xi_\sigma} = [2]\phi.$

So we have shown that one can identify $H^1(G_{\mathbb{Q}/\mathbb{Q}}, E[2])$ with our equivalence classes of 2-coverings. Moreover, it is clear from the correspondence that an element in $H^1(G_{\mathbb{Q}/\mathbb{Q}}, E[2])$ is everywhere locally trivial if and only if the associated 2-covering has a point in every completion $\mathbb{Q}_p$. Hence we have proven the proposition (and in fact also the characterisation of soluble 2-coverings!).

Remark. Note that the same proof works for any number field $K$ instead of $\mathbb{Q}$ and any $n$-Selmer group.

1.2. The quartic associated to a locally soluble 2-covering. Let $(C, \phi, \theta)$ be a 2-covering of an elliptic curve $E/\mathbb{Q}$. Consider the mapping

$C \times C \rightarrow E$

$(P, Q) \mapsto \theta(P) + \theta(Q).$

It is defined over $\mathbb{Q}$ and induces a mapping

$\mu : \{ \text{positive divisors of degree 2 on } C \} \rightarrow E$

also defined over the rationals by simply mapping the 2 points giving the divisor.

Proposition 1.2. If $C$ is a curve corresponding to an everywhere locally trivial 2-covering, then $C$ has a positive rational degree 2 divisor.

Proof. Let $\phi : C \rightarrow E$ denote the isomorphism and $\theta : C \rightarrow E$ the degree 4 map. Let $\phi^\sigma$ denote the induced map on divisors $\text{Div}(E) \rightarrow \text{Div}(C)$. Recall that for an elliptic curve, two divisors are linearly equivalent if and only if they have the same degree and the sum of their points are identical (this follows from Riemann-Roch). Hence the divisors that map to $O$ through $\mu$ are those linearly equivalent to $\phi^\sigma 2(O)$. Denote by $|D|$ the set of positive divisors that are linearly equivalent
to a divisor $D$ (it is called a complete linear system). The set $|D|$ is in one-to-one correspondence with

$$\{ f \in \mathbb{Q}(C) : (f) + D \geq 0 \}/\mathbb{Q}^x,$$

where $(f)$ denotes the divisor associated to $f$.

Let $K$ be a field. Recall that by Riemann-Roch’s theorem, the vector space

$$\mathcal{L}(D) = \{ f \in K(C) : (f) + D \geq 0 \} \cup \{ 0 \}$$

has dimension the degree of $D$ (here $D$ is a divisor over a curve of genus $1$ over $K$). Hence $|D|$ identifies with the projective space $\mathbb{P}(\mathcal{L}(D)) = \mathbb{P}^{\deg D-1}$. Moreover, by a general version of Riemann-Roch (see [Lor96] 9.4), if $G_{K/L}$ fixes $D$ for some Galois extension $L/K$, $|D|$ identifies with $\mathbb{P}^{\deg D-1}(L)$.

Therefore $2(O)$ identifies with $\mathbb{P}^1(\mathbb{Q})$. In the same way, the linear system $|\phi^*2(O)|$ is parametrized by a twist of $\mathbb{P}^1$, i.e. a curve of genus $0$ that is isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$, denoted $S$. Now since the map $\mu$ is defined over the rationals, we see that if a divisor $(X_1) + (X_2) \mapsto O \in E$, the fields of definition $\mathbb{Q}(X_1)$ and $\mathbb{Q}(X_2)$ are the same. This means that if $C$ has points in $\mathbb{Q}_p$, so does $S$. But for $S$, the Hasse principle holds, so we get that $S$ has a rational point. The corresponding divisor, in turn, is rational.

We obtain:

**Proposition 1.3.** An element in the 2-Selmer group can be represented by a curve

$$C : y^2 = g(x) - ax^4 + bx^3 + cx^2 + dx + e$$

with rational coefficients.

**Proof.** Let $C$ be a curve in the corresponding equivalence class of 2-coverings. Let $D$ denote the divisor from the previous proposition. By the Riemann-Roch theorem the $\mathbb{Q}$-vector space $\mathcal{L}(D)$ has dimension 2. Since $D$ is positive, $\mathcal{L}(D)$ contains the constant functions. Denote by $x$ a non-constant function in $\mathcal{L}(D)$. Now consider the space $\mathcal{L}(2D)$ of dimension 4. It contains $1, x, x^2$. Let $v$ be a function linearly independent of these three. Finally consider the space of dimension 8 over $\mathbb{Q}$: $\mathcal{L}(4D)$. It contains the functions

$$1, x, x^2, x^3, x^4, v, v^2, xv, x^2v.$$

So we get a linear dependence relation between them. Moreover, the coefficient of $v^2$ in this relation is invertible. Assume otherwise, then $v \in \mathbb{Q}(x)$. But $(x) = 0$ if and only if $x$ is a constant function on $C$ and because $C$ has genus 1, $x$ has no simple pole. This means that $(x)$ has exactly the same poles as $D$. Hence, the minimal relation giving $v \in \mathbb{Q}(x)$ only contains $1, x, x^2$ since otherwise $v \notin \mathcal{L}(2D)$. This shows that $v$ is linearly dependent of $1, x, x^2$ which is a contradiction. So there exists a relation with rational coefficients

$$v^2 - 2n(2x^2 + mx + n) = ax^4 + bx^3 + cx^2 + dx + e.$$

The substitution $y - v = lx^2 + mx - n$ now gives an equation of the desired form. To show that the curve defined by this equation is $C$, it is enough to show that

$$\mathbb{Q}(x, y) = \mathbb{Q}(C).$$

But both contain $y$ and are quadratic extensions of $\mathbb{Q}(x)$. \qed

We ask the question of when, conversely, two quartics give equivalent 2-coverings.
3. THE AVERAGE RANK OF AN ELLIPTIC CURVE

Definition. We say that two binary quartic forms $f$, $f'$ with coefficients in a field $K$ are $K$-equivalent if and only if there exists $\mu \in K$ and $\gamma \in GL_2(K)$ such that

$$f = \mu^2(\gamma \cdot f').$$

If $K = \mathbb{Q}$, we just say equivalent.

Proposition 1.4. Two quartics $g$ and $g'$ give rise to the same equivalence class of 2-coverings if and only if their corresponding binary quartic forms are equivalent.

