Saturation of Mordell-Weil Groups of Elliptic Curves over Number Fields

by Martin Prickett, M.A., M.Sc.

Thesis submitted to the University of Nottingham for the degree of Doctor of Philosophy, January 2004

Contents

Abstract

Given a subgroup B of a finitely-generated abelian group A, the saturation $\overline{B}$ of B is defined to be the largest subgroup of A containing B with finite index.

In this thesis we consider a crucial step in the determination of the Mordell-Weil group of an elliptic curve, $E(K)$. Methods such as Descent may produce subgroups H of $E(K)$ with $[\overline{H} : H] > 1$. We have determined an algorithm for calculating $\overline{H}$ given H, and hence for completing the process of finding the Mordell-Weil group. Our method has been implemented in MAGMA with two versions of the programs; one for general number fields K and the other for $\mathbb{Q}$. It builds upon previous work by S. Siksek.

Our problem splits into two. First we can use geometry of numbers arguments to establish an upper bound N for the index $[\overline{H} : H]$. Second for each remaining prime $p < N$ we seek to prove either that H is $p-$saturated, i.e. $p \nmid [\overline{H} : H]$, or to enlarge H by index p.

To solve the first problem,

1. We have devised and implemented an algorithm that searches for points on $E(K)$ up to a specified naive height bound.

2. We have devised and implemented an algorithm that calculates the subgroup $E_{gr}(K)$ of points with good reduction at specified valuations.

3. We have implemented joint work with S. Siksek and J. Cremona to calculate an upper bound on the difference of the canonical and naive height of points on an elliptic curve.

4. We have helped to devise and have implemented joint work with S. Siksek and J. Cremona to calculate a lower bound on the canonical heights of non-torsion points on $E(K)$ with K a totally real field.

To solve the second problem,

1. As in earlier work by Siksek, we use homomorphisms to prove $p-$saturation for primes p. We however use the Tate-Lichtenbaum pairing, and we show that, using this pairing, our method will always prove H is $p-$saturated if that is the case.

2. We show that Siksek's original method will fail for some curves.

Acknowledgements

I am indebted to my supervisor, John Cremona, for assistance, inspiration, and for suggesting the topic of the thesis to me. I would also like to thank Samir Siksek for his help and for our cooperative work. Thanks are due to the EPSRC and GCHQ for their financial support.

Finally, I would like to thank my parents for their patience and encouragement.

Chapter 1

Introduction

Given a subgroup B of a finitely-generated abelian group A, the saturation $\overline{B}$ of B is defined to be the largest subgroup of A containing B with finite index. This thesis considers the problem of saturation in the group $A = E(K)$, the Mordell-Weil group of an elliptic curve E defined over a number field K and where B is the subgroup generated by the known points on the curve. The context of our problem is, for example, when computing $E(K)$ by 2-descent, where we normally obtain a set of independent points which generate a subgroup of $E(K)$ of finite (odd) index, and wish to extend to a basis for the full group $E(K)$. For many curves of high rank, however, the exact rank is unknown and we just have sets of independent points which we know lie on the given curve. Our method is flexible enough to calculate the saturation in this case, despite the saturation not being all of $E(K)$.

The problem divides into two parts, which have involved approximately equal effort in this thesis: first to determine an upper bound N for the index $n = [\overline{B} : B]$, and second to decide, for each prime p less than N, whether or not B is p-saturated (in the obvious sense.)

We give a set of techniques for solving the first problem, all using geometry of numbers arguments, and most searching for points of low naive heights on elliptic curves. Some of these methods rely on working with the points of good reduction at subsets of the set of valuations of K. We then need to calculate the index of the subgroup of points with good reduction at these valuations. We can take the lowest N from all of our methods to use as our upper bound.