Proof. Let $C$ be the curve defined by the quartic $y^2 = g(x)$. We may assume that it has non-zero discriminant. Then the curve has genus 1 and so the Jacobian of $C$ is an elliptic curve $E$, where we identify $Pic^0(C) \cong E$ as in theorem 3.6. Define a 2-covering of the Jacobian of $C$ by taking a root $\xi$ of $g(x)$ and setting

$$\theta : C \to Pic^0(C)$$

$$P \mapsto [2(P) - 2(\alpha)],$$

where $\alpha = (\xi, 0)$ and the brackets denote the equivalence class. Also, note that $\theta$ is defined over $\mathbb{Q}$. In addition to that, we know that there is an isomorphism $\phi : C \to Pic^0(C) \cong E$ over $\mathbb{Q}$ by definition of the Jacobian. Hence the map

$$\theta : C \to E$$

$$P \mapsto 2(\phi(P) - \phi(\alpha))$$

yields a commutative diagram

$$\begin{array}{ccc}
E & \xrightarrow{[2]} & E \\
\phi \downarrow & & \downarrow \phi \\
C & \xrightarrow{\theta} & E
\end{array}$$

Moreover, $\theta$ is defined over the rationals and $\phi$ is defined over $\mathbb{Q}(\alpha)$ so we have our desired 2-covering. Note that by construction $\alpha \in \ker \theta$ so it is clear that the equivalence class of the covering does not depend on the choice of the root $\xi$ (see the proof of 1.1). It follows for the same reason that two curves $C : y^2 = g(x)$ and $C' : y'^2 = g'(x')$ give the same equivalence class of two coverings if and only if there is an isomorphism $\psi : C \to C'$ such that the roots of $g$ and $g'$ are in correspondence. But $C$ and $C'$ are given by homogeneous equations of the form

$$C : y^2z^2 = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4,$$

with rational coefficients. Hence it is necessary that the isomorphism $\psi$ is bilinear on the $x$ and $z$-coordinates, since otherwise the respective roots do not correspond. This condition is also sufficient. Also, by looking at the left-hand side of the equation, it is clear that the forms $g$ and $g'$ can differ by a perfect square. We conclude that such a morphism exists and is defined over the rationals if and only if there are $\alpha, \beta, \gamma, \delta, \lambda \in \mathbb{Q}$ with

$$g'(x, z) = \lambda^2g(\alpha x + \beta z, \gamma x + \delta z).$$

Therefore, it is an isomorphism if and only if in addition to that $\alpha \delta - \beta \gamma \neq 0$. But this is exactly saying that $g$ and $g'$ are equivalent. \qed
1.3. Correspondence and invariants. For an elliptic curve of the form
\[ E_{A,B} : y^2 - x^3 + Ax + B, \]
define the quantities
\[ I(E) = -3A \]
\[ J(E) = -27B. \]

Also, for a quartic
\[ g(x) = ax^4 + bx^3 + cx^2 + dx + e \]
recall that the invariants \( I = 12ae - 3bd + c^2 \) and \( J = 72ace + 9bdc - 27ad^2 - 27eb^2 - 2c^3 \) generate the polynomial invariant ring for the action of \( GL_2(\mathbb{Z}) \) on the associated binary quartic form
\[ ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4, \]
for any \( a, b, c, d, e \in \mathbb{Z}. \)

**Proposition 1.5.** The set of elements in the 2-Selmer group of \( E/\mathbb{Q} \) is in bijection with the set of equivalence classes of locally soluble integral binary quartic forms having invariants \( \lambda^4I(E) \) and \( \lambda^6J(E) \) for some \( \lambda \in \mathbb{Q}. \)

**Proof.** Let \( C : y^2 - g(x) \) be a homogeneous space for \( E, \) with \( g(x) \) a quartic. We know that if \( g \) has a rational root, \( C \) is isomorphic to \( E \) over \( \mathbb{Q}. \) So in order to find the equation of \( E \) in terms of the invariants \( I, J \) of the quartic \( g \) (or more precisely, the binary quartic form \( g(x,y) \) associated to \( g \)), the idea is to assume \( g \) has a rational root and transform the quartic under equivalence to obtain an equation of the form
\[ y^2 - Ax^3 + Bx + C. \]
This is performed in ([SZ03] Prop. 7.28). We get:
\[ E : y^2 - x^3 - 27I - 27J. \]

Conversely, observe that under equivalence \( g \sim g', \) the invariants are related by
\[ I(g) - \lambda^4I(g') \]
\[ J(g) - \lambda^6J(g') \]
for some \( \lambda \in \mathbb{Q}. \) Hence for any 2-covering \( y^2 - g(x) \) of \( E, \) \( g \) has invariants \( \lambda^4I(E) \) and \( \lambda^6J(E). \) Finally, up to equivalence, we can always make sure that all the coefficients of a quartic are integers.

Let \( f \) be such an integral binary quartic form having invariants \( I \) and \( J. \) The following lemmas (lemmas 3.4.5 from [BSD63]) allow us to reduce the size of \( \lambda. \)

**Lemma 1.6.** If \( p \geq 5 \) is a prime such that \( p^4|I \) and \( p^6|J \) and if the equation \( y^2 - f(x,y) \) has a solution over \( \mathbb{Q}_p, \) then there exists an integral binary quartic form equivalent to \( f \) with invariants \( p^{-4}I \) and \( p^{-6}J. \)

**Lemma 1.7.** If \( 3^6|I \) and \( 3^4|J \) and the equation \( y^2 - f(x,y) \) has a solution over \( \mathbb{Q}_3, \) then there exists an integral binary quartic form equivalent to \( f \) with invariants \( 3^{-4}I \) and \( 3^{-6}J. \)

**Lemma 1.8.** If \( 2^6|I \) and \( 2^4|J \) and the equation \( y^2 - f(x,y) \) has a solution over \( \mathbb{Q}_2, \) then there exists an integral binary quartic form equivalent to \( f \) with invariants \( 2^{-4}I \) and \( 2^{-6}J. \)

We piece all these results together to obtain the following theorem.
3. The Average Rank of an Elliptic Curve

**Theorem 1.9.** Let \( E/Q \) be a fixed elliptic curve with invariants \( I \) and \( J \). The elements of the 2-Selmer group of \( E \) are in one-to-one correspondence with \( \text{PGL}_2(Q) \)-equivalence classes of locally soluble integral binary quartic forms having invariants \( 2^4I \) and \( 2^6J \).

**Proof.** Let \( f \) be a locally soluble integral binary quartic form with invariants \( \lambda^3I \) and \( \lambda^6J \). Without loss of generality, we can assume that \( \lambda \in 2\mathbb{Z} \), since we are always allowed to multiply by a square and stay in the same equivalence class.

By the previous lemmas, we can also assume that no prime greater than 3 divides \( \lambda \). Also, if 3 divides \( \lambda \), then \( 3^2|\lambda^3I \) and \( 3^3|\lambda^6J \) because \( I \) and \( J \) themselves are divisible by 3 (resp. \( 3^3 \)). We can thus ensure that 3 does not divide \( \lambda \). Finally, if \( 4|\lambda \), we can again use the third lemma. We end up with \( \lambda = 2 \). We conclude by observing that two integral binary quartic forms having the same invariants are equivalent if and only if they are \( \text{PGL}_2(Q) \)-equivalent. If \( f' = \mu^6(\gamma \cdot f) \), then on the one hand \( I(f') = \mu^4(\det \gamma)^3I(f) \) and on the other hand \( J(f') = \mu^6(\det \gamma)^6J(f) \). So \( \det \gamma^2 - 1/\mu^2 \) which completes the proof. \( \square \)

2. Counting integral binary quartic forms with bounded invariants

In the previous section, we have established a correspondence between elements in the 2-Selmer group and integral binary quartic forms, as well as their respective invariants. The next step is to count equivalence classes of such forms for bounded invariants. This section, based on ([BS10], 2), gives an outline of how this is done. We use the same notations, namely:

- \( V_2 \) denotes the \( \mathbb{R} \)-vector space of binary quartic forms;
- \( I \) and \( J \) are the usual polynomial invariants for a binary quartic form;
- \( \Delta = (4I^3 - J^2)/27 \) denotes its discriminant;
- the height of a binary quartic form is \( H(f) = H(I, J) = \max(||I||^3, ||J||^2/4) \);
- \( V_2 \) denotes the lattice in \( V_2 \) consisting of integral binary quartic forms and for \( i = 0, 1, 2 \), the set \( V_2^{(i)} \) consists of those forms having \( 4 - 2i \) roots in \( \mathbb{P}_1(\mathbb{R}) \).

The strategy is to first prove the following theorem:

**Theorem 2.1.** For any \( \text{GL}_2(\mathbb{Z}) \)-invariant \( S \subset V_2 \), if \( N(S, X) \) denotes the number of \( \text{GL}_2(\mathbb{Z}) \)-equivalence classes of irreducible elements \( f \in S \) with \( H(f) < X \) then:

\[
\begin{align*}
(1) \quad & N(V_2^{(0)}; X) = \frac{4\zeta(2)}{15}X^{5/6} + O(X^{3/4+\epsilon}); \\
(2) \quad & N(V_2^{(1)}; X) = \frac{32\zeta(2)}{135}X^{5/6} + O(X^{3/4+\epsilon}); \\
(3) \quad & N(V_2^{(2)}; X) = \frac{32\zeta(2)}{135}X^{5/6} + O(X^{3/4+\epsilon}).
\end{align*}
\]

We are ultimately interested in the average number of such forms, so we look at which pairs of invariants can actually occur, in the same way as for a quadratic form a discriminant is \( = 0, 1(4) \). We get:

**Theorem 2.2.** Let \( n_0 = 4, n_1 = 2 \) and \( n_2 = 2 \). Then

\[
\lim_{X \to \infty} \frac{N(V_2^{(2)}; X)}{|\{ (I, J) \text{ eligible: } H(I, J) < X, (-1)^i\Delta(I, J) > 0 \}|} = \frac{2\zeta(2)}{n_1}.
\]

To prove theorem 2.1, one needs to study the action of \( \text{GL}_2(\mathbb{Z}) \) on \( V_2 \):

- one computes a fundamental domain for the action of \( \text{GL}_2(\mathbb{Z}) \) on \( V_2 \);
- one would like to count integral points on this fundamental domain, however the domain is not compact and has a cusp at infinity.
the points corresponding to irreducible quartic forms are relatively rare in the cuspidal region and one succeeds by counting only these.

2.1. Fundamental domains for the action of $GL_2(\mathbb{Z})$. Let us first explicit fundamental domains for the action of $GL_2(\mathbb{R})$ on $V_2$. Clearly, $V_2^2$ can be partitioned into positive and negative definite forms, denoted $V_2^2^+$ and $V_2^2^-$.

**Lemma 2.3.** A fundamental set for the action of $GL_2(\mathbb{R})$ on $V_2^1$ can be constructed by choosing one form $f(I, J)$ for each pair of invariants such that $H(I, J) - 1$ and

\[
\begin{aligned}
\Delta(I, J) < 0 & \quad \text{if } i = 1 \\
\Delta(I, J) > 0 & \quad \text{otherwise}.
\end{aligned}
\]

**Proof.** First, fix invariants $I$ and $J$. If $\Delta < 0$, then the forms are in $V_2^1$, whereas if $\Delta > 0$ we land in one of the other three cases (cf. [Cre99]). Furthermore, one can see that $GL_2(\mathbb{R})$ is "large enough" to act transitively on the forms with invariants $I, J$ in each of the $V_2^2$. Conversely, two forms $f$ and $f'$ are equivalent only if there exists $\lambda > 0$ such that $I(f) = \lambda^2 I(f')$ and $J(f) = \lambda^3 J(f')$, since $I(\gamma f) = -\gamma^2 I(f)$ and $J(\gamma f) = -\gamma^3 J(f)$ for $\gamma \in GL_2(\mathbb{R})$. This is the same as requiring the existence of $\lambda$ such that $H(\lambda^2 I, \lambda^3 J) - 1$. Thus it suffices to pick one representative for each pair $(I, J)$ where the height is 1.

As fundamental subsets $L^1_\nu$ we may choose:

\[
\begin{aligned}
L^1_\nu = & \{ x^3 y - 1/3 xy^3 - t/27 y^4 : |t| \leq 2 \} \\
L^1_\nu^- = & \{ x^3 y - s/3 xy^3 = 2/27 y^4 : |s| \leq 1 \} \cup \{ x^3 y - 1/3 xy^3 - t/27 y^4 : |t| \leq 2 \} \\
L^2_\nu^+ = & \{ 1/16 x^4 - \sqrt[3]{2-t}/3 x^3 y + 1/2 x^2 y^2 + y^4 : |t| \leq 2 \} \\
L^2_\nu^- = & \{ f : -f \in L^2_\nu^+ \}.
\end{aligned}
\]

Note that these sets are compact subsets of $V_2$. Let now $\mathcal{F}$ denote the fundamental domain for the action of $GL_2(\mathbb{Z})$ on $GL_2(\mathbb{R})$ given as follows in the $N^\nu A'K\Lambda$-decomposition of $GL_2(\mathbb{R})$: 

\[
\mathcal{F} = \{ n\alpha k \lambda : n(u) \in N^\nu(t), \alpha(t) \in A', k \in K, \lambda \in \Lambda \}
\]

where $K = SO_2(\mathbb{R})$ and

\[
N^\nu(\alpha) = \left\{ \begin{pmatrix} 1 \\ u \\ 1 \end{pmatrix} : \det u = 1 \right\}, A' = \left\{ \begin{pmatrix} t^{-1} \\ 1 \end{pmatrix} : t \geq \sqrt{3}/2 \right\}
\]

and $\Lambda$ are the scalar matrices with positive entries and $\nu(\alpha)$ is a subset of $[-1/2^21/2]$. For details, see [PR94].

**Proposition 2.4.** For any $h \in GL_2(\mathbb{R})$, the number of irreducible integral forms in $\mathcal{F} h L^1_\nu$ with height less than $X$ is equal to $n_1 \cdot N(V_2; X)$, where $n_1 = 2$ and $n_1 = 4$ otherwise and where the points with $GL_2(\mathbb{Z})$-stabilizers of cardinality $2r \geq 4$ are counted with weight $1/r$.

Before we show this, consider the following 2 results, proven in ([BS10] 3.8):

**Lemma 2.5.** Let $f$ be an element in $V_2^1$ with nonzero discriminant. Then the order of the stabilizer of $f$ in $GL_2(\mathbb{R})$ is 4 if $i = 1$ and 8 otherwise.

**Lemma 2.6.** Let $h \in GL_2(\mathbb{R})$. The number of integral binary quartic forms of height $H < X$ whose stabilizer in $GL_2(\mathbb{Z})$ has size $\geq 2$ is $O(X^{3/4+\epsilon})$. 
In particular, the second lemma says that these exceptions do not occur too often.