For the second problem, the method consists in constructing a group homomorphism $f : E(K) \to \mathbb{F}_p^N$ which is injective on B/pB. Two methods are described for finding f, both using auxiliary primes $\mathfrak{q}$ such that $p|\#E(\mathbb{F}_\mathfrak{q})$. Both these methods have been implemented in the programming language MAGMA for general number fields K and separately[1] for $K = \mathbb{Q}$. The first method, due to Siksek, is to map to a subgroup of order p in $E(\mathbb{F}_\mathfrak{q})$ and hence (via an elliptic curve discrete logarithm) to $\mathbb{F}_p$. This has certain drawbacks which are described. A newer and more elegant method using a map related to the Tate-Lichtenbaum pairing is described, where the map is to $\mathbb{F}_\mathfrak{q}^*/(\mathbb{F}_\mathfrak{q}^*)^p$ for $N(\mathfrak{q}) \equiv 1$ (mod p), and hence (via a discrete logarithm in $\mathbb{F}_\mathfrak{q}^*$) to $\mathbb{F}_p$. The resulting algorithm works well in practice, despite the restriction that only primes $N(\mathfrak{q}) \equiv 1$ (mod p), can be used. We have proved that the use of sufficiently many primes $\mathfrak{q}$ will always be sufficient to prove that a $p-$saturated subgroup of $E(K)$ is indeed $p-$saturated.

1.1 Structure of the thesis.

A local - global principle of the points on elliptic curves on finite fields versus number fields is proved in Chapter 2. This is the result we need to show that our method of $p-$saturation via the Tate-Lichtenbaum pairing confirms $p-$saturation in finite time. Our proof uses Galois Theory, Elementary Group Theory and Tchebotarev's Density Theorem. We note that several other authors have produced similar and equivalent results, but felt our proof, which uses elementary methods and was derived independently, deserved inclusion for completeness.

[1] See www.maths.nott.ac.uk/personal/pmxpm for the MAGMA implementation of the algorithms in this thesis.

In Chapter 3, we describe our method and Siksek's method [17],[18] of $p-$saturation, the second part of our saturation problem defined above. We prove that our method is always successful in finite time in the case of $p-$saturated input, and prove that there are elliptic curves and points for which Siksek's method fails while ours succeeds. We also describe the method of Frey-Ruck-Muller [9] for calculating the Tate-Lichtenbaum pairing. In fact in practice, we use both our method and Siksek's method of finding homomorphisms f because this makes our programs run faster.

Chapters 4, 5, 6 are all concerned with the first part of our saturation problem defined above; that of determining an upper bound N on $n = [\overline{B} : B]$. In Chapter 4, we provide a statement of the results from a joint paper in progress of Cremona, Siksek and myself [2]. This paper provides a method for calculating an upper bound on the difference between naive and canonical height of points on $E(K)$. In Chapter 5, we describe a method for searching for all points on $E(K)$ of bounded naive height. In combination with Chapter 4, this means we have a method for searching for all points of bounded canonical height on $E(K)$, and hence we can determine a lower bound λ on the least canonical height of a non-torsion point on $E(K)$. Our bound λ is a prerequisite for the three different methods of calculating N described in Chapter 6. Two use the upper bound and searching of chapters 4 and 5 to obtain λ but the third uses analytical techniques instead and it runs in far less time than sometimes lengthy searching and calculation of the upper bound.

Finally, in Chapter 7, we bring together the methods of the thesis and demonstrate the complete saturation process. We also demonstrate a method which often succeeds in proving that sets of points on elliptic curves are independent.

1.2 Notation

The following notation has been used throughout the thesis:

Let E be an elliptic curve given by the Weierstrass equation:

$$E: \quad Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

where $a_1, \ldots, a_6$ are in the ring of integers $\mathfrak{O}_K$ of a number field K. These inclusions of fields hold: $\mathbb{Q} \subseteqq K \subseteqq K_1 \subseteq K_2$, where $\mathbb{Q}$ is the rational numbers. K is the field of definition of the elliptic curve E, and K_1/K and K_2/K_1 are finite, Galois extensions to be made specific later. Let $\overline{K}$ denote the algebraic closure of K.

p is a rational prime; $\mathfrak{q}$ is a prime ideal of K. Also, $\mathbb{F}_{\mathfrak{q}} = \mathfrak{O}_K/\mathfrak{q}$.