**Proof of the proposition.** By the first lemma, an irreducible element has a stabilizer of order \(2^{n_i}\) in \(GL_2(\mathbb{R})\), with the notations of the proposition. But we see that \(\mathcal{F}hL_{L'}^i\) contains (as a multiset) \(m(x)\) copies of a \(GL_2(\mathbb{Z})\)-equivalence class \(x\) in \(V_2^i\), where

\[
m(x) = \frac{1}{n_i} \text{Stab}_{GL_2(\mathbb{R})}(x) / \text{Stab}_{GL_2(\mathbb{Z})}(x).
\]

We conclude, since the stabilizer in \(GL_2(\mathbb{Z})\) of a form always contains 1 and \(-1\) and hence \(m(x) \leq n_i\). \(\square\)

Unfortunately any single domain \(\mathcal{F}hL_{L'}^i\) is not compact anymore. The trick is to let \(h\) range over a certain compact subset \(G_0\) so as to facilitate counting in the part that goes off to infinity and then average out. This will be performed in the next section. It remains to say what happens with reducible forms.

**Proposition 2.7.** For any \(h \in G_0 \subset GL_2(\mathbb{R})\), \(G_0\) compact, the number of reducible integral binary quartic forms in \(\mathcal{F}hL_{L'}^i\) of height less than \(X\) and with non-trivial leading coefficient is \(O(X^{2/3+\epsilon})\) and the implied constant depends only on \(G_0\).

**Proof.** See ([BS10], 2.2). \(\square\)

### 2.2. Averaging over a compact

Let \(G_0\) be a fixed compact set in \(GL_2(\mathbb{R})\) with non-empty interior, \(K = SO_2(\mathbb{R})\)-invariant on the left, and such that every element in \(G_0\) has determinant at least 1. Observe that for any \(GL_2(\mathbb{Z})\)-invariant subset \(S \subset V_2^i\), we can express the number \(N(S, X)\) of irreducible \(GL_2(\mathbb{Z})\)-orbits in \(S\) with height less than \(X\) by averaging over \(G_0\):

\[
N(S, X) = \frac{\int_{h \in G_0} \frac{1}{n_i} \chi(x \in \mathcal{F}hL_{L'}^i \cap S^{\text{irr}} : H(x) < X) dh}{\int_{h \in G_0} dh},
\]

where \(S^{\text{irr}}\) denotes the irreducible elements in \(S\). This follows from our previous considerations, and it is also clear that the denominator is a constant \(C' > 0\). We compute the numerator.

**Lemma 2.8.** With the previous notations,

\[
N(S, X) = \frac{1}{C'} \int_{g \in \mathcal{F}} \frac{1}{n_i} \chi(x \in S^{\text{irr}} \cap gG_0L_{L'}^i : H(x) < X) dg.
\]

**Proof.** For \(x \in V_2^i\) let \(x'\) denote the unique point in \(L_{L'}^i\) that is \(GL_2(\mathbb{R})\)-equivalent to \(x\). We have

\[
N(S, X) = \frac{1}{C'} \sum_{x \in S^{\text{irr}}, H(x) < X} \int_{h \in G_0} \frac{1}{n_i} \chi(g \in \mathcal{F} : x = ghx') dh.
\]
If \( x \in S^{irr} \), there are a finite number of elements \( g_1, \ldots, g_n \in GL_2(\mathbb{R}) \) such that \( g_j x' = x \). So we get

\[
\int_{h \in G_0} \sharp \{ g \in \mathcal{F} : x - ghx' \} \, dh = \sum_j \int_{h \in G_0} \sharp \{ g \in \mathcal{F} : gh = g_j \} \, dh - \sum_j \int_{h \in G_0 \cap \mathcal{F}^{-1} g_j} \, dh
\]

\[
- \sum_j \int_{g \in G_0 \cap \mathcal{F}^{-1}} \, dg \quad (dh \text{ is } GL_n(\mathbb{R}) \text{-invariant})
\]

\[
- \sum_j \int_{g \in \mathcal{F}} \sharp \{ h \in G_0 : gh = g_j \} \, dg
\]

\[
- \int_{g \in \mathcal{F}} \sharp \{ h \in G_0 : x - ghx' \} \, dg.
\]

And so by replacing in equation 7 the result follows. \( \square \)

Under the decomposition \( N''A'KA \), we rewrite

\[(8)\]

\[N(S; X) = \frac{1}{C_t} \int_{N''(t)A''A} \sharp \{ x \in S^{irr} \cap \alpha(t) \lambda kG_0L_V^1 : H(x) < X \} t^{-2}d\nu \, d\lambda \, d\alpha \]

where \( K \) is a constant that bounds the absolute value of the leading coefficient on all \( G_0L_V^1 \).

\[N(S; X) = \frac{1}{C_t} \int_{g \in N''(t)A''A} \sharp \{ x \in S^{irr} \cap B(n, t, \lambda, X) \} t^{-2}d\nu \, d\lambda \, d\alpha \]

for \( B(n, t, \lambda, X) = \alpha(t) \lambda kG_0L_V^1 \cap \{ x \in V_Z^1 : H(x) < X \} \). We need the following estimate for the number of points in \( B(n, t, \lambda, X) \).

**Lemma 2.9.** The number of points of \( G_0L_V^1 \) that end up in \( B(n, t, \lambda, X) \) with non-trivial leading coefficient is

\[
\begin{cases}
0 & \text{if } C\lambda/t < 1; \\
\frac{\text{Vol}(B(n, t, \lambda, X)) + O(\max\{C^4t^4\lambda^16, 1\})}{\text{Vol}(B(n, t, \lambda, X))} & \text{otherwise,}
\end{cases}
\]

where \( C \) is a constant that bounds the absolute value of the leading coefficient on all \( G_0L_V^1 \).

**Proof.** This follows from a result by Davenport ([Dav64]). See ([BS10] Prop. 2.5) and the ensuing discussion. \( \square \)

We finally prove:

**Proposition 2.10.** Let \( R_X(hL_V^1) \) denote the integral elements in \( \mathcal{F}hL_V^1 \) of height \( H < X \), where \( h \in G_0 \). Then

\[N(V_Z^1; X) = \text{Vol}(R_X(L_V^1))/n_i + O(X^{3/4+\varepsilon}).\]

**Proof.** First of all, note that the previous lemma does not count elements that verify the assumptions of proposition 2.7. Hence we work up to an error of \( O(X^{3/4+\varepsilon}) \). Also, since elements in \( G_0L_V^1 \) have heights of at least one by definition, and that the matrix that acts on them has determinant \( \lambda^2 \), we see that if we want to end up in \( B(n, t, \lambda, X) \), we need \( \lambda < X^{1/24} \). Now use the previous lemma and equation (9) to write \( N(V_Z^1; X) \cdot C^t \) as

\[
\int_{X^{1/24}}^{X^{1/4}} \int_{\sqrt{\lambda}/2}^{C^t\lambda} \int_{N''(t)} \left( \frac{\text{Vol}(B(n, t, \lambda, X)) + O(\max\{C^4t^4\lambda^{16}, 1\})}{\text{Vol}(B(n, t, \lambda, X))} \right) t^{-2}d\nu \, d\lambda \, d\alpha.
\]
The second term in the integral gives

$$\int_{X^{1/4}}^{X^{1/2}} O(\lambda^{19}) d\lambda = O(X^{3/4}).$$

On the other hand, the first summand is

$$\int_{G_0} \text{Vol}(R_X(hL^i)) dh - O\left(\int_{X^{1/4}}^{X^{1/2}} \int_{\mathcal{N}(t)} \text{Vol}(B(n,t,\lambda,X)) t^{-2} d\nu d\tau d\lambda \right).$$

Since \(\text{Vol}(R_X(hL^i))\) is independent of \(h\), the left term is just equal to

$$C^i n_i \text{Vol}(R_X(L^i_V)).$$

It remains to show that the second term is \(O(X^{3/4+\epsilon})\). An element in \(\Lambda\) acts on \(G_0 L\) by multiplying each coefficient of \(ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4\) by \(\lambda^i\). Thus we see that \(\text{Vol}(B(n,t,\lambda,X))\) is \(O(\lambda^{20})\). Then \(\int_{\mathcal{N}(t)} O(\lambda^{20}) t^{-2} d\nu d\tau d\lambda\) is \(O(\lambda^{19})\) and the whole term is again \(O(X^{3/4})\).

2.3. Proof of the main results. We first prove theorem 2.1. By proposition 2.10, it remains to compute the volume of \(R_X(L^i_V)\). Let

$$R^i_V = \Lambda L^i_V.$$ 

Then \(R^i_V\) is in one-to-one correspondence with the set of pairs \((I,J) : I^3 - J^2/4 > 0\) if \(i \neq 1\) and \((I,J) : I^3 - J^2/4 < 0\) if \(i = 1\). On these sets, there is a natural measure \(dI dJ\) so there is a natural measure on \(R^i_V\) which we also denote \(dI dJ\). Furthermore, if \(R^i_V(X)\) denotes the elements of \(R^i_V\) with height less than \(X\), we get

$$\text{Vol}(R_X(L^i_V)) = \text{Vol}(\mathcal{F}_{SL_2} \cdot R^i_V(X)),$$

where \(\mathcal{F}_{SL_2}\) denotes the fundamental domain for \(SL_2(\mathbb{Z})\) on \(SL_2(\mathbb{R})\) obtained by setting \(\lambda = 1\) in \(\mathcal{F}\). The following lemma allows us to use the natural measure on \(R^i_V\) for the computation of \(\text{Vol}(\mathcal{F}_{SL_2} \cdot R^i_V(X))\).

**Lemma 2.11.** For any measurable function \(\phi\) on \(V^*_2\), we have

$$\frac{2}{27 n_i} \int_{R^i_V} \int_{SL_2(\mathbb{R})} \phi(g \cdot p_{I,J}^i) dgdIdJ - \int_{V^*_2} \phi(v) dv,$$

where \(p_{I,J}^i\) is a point in \(R^i_V\) having invariants \(I\) and \(J\). Note that by definition of \(L^i_V\), there is at most one such element. Also, \(d\nu\) denotes the measure on \(SL_2(\mathbb{R})\) coming from the \(\text{NAN}\) decomposition.

**Proof.** This follows from Proposition 2.8 in [BS10].

We apply this lemma to the measurable function \(n_i^{-1} \cdot 1_{\mathcal{F}_{SL_2} R^i_V(X)}\) to get:

$$\text{Vol}(\mathcal{F}_{SL_2} \cdot R^i_V(X)) = \frac{2}{27} \int_{R^i_V(X)} \int_{\mathcal{F}_{SL_2}} dgdIdJ,$$

where the factor \(n_i\) disappears because \(V^*_2\) is covered by \(n_i\) copies of \(SL_2(\mathbb{R}) \cdot R^i_V\). Then there is the result:

**Lemma 2.12.**

$$\int_{\mathcal{F}_{SL_2}} dg = \zeta(2).$$

**Proof.** This is a classical result, since \(\int_{\mathcal{F}_{SL_2}} dg\) is the volume of the fundamental domain for the modular group. See ([PR94] 4.6) or ([Ser77] 7).

Finally, theorem 2.1 follows form the following result and proposition 2.10.
Proposition 2.13.

\[
\text{Vol}(R_X(L^1_V)) = \left\{ \begin{array}{ll}
\frac{16}{135} \zeta(2)X^{5/6} & i = 0, 2+,-2- \\
\frac{64}{135} \zeta(2)X^{5/6} & i = 1.
\end{array} \right.
\]

Proof. It remains to evaluate the integral \( \int_{R^1_V} dI dJ \). If \( i = 0, 2+, -2- \), it becomes

\[
\int_{-1}^{1/3} \int_{-1}^{1/3} dI dJ - \int_{-1}^{1/3} 4I^{3/2} dI - 8/5X^{5/6}.
\]

If \( i = 1 \), then this time \( I^3 - J^2/4 < 0 \) and we get

\[
\int_{R^1_V} dI dJ = 32/5X^{5/6}.
\]

As for theorem 2.2, it follows from theorem 2.1 and the following proposition.

Proposition 2.14. The number of pairs \((I, J)\in\mathbb{Z}\times\mathbb{Z}\) that are eligible and have bounded height \(H(I, J) < X\) are, respectively:

\[
\left\{ \begin{array}{ll}
\frac{8}{135} X^{5/6} + O(X^{1/2}) & \text{if } \Delta(I, J) > 0 \\
\frac{32}{135} X^{5/6} + O(X^{1/2}) & \text{if } \Delta(I, J) < 0.
\end{array} \right.
\]

Proof. See Proposition 2.10 in [BS10].

3. The remainder of the proof

We have established a correspondence between the 2-Selmer group and \(PGL_2(\mathbb{Q})\)-equivalence classes of locally soluble quartic forms. Then in the previous section, we counted \(GL_2(\mathbb{Z})\)-equivalence classes of such (irreducible) quartics. However, putting these two results together to prove the theorem is the most technical part. For a better overview, we give an outline of the remaining steps. Then in the last and final section, we highlight some of the deeper results behind the proofs omitted here.

3.1. From \(PSL_2(\mathbb{Q})\) to \(GL_2(\mathbb{Z})\). From now on, we consider a slightly different action of \(GL_2(R)\) on \(V_R\), \(R\) a ring. Namely

\[
\gamma \cdot f(x, y) = \frac{1}{\det(\gamma)^2} f((x, y) \cdot \gamma).
\]

Under this definition, the action descends to \(PGL_2(R)\). First of all, it is useful to consider only the cases where \(E\) has automorphism group \(\mathbb{Z}/2\mathbb{Z}\), when the elliptic curve is called rigid. This occurs when \(I(E)\) and \(J(E)\) are non-zero (see [Sil09] 3.10). Then one can check that in this case, analogously to our results in the first section, if we consider soluble 2-coverings instead of locally soluble ones, we end up with a bijection

\[
E(K)/\mathbb{Z} \leftrightarrow \text{(soluble } K\text{-equivalence classes of quartics)},
\]

once we fix invariants \(I\) and \(J\) for both. By soluble quartic we mean that the equation \(z^2 - f(x, y)\) has a solution in \(\mathbb{F}^2(K)\), where \(K\) is a field. The following result holds:

Lemma 3.1. Let \(E/K\) with nonzero invariants. Let \(f\) be a \(K\)-equivalence class of binary quartic forms corresponding to an element in \(E(K)/2E(K)\). Then the size of the stabilizer of \(f\) in \(PGL_2(K)\) is \(\#E(K)[2]\).

Thus it makes sense to consider only those curves that have no rational 2-torsion:
Lemma 3.2. The total number of elements in the union of the 2-Selmer groups of all \( E/\mathbb{Q} \) having non-trivial rational 2-torsion and height bounded by \( X \) is \( O(X^{3/4}) \).