Let $\zeta_p \in \overline{K}$ denote a p'th root of unity.

We also require the following notation:

M_K	the set of all valuations on K,
M_K^0	the set of non-archimedean valuations on K,
M_K^∞	the set of archimedean valuations on K,
v	a valuation on K,
n_v	the local degree $[K_v : \mathbb{Q}_v]$.

Our canonical heights are double those in Silverman's book, [21].

Chapter 2

A Local - Global Principle for points on Elliptic Curves

In this chapter we present theoretical results which prove that the algorithm for saturating at an individual prime p (see chapter 3) works correctly. Since our technique of saturation involves projecting points $P_1, \ldots, P_s$ on the elliptic curve $E(K)$, to points on reduced curves over finite fields, it is only natural that a Local - Global Principle is such a result.

Define the natural maps

$$\lambda_{\mathfrak{q}} : E(K) \to E(\mathbb{F}_{\mathfrak{q}})$$
$$\overline{\lambda}_{\mathfrak{q}} : E(K)/pE(K) \to E(\mathbb{F}_{\mathfrak{q}})/pE(\mathbb{F}_{\mathfrak{q}})$$

Define $S = \{\mathfrak{q} \lhd \mathfrak{O}_K : \mathfrak{q}$ is a prime ideal and E has bad reduction at $\mathfrak{q}\}$.

2.1 Statement of Theorems

Theorem 2.1.1.

$$(\prod_{\mathfrak{q}\notin S} \overline{\lambda}_{\mathfrak{q}}) : E(K)/pE(K) \hookrightarrow \bigoplus_{\mathfrak{q}\notin S} E(\mathbb{F}_{\mathfrak{q}})/pE(\mathbb{F}_{\mathfrak{q}})$$

is injective.

Theorem 2.1.2.

$$\forall P \in E(K)\backslash pE(K), \exists \mathfrak{q} \notin S : \lambda_{\mathfrak{q}}(P) \notin pE(\mathbb{F}_{\mathfrak{q}})$$

In fact for each such P there are infinitely many such $\mathfrak{q}$.

Given Theorem 2.1.1, since $E(K)$ is finitely generated, there clearly exists a rational integer $N > 0$ such that

Corollary 2.1.3.

$$E(K)/pE(K) \hookrightarrow \bigoplus_{\mathfrak{q}\notin S, N(\mathfrak{q})\leq N} E(\mathbb{F}_{\mathfrak{q}})/pE(\mathbb{F}_{\mathfrak{q}}) \qquad \textit{is} \quad \textit{injective}$$

Theorem 2.1.4. *Same as Theorem 2.1.1 restricting to $N(\mathfrak{q}) \equiv 1$ (mod p) only.*

2.2 Background on methods of proof

We prove all of these theorems using Galois Theory, Group Theory, and the Chebotarev Density Theorem:

2.2.1 Statement of Chebotarev Density Theorem

Let K_2 be a finite Galois extension of K and set $H = Gal(K_2/K)$. To each prime $\mathfrak{q}$ of K unramified in K_2/K there exists a conjugacy class of Frobenius elements of H, $[\frac{K_2/K}{\mathfrak{Q}}]$, $\mathfrak{q}\mathfrak{O}_{K_2} = \mathfrak{Q}_1\mathfrak{Q}_2\ldots\mathfrak{Q}_g$ and $\forall x \in \mathfrak{O}_{K_2}$, $x^{[\frac{K_2/K}{\mathfrak{Q}}]} \equiv x^{N(\mathfrak{q})} \quad (mod \quad \mathfrak{Q})$

Theorem 2.2.1. *(Chebotarev Density Theorem).[12] Using the above notation, let $\sigma \in H$ and suppose that σ has c conjugates in H. Then the set of primes of K which have a prime divisor in K_2 whose Frobenius automorphism is σ has density $\frac{c}{|H|}$.*