This is proved by counting the reducible cubic forms with integer coefficients (Lemma 3.3 in [BS10]). By counting only curves with \( IJ = 0 \) in the previous section one can also prove:

Lemma 3.3. The number of total elements in the union of 2-Selmer groups of non-rigid elliptic curves \( E/\mathbb{Q} \) of height bounded by \( X \) is \( O(X^{3/4}) \).

Because we average over a number of curves that is \( O(X^{5/8}) \), we can ignore these cases.

If \( F \) is a set of elliptic curves, denote by \( F^{\text{inv}} \) the set of invariants \([I(E), J(E)) : E \in F]\) and denote \( F^p \) the \( p \)-adic closure in \( \mathbb{Z}_p \times \mathbb{Z}_p \). Also, for any invariants \((I, J)\), if \( C_1, \ldots, C_k \) is a set of \( \text{PGL}_2(\mathbb{Q}) \)-orbits on the set of integral binary quartic forms having invariants \( I \) and \( J \), there is a maximal subset \( C_1, \ldots, C_i \) of \( \text{PGL}_2(\mathbb{Q}) \)-inequivalent classes. Denote by \( S^I \) the union of integral binary quartic forms in these \( C_i \). Also denote by \( SF \) the union of \( S^I \) for \((I, J) \in F^{\text{inv}} \). To prove the theorem, we need to be able to compute the size of such an \( SF \). We compute it locally first. For this purpose, let \( S^F \) denote the \( p \)-adic closure of \( SF \) in \( \mathbb{V}_p \).

Proposition 3.4. The \( p \)-adic density \( \mu_p(S^F_p) \) is \( [2^{10}/3]^3_p \cdot M_p(V, F) \), where

\[
M_p(V, F) = 1 - 1/2^2 \int_{F_p^{\text{inv}}} \sum_{E_{1,2} \in E_{1,2}} \frac{1}{\nu_{E_{1,2}}^2} \text{d}I\text{d}J.
\]

Proof. We give a sketch of the proof. Define

\[
B^F_p = \cup_{(I, J) \in F_p^{\text{inv}}} \text{PGL}_2(\mathbb{Z}_p) \cdot B^I_{p, J},
\]

where \( B^I_{p, J} \) is a set of representatives for the action of \( \text{PGL}_2(\mathbb{Z}_p) \) on the set of soluble binary quartic forms in \( \mathbb{V}_p \) with invariants \( 2^4 I \) and \( 2^6 J \). The set \( B^F_p \) is almost \( S^F_p \):

\[
\int_{S^F_p} \frac{1}{\nu_{E_{1,2}}^2} \text{d}I\text{d}J = \int_{B^F_p} \frac{1}{\nu_{E_{1,2}}^2} \text{d}I\text{d}J.
\]

Now, similarly as in 2.11, a change of variable yields

\[
\int_{B^F_p} \frac{1}{\nu_{E_{1,2}}^2} \text{d}f = |C|_p \text{Vol(PGL}_2(\mathbb{Z}_p)) \int_{F_p^{\text{inv}}} \sum_{E_{1,2} \in E_{1,2}} \frac{1}{\nu_{E_{1,2}}^2} \text{d}I\text{d}J.
\]

The constant \( C \) is \( 2^{10}/27 \), because the invariants are \( 2^4 I \) and \( 2^6 J \) as opposed to \((I, J)\) in lemma 2.11. Again, we can disregard the case where \( I \) or \( J \) is trivial since here it is a set of measure 0. Then we have seen that \( \frac{1}{2} \text{Stab}_{\text{PGL}_2(\mathbb{Q}_p)}(f) = \frac{1}{2} E(\mathbb{Q})[2] \). Finally, one checks that the volume of \( \text{PGL}_2(\mathbb{Z}_p) \) with respect to the \( \mathbb{Q} \)-adic decomposition of \( \text{PGL}_2(\mathbb{Q}_p) \) is \( 1 - 1/p^2 \) if \( p \geq 3 \) and \( 2(1 - 1/4) \) if \( p = 2 \), so that either way the proposition holds.

The quantity \( M_p(V, F) \) may be thought of as the mass of all isomorphism classes of soluble 2-coverings over \( \mathbb{Q}_p \).

The proof suggests that the case where two forms \( f \) and \( f' \) are \( \text{PGL}_2(\mathbb{Q}_p) \)-equivalent, but not \( \text{PGL}_2(\mathbb{Z}_p) \)-equivalent is relatively rare. Also, we are ultimately interested in locally soluble forms. Thus if \( f \in \mathbb{V}_p \) is not \( \mathbb{Q}_p \)-soluble or if \( \exists f' \) such that the forms \( f \) and \( f' \) are \( \text{PGL}_2(\mathbb{Q}_p) \)-equivalent, but not \( \text{PGL}_2(\mathbb{Z}_p) \)-equivalent, we say that \( f \) is bad at \( p \).
3. THE REMAINDER OF THE PROOF

Thus the following proposition is crucial. For remarks on the proof, see the next section.

**Proposition 3.5.** The number of $\text{PGL}_2(\mathbb{Z})$-equivalence classes in $V_\mathbb{Z}$ that are bad at $p$ and have height less than $X$ is $O(X^{5/3}/p^{5/3})$, where the implied constant does not depend on $p$.

### 3.2. The proof of the theorem.

As for this part, we use the following height for elliptic curves:

$$H'(E) = \max(|H(E)|^3, |J(E)|^2/4) - 27/4H(E).$$

Furthermore, for us $F$ will denote the set of all elliptic curves defined over $\mathbb{Q}$.

**Remark.** In fact, Bhargava defined a notion of large set of elliptic curves, over which all the subsequent results still hold if $F$ is such a large set.

Finally, let $M_p(U_1, F)$ denote the proportion of pairs in $F_p^{\text{inv}}$ i.e

$$M_p(U_1, F) = \int_{(I, J) \in F_p^{\text{inv}}} dIdJ$$

where $dIdJ$ is such that $\mathbb{Z}_p \times \mathbb{Z}_p$ has mass one. Let us compute the product of the local masses:

**Proposition 3.6.** We have

$$\prod_p \frac{M_p(V, F)}{M_p(U_1, F)} = \frac{2}{\zeta(2)}.\]"
PROPOSITION 3.8. Let \( N_\mathbb{Q}(S^F, X) \) denote the number of \( \text{PGL}_2(\mathbb{Q}) \)-equivalence classes of locally soluble irreducible binary quartic forms having invariants \( 2^4 I \) and \( 2^J \), where \((I, J) \in F^{mn} \) and \( H(I, J) < X \). Then

\[
N_\mathbb{Q}(S^F, X) = N(V_2^0 \cup V_2^{2+} \cup V_2^1, X) \prod_p \mu_p(S^F) + o(X^{5/6}).
\]

PROOF. (Note: this proof will be corrected soon...) Let us compute \( N_\mathbb{Q}(S^F \cap V_2^1, X) \). Let \( \nu_p(S_F) \) denote the elements which are \( \mathbb{Q}_p \)-soluble. We have for a fixed positive integer \( n \):

\[
N((\cap_{p < n} \nu_p(S^F)) \cap V_2^1, X) = N(V_2^1, X) \prod_{p < n} \mu_p(S^F) + O(X^{3/4}),
\]

since there are finitely many primes and finitely many congruence conditions and so we can use the previous proposition. Letting \( n, X \to \infty \), we obtain an upper bound:

\[
\limsup_{X \to \infty} \frac{N(\nu(S^F) \cap V_2^1, X)}{X^{5/6}} = \frac{N(V_2^1, X) \prod_{p < n} \mu_p(S^F)}{X^{5/6}},
\]

where \( \nu(S^F) \) denotes the locally soluble elements. For a lower bound, observe that

\[
\cap_{p < n} \nu_p(S^F) \subset (\nu(S_F) \cup \bigcup_p (S^F \setminus \nu_p(S^F))).
\]

Hence

\[
\lim_{X \to \infty} \frac{N(\nu(S^F) \cap V_2^1, X)}{X^{5/6}} \geq \frac{N(V_2^1, X) \prod_{p < n} \mu_p(S^F)}{X^{5/6}} + O(\sum_{p \geq n} p^{-5/3}),
\]

by the uniformity estimate of proposition 3.5. Letting \( n \to \infty \) again we get:

\[
N(\nu(S^F) \cap V_2^1, X) = N(V_2^1, X) \prod_p \mu_p(S^F) + o(X^{5/6}).
\]

We conclude, since we do not need to consider \( N(\nu(S^F) \cap V_2^{2-}, X) \).

Via the same procedure, one proves:

PROPOSITION 3.9. \( \sharp \{ E \in F : H'(E) < X \} = \sharp \{ (I, J) : H'(I, J) < X \} \prod_p \mu_p(F_p^{mn}) + o(X^{5/6}) \).

Note that this requires another uniformity estimate ([BS10], 3.18). Define the sets

\[
R^+_X = \{ (i, j) \in \mathbb{R}^2 : |i| < X^{1/3}, |j| < 2X^{1/2}, 4i^3 - j^2 > 0 \}
\]

and

\[
R^-_X = \{ (i, j) \in \mathbb{R}^2 : |i| < X^{1/3}, |j| < 2X^{1/2}, 4i^3 - j^2 < 0 \}.
\]

We now prove the theorem.

PROOF OF THEOREM 0.6. We want to show

\[
\lim_{X \to \infty} \frac{\sum_{H'(E) \leq X} (S(E)^2 - 1)}{\sharp \{ E : H'(E) < X \}} = 2.
\]

In fact, the theorem holds for any "large enough" set \( F \) of elliptic curves, but as mentioned before, here \( F \) stands for the set of all elliptic curves over \( \mathbb{Q} \). The numerator on the left is just \( N_\mathbb{Q}(S^F, 2^{12}X) \), since the correspondence between elements in the 2-Selmer group and \( \text{PGL}_2(\mathbb{Q}) \)-equivalence classes of quartics multiplies the invariants by \( 2^4 \) and \( 2^9 \), respectively, and so the height is multiplied by \( 2^{12} \). Also,
4. Remarks on the proof

In this section, we talk about some elements of the proof which were omitted here and about how this result fits into the context of Bhargava’s higher composition laws. In the first paper of the "higher composition laws" series [Bha04a], one of the main reasons why the results are so beautiful is that quadratic rings (i.e. rings that have rank 2 as \( \mathbb{Z} \)-modules) are parametrized by their discriminant and so orders in quadratic and cubic fields are easy to parametrize. Naturally, the question is whether there is a similar description for cubic and quartic rings (i.e. \( \mathbb{Z} \)-modules of ranks 3, 4). This is discussed in the third paper of the series [Bha04c]. For cubic rings, there is the result:

**Proposition 4.1.** Up to isomorphism, cubic rings are parametrized by \( GL_2(\mathbb{Z}) \)-equivalence classes of integral binary cubic forms.

This was already established by Delone-Fadeev in [DF64]. However, because of increasing complexity, a similar approach for quartic rings fails and so Bhargava introduces the notion of resolvent rings.
4.1. Cubic resolvent rings. Let $R$ be a ring of rank $k$ over $\mathbb{Z}$. Similarly as for fields, define the trace of an element $\alpha \in R$ to be the trace of the multiplication-by-$\alpha$ endomorphism $m_\alpha$. Also, define the discriminant of $\alpha$ to be the discriminant of the characteristic polynomial of $m_\alpha$. Finally, define the discriminant of the ring:
$$\text{Disc}(R) = \det(\text{Tr}(\alpha_i \alpha_j)),$$
where $\{\alpha_1, \ldots, \alpha_k\}$ is a $\mathbb{Z}$-basis of $R$. We need an analogue of Galois closure for such rings:

**Definition.** The $S_k$-closure of the ring $R$ of rank $k$ is the ring $\bar{R}$ given by the quotient $R^{\otimes k}/J_R$, where $J_R = \{r \in R^{\otimes k} : nr \in I_R$ for some $n \in \mathbb{Z}\}$ and $I_R$ is the ideal in $R^{\otimes k}$ generated by all elements of the form
$$(x \otimes 1 \otimes \ldots \otimes 1) + (1 \otimes x \otimes \ldots \otimes 1) + \cdots + (1 \otimes 1 \otimes \ldots \otimes x) - \text{Tr}(x)$$
for $x \in R$. Note that $\text{Tr}(x)$ really denotes $\text{Tr}(x)(1 \otimes \ldots \otimes 1)$.

The symmetric group $S_k$ acts naturally through automorphisms on $\bar{R}$. Moreover, the subring of elements fixed by this action is $\mathbb{Z}$, which justifies the terminology. Let now $Q$ be a quartic ring. We would like to have a cubic ring $R$, together with a map $\phi : Q \rightarrow R$ that preserves discriminants of elements. Such a map is given by
$$\tilde{\phi} : x \mapsto x' + x'' x''',$n
where $x, x', x'', x'''$ denote the conjugates of $x$ in the $S_4$-closure $\bar{Q}$ of $Q$. One verifies that all the elements $\tilde{\phi}(x)$ indeed lie in one single cubic ring, and this leads us to define the cubic invariant ring
$$R^{\text{inv}}(Q) = \mathbb{Z}[\tilde{\phi}(x) : x \in Q].$$

**Definition.** A cubic resolvent ring of $Q$ is a cubic ring $R$ such that $\text{Disc}(Q) = \text{Disc}(R)$ and $R^{\text{inv}}(Q) \subseteq R$.

There is the following result:

**Proposition 4.2.** Every quartic ring has a cubic resolvent ring. Furthermore, a maximal quartic ring has a unique resolvent ring.

With these definitions, one again gets a nice correspondence:

**Theorem 4.3.** There is a canonical bijection between the set of $\text{GL}_3(\mathbb{Z}) \times \text{GL}_3(\mathbb{Z})$-orbits on the space of pairs of integral ternary quadratic forms and the set of isomorphism classes of pairs $(Q, R)$, where $Q$ is a quartic ring and $R$ is a cubic resolvent ring.

**Proof.** This is one of the main theorems of [Bha04c].

4.2. Monogenicity and binary quartic forms. We would like to count binary quartic forms. It is therefore useful to establish a link with orders in number fields so as to have a better understanding of these objects.