2.2.2 Motivation for use of Galois Theory in proof

The strategy used in the proof of Theorem 2.1.2 is to consider Galois representations. Given

$$P \in E(K) \backslash pE(K) \tag{2.1}$$

we wish to show there exist infinitely many $\mathfrak{q} : N(\mathfrak{q}) \equiv 1 \bmod p$ such that

$$\lambda_{\mathfrak{q}}(P) \in E(\mathbb{F}_{\mathfrak{q}}) \backslash pE(\mathbb{F}_{\mathfrak{q}}). \tag{2.2}$$

We have a polynomial equation whose roots correspond to solutions $Q \in E(K)$ of $pQ = P$.

(2.1) $\iff$ this equation has no rational roots.

(2.2) $\iff$ this equation has no roots mod $\mathfrak{q}$.

Conditions (2.1) and (2.2) can be reinterpreted in terms of Galois actions.

2.2.3 Definitions of Galois extensions used in the proof of the Local -Global Principle

Take $E(K)$ and p a prime. Then:

$$E[p] = \{T \in E(\overline{K}) : pT = 0\}$$

As an abstract group, $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$. This is however a non-canonical isomorphism as it relies on a choice of basis for $E[p]$: T_1, T_2.

$E[p]$ is also a Galois module. Take $K_1 = K(E[p]) = K(x_1, y_1, x_2, y_2)$ where $T_i = (x_i, y_i)$ so that all points in E[p] are defined over K_1.

K_1/K is a finite extension, and is Galois since the algebraic conjugate of any T in $E[p]$ is also in $E[p]$. Let $G = G_K = \mathrm{Gal}(\overline{K}/K)$. Then $\forall T \in E[p], \forall \sigma \in G, \quad T^\sigma \in E[p]$. So G acts on $E[p]$. The kernel of the action is G_{K_1} using the obvious notation, since, $\sigma \in G$ and σ acts trivially on $E[p] \iff T_1^\sigma = T_1$ and $T_2^\sigma = T_2 \iff \sigma$ fixes $x_1, y_1, x_2, y_2 \iff \sigma$ fixes all of $K_1 \iff \sigma \in G_{K_1}$.

$G_K/G_{K_1} = \mathrm{Gal}(K_1/K)$ is finite and acts faithfully on $E[p]$.

$$\rho : G_K/G_{K_1} \hookrightarrow \mathrm{Aut}E[p] \cong B \leq GL(2, \mathbb{Z}/p\mathbb{Z}),$$

$$T_1^\sigma = a_\sigma T_1 + b_\sigma T_2,$$

$$T_2^\sigma = c_\sigma T_1 + d_\sigma T_2,$$

$$\sigma \mapsto \rho(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix},$$

$$\rho : G_K/G_{K_1} \hookrightarrow GL(2, \mathbb{Z}/p\mathbb{Z}),$$

$$\deg(K_1/K) \leq |GL(2, \mathbb{Z}/p\mathbb{Z})| = (p^2 - 1)(p^2 - p).$$

Now let $Q \in E(K)$ and choose $P_0 \in E(\overline{K})$ such that $pP_0 = Q$. Note that:

$$\{P \in E(\overline{K}) | pP = Q\}$$

$$= \{P_0 + T | pT = 0\}$$

$$= P_0 + E[p].$$

Let

$$K_2 = K(\frac{1}{p}Q) = K(x_1, y_1, \ldots, x_{p^2}, y_{p^2}),$$

where

$$P_i = (x_i, y_i) \in P_0 + E[p] \text{ for } i = 1, \ldots, p^2.$$

We have $K_1 \subseteqq K_2$ since $\forall T \in E[p],\ T = (P_0 + T) - P_0 \in E(K_2)$. This is because $(P_0 + T) \in E(K_2)$, and $P_0 \in E(K_2)$. So $K_2 = K_1(P_0)$.

The field extension K_2/K_1 depends on point Q only whilst the extension K_1/K depends on p only, not on Q.