**Definition.** A cubic ring is said to be monogenic if it is generated by a single element as a $\mathbb{Z}$-algebra. A monogenized cubic ring is a pair $(C, x)$ consisting of a monogenic cubic ring $C$ and a generator $x$. A monogenic cubic field is a field whose ring of integers is monogenic.

Over a principal ideal domain $R$, a monic binary cubic form $g(X, Y)$ gives rise to a monogenized cubic ring via the quotient
$$R[X]/g(X, 1).$$
We identify monogenized cubic rings $(C, x)$ and $(C', x')$ if there is an isomorphism $\phi : C \rightarrow C'$ such that $\phi(x) = x' + u$ for some $u \in R$. On the other hand, a
monogenized cubic ring \((C, x)\) yields a monic binary cubic form: the characteristic polynomial of multiplication-by-\(x\). So we get:

**Proposition 4.4.** There is a bijection between \(N_R\)-orbits on the space of monic binary cubic forms and monogenized cubic rings over \(R\), where

\[
N_R = \left\{ \left( \frac{1}{u} \right) \ ; u \in R \right\}.
\]

Note that under this action, a monic cubic form \(g(X, Y) = X^3 + rX^2 + sXY^2 + tY^3\) again has two polynomial invariants \(I\) and \(J\):

\[
I = r^2 - 3s, \\
J = -2r^3 + 9rs - 27t.
\]

Having established this, among others one gets the following result:

**Theorem 4.5 (Wood [Woo09]).** There is a canonical bijection between \(GL_2(\mathbb{Z})\)-equivalence classes of integral binary quartic forms and isomorphism classes of pairs \((Q, C)\) where \(Q\) is a quartic ring (over \(\mathbb{Z}\)) and \(C\) is a monogenized cubic resolvent ring of \(Q\).

If we restrict this result to maximal orders and denote by \(Cl^*_2\) the 2-torsion subgroup in the (narrow) class group as well as the respective duals by \((Cl^*_2)^*\) we get the desired result:

**Theorem 4.6 (Theorem 3.10 [BS10]).** Let \(g\) be an irreducible monic integral binary cubic form having invariants \(I\) and \(J\) such that the corresponding cubic ring \(C - \mathbb{Z}[X]/g(x)\) is maximal.

1. If \(4I^3 - J^2 > 0\) there is a canonical bijection between \(Cl^*_2(C)^*\) and \(GL_2(\mathbb{Z})\)-equivalence classes of integral binary quartic forms of invariants \(I\) and \(J\).
2. If \(4I^3 - J^2 < 0\) there is a canonical bijection between elements of \(Cl_2(C)^*\) and \(GL_2(\mathbb{Z})\)-equivalence classes of integral binary quartic forms having invariants \(I\) and \(J\).

In particular, the theorem shows that if \(I\) and \(J\) occur as invariants of a maximal monogenic cubic ring \(C\), the set of \(GL_2(\mathbb{Z})\)-equivalence classes of integral binary quartic forms with such invariants is naturally an elementary abelian 2-group!

### 4.3. Maximality

Remark that a cubic ring \(C\) (and similarly for a quartic ring) is maximal if and only if for all primes \(p\) it is maximal at \(p\), meaning that \(C \otimes \mathbb{Z}_p\) is the maximal cubic ring over \(\mathbb{Z}_p\) contained in \(C \otimes \mathbb{Q}_p\). We also say that a pair \((Q, C)\) consisting of a quartic ring and a cubic resolvent ring is strongly maximal (at \(p\)) if both \(Q\) and \(C\) are maximal (at \(p\)). To quantify the failure of maximality, the idea is therefore to start with local considerations. Namely, a binary quartic form \(f\) defines four points in \(\mathbb{P}^1_{\mathbb{F}_p}\) by looking at the roots of the reduced form modulo \(p\). Hence define a symbol:

\[
(f, p) = (f_1^{e_1}, f_2^{e_2}, \ldots),
\]

where \(f_i\) indicates the degree of the field of definition of the \(i\)-th root over \(\mathbb{F}_p\) and \(e_i\) is the multiplicity of the root. The symbol \((f, p)\) thus contains information about the splitting behaviour of the corresponding quartic ring at \(p\). Then one looks at which symbols give maximal rings and computes local densities for each possible occurring symbol. This is performed in ([BS10] 3.5). All of these considerations then facilitate the proof of some results that were needed throughout the proof of the average rank of the 2-Selmer group, see for instance the proof of lemma 2.6 in ([BS10] 3.8).
4.4. Uniformity estimates. Finally, the last element needed is an uniformity estimate. Let $\mathcal{W}_p(V)$ denote the elements in $V_2$ (integral binary quartic forms) which are not strongly maximal at $p$, meaning that the corresponding pair $(Q,C)$ consisting of quartic ring and cubic resolvent ring isn’t strongly maximal at $p$. Bhargava and Shankar prove:

**Proposition 4.7** (Prop 3.18 [BS10]). If $N(\mathcal{W}_p(V); X)$ denotes the not strongly maximal forms of height bounded by $X$ then

$$N(\mathcal{W}_p(V); X) = O(X^{5/6}/p^{5/3}),$$

where the implied constant is independent of $p$.

To prove this estimate, it isn’t enough to consider monogenized cubic fields. Thus Bhargava defines submonogenized cubic fields.

**Definition.** A submonogenized cubic field of index $n$ is a field $K$ such that the ring of integers $R$ of $K$ is a cubic ring, together with an element $x \in R$ such that $x$ generates a subring of index $n$ in $R$.

In particular, monogenized cubic fields are submonogenized of index 1. Then in section 4 of [BS10], essentially the same procedure as for monogenized cubic rings is carried through under this more general setting, which finally ends up proving the desired estimate. Now recall the following result that we used in the proof (proposition 3.5):

**Proposition.** The number of $PGL_2(\mathbb{Z})$-equivalence classes in $V_2$ that are bad at $p$ and have height less than $X$ is $O(X^{5/6}/p^{5/3})$, where the implied constant does not depend on $p$.

It turns out that this result is merely a restatement of the uniformity estimate above, namely the bad equivalence classes are not maximal! See the proof of proposition 5.13 in [BS10]. Once we have remarked this, we can answer the question of how big the set of elliptic curves $F$ that we average over has to be so that the same results hold:

**Definition.** Let $F$ be a set of elliptic curves over $\mathbb{Q}$. We say that $F$ is large at a prime $p$ if the set of all monogenized cubic rings over $\mathbb{Z}_p$ having invariants equal to $(I,J) \in F^{inv} (\mathbb{Z}_p) \times F^{inv} (\mathbb{Z}_p)$ contains all the maximal monogenized cubic rings over $\mathbb{Z}_p$. The set $F$ is large if large at cofinitely many primes.

Note that of course the set of all elliptic curves is large. In particular, the uniformity estimate above still holds and Bhargava in fact proved the following stronger theorem.

**Theorem 4.8.** When elliptic curves $E$ in any large family are ordered by height, the average size of their 2-Selmer groups is 3.
Bibliography


[Har77] Robin Hartshorne, Algebraic geometry, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52. MR 0463157 (57 #3116)


[Mil09] , Algebraic geometry (v5.20), 2009, Available at www.jmilne.org/math/, pp. 239+vi.