2.3 Proof of the Principle

We prove Theorem 2.1.1 in stages by proving lemmas that imply it. Lemma 2.3.1 is the first such.

Lemma 2.3.1. *(Analysis of Galois Groups.) For p a rational prime, set $K_2 = K(\frac{1}{p}Q)$ for Q any point chosen on $E(K)$. Then there is an injective homomorphism $\rho : Gal(K_2/K) \hookrightarrow AGL(2, \mathbb{F}_p)$.*

We observe that the following holds, although it is not necessary for our proof.

Lemma 2.3.2. *(Serre) If $E(K)$ does not have complex multiplication, then for almost all p, $\rho(Gal(K_1/K)) = GL(2, \mathbb{Z}/p\mathbb{Z})$.*

Proof. See [16]. □

2.3.1 Some prerequisites and implications of Lemma 2.3.1

Lemma 2.3.3. *K_1/K and K_2/K are unramified outside p and primes of bad reduction for E.*

Proof. 1. Suppose $\mathfrak{q}$ is a prime of K, which is not a divisor of p nor a prime of bad reduction for E, with $\mathfrak{Q}$ being one of its extensions to K_1. Then the condition K_1/K is unramified at $\mathfrak{Q}$ is equivalent to the extension $K_{1\mathfrak{Q}}/K_{\mathfrak{q}}$ being unramified with $K_{1\mathfrak{Q}}$ and $K_{\mathfrak{q}}$ being the local completions of K_1 and K at $\mathfrak{Q}$ and $\mathfrak{q}$ respectively. [19, Theorem 7.1 on p.184] implies that $K(E[p]) = K_1$ is unramified outside p and primes of bad reduction for E as required.

2. The field K_1 depends on p and E whilst K_2 depends on the point Q being divided by p. There are only finitely many fields K_2 because $E(K)/pE(K)$ is finite. Define $L = K([p]^{-1}E(K))$, the compositum of all fields K_2. Then, [19, Proposition 1.5, p.193] implies that the extension L/K_1 is unramified outside of our set. Together with our proof in (1) above that K_1/K is unramified, this proves that K_2/K is unramified outside of our set.

□

Lemma 2.3.4. *Take $\sigma \in Gal(K_2/K)$ and ρ as in Lemma 2.3.1. We have $\rho(\sigma) : x \in \mathbb{F}_p^2 \to Mx + v$ where $M \in GL(2, \mathbb{F}_p)$ and $v \in \mathbb{F}_p^2$ Then it follows that:*

$$det\rho : \sigma \to det(\rho(\sigma)) = det(M) \in \mathbb{F}_p^*$$

is the p'th cyclotomic character of H. This means, $\forall \sigma \in \mathrm{Gal}(\overline{K}/K), \zeta_p^\sigma = \zeta_p^{n(\sigma)}$ for some $n(\sigma) \in \mathbb{F}_p^*$ where $n(\sigma) = det(\rho(\sigma))$.

Proof. 1. For $\sigma \in \mathrm{Gal}(K_1/K)$, a standard result which follows easily from properties of the Weil Pairing is that $\det(\sigma)$ is the cyclotomic character of H.

2. Identify $\mathrm{Gal}(K_2/K)$ with a subgroup of $AGL(2, \mathbb{F}_p)$ by fixing a basis for $E[p]$. Each $\sigma \in \mathrm{Gal}(K_2/K)$ has the form $x \to Mx + v$ where $M = \rho(\sigma|K_1) \in GL(2, \mathbb{F}_p)$. So $\sigma \to \det M$ is the cyclotomic character by (1).

□

Remark 2.3.5. *Regarding Lemma 2.3.4, the Weil Pairing implies that $\zeta_p \in K_1$. In what follows, $\mathfrak{q}$ is a prime of K, and $p \nmid N(\mathfrak{q})$. Also $\mathfrak{q}$ is of good reduction (so by Lemma 2.3.3, K_1/K is unramified at $\mathfrak{q}$.)*

Lemma 2.3.6. *$det(\rho(\mathrm{Frob}_{\mathfrak{Q}}))$ only depends on $\mathfrak{q}$.*

$$det(\rho(\mathrm{Frob}_{\mathfrak{Q}})) \equiv N(\mathfrak{q}) \qquad (mod \quad p).$$

Proof. Extending the proof of Lemma 2.3.4, taking $\sigma = \mathrm{Frob}\mathfrak{Q}$ we get $\det(\rho(\sigma)) \equiv N(\mathfrak{q})$ (mod p), since on ζ_p the effect of $\mathrm{Frob}\mathfrak{Q}$ is $\zeta_p \to \zeta_p^{N(\mathfrak{q})}$.

Note that although $\mathrm{Frob}_{\mathfrak{Q}}$ does depend on which prime $\mathfrak{Q}$ above $\mathfrak{q}$ we take , it only does so up to conjugacy, so the determinant of $\rho(\mathrm{Frob}_{\mathfrak{Q}})$ is a well-defined element of $\mathbb{F}_p^*$ depending only on $\mathfrak{q}$ not on $\mathfrak{Q}$. □

2.3.2 Proof of Lemma 2.3.1

For $\sigma \in \mathrm{Gal}(K_2/K_1)$ set $T_\sigma = P_0^\sigma - P_0$.

Note that $T_\sigma \in E[p]$ since

$$\begin{aligned} pT_\sigma = pP_0^\sigma - pP_0 =& (pP_0)^\sigma - (pP_0) \\ =& Q^\sigma - Q \\ =& 0 \text{ since } Q \in E(K). \end{aligned}$$

Moreover for all $P \in P_0 + E[p]$ we have, for $\sigma \in \mathrm{Gal}(K_2/K_1)$,

$$P^\sigma - P = (P_0 + T)^\sigma - (P_0 + T) = P_0^\sigma - P_0 = T_\sigma$$

(since $T^\sigma = T$), so σ acts on $P_0 + E[p]$ by translation by T_σ.

Moreover it is easy to check that the map $\sigma \to T_\sigma$ is a homomorphism $\mathrm{Gal}(K_2/K_1) \to E[p]$. As it is clearly injective we have

$$\mathrm{Gal}(K_2/K_1) \hookrightarrow E[p] \cong (\mathbb{Z}/p\mathbb{Z})^2.$$

Thus $\sigma \in \mathrm{Gal}(K_2/K_1)$ acts as a translation.

Recall $E[p] = \langle T_1, T_2 \rangle$. We have that $\mathrm{Gal}(K_2/K)$ acts faithfully on

$$P_0 + E[p] = \{P_0 + rT_1 + sT_2 | (r,s) \in \mathbb{F}_p^2\}.$$

Identifying this set with $\mathbb{F}_p^2$ allows us to identify $\mathrm{Gal}(K_2/K)$ with a subgroup of $AGL(2, \mathbb{F}_p)$. For $\sigma \in \mathrm{Gal}(K_2/K)$,

$$(P_0 + rT_1 + sT_2)^\sigma = P_0^\sigma + r'T_1 + s'T_2 = T_\sigma + P_0 + r'T_1 + s'T_2,$$

where

$$\rho(\sigma) \begin{pmatrix} r \\ s \end{pmatrix} = \begin{pmatrix} r' \\ s' \end{pmatrix}$$

and here $\rho(\sigma) = \rho(\sigma|K_1)$. Writing $T_\sigma = r_\sigma T_1 + s_\sigma T_2$ we have

$$(P_0 + rT_1 + sT_2)^\sigma = P_0 + r''T_1 + s''T_2,$$

where

$$\begin{pmatrix} r'' \\ s'' \end{pmatrix} = \begin{pmatrix} r_\sigma \\ s_\sigma \end{pmatrix} + \begin{pmatrix} r' \\ s' \end{pmatrix} = \begin{pmatrix} r_\sigma \\ s_\sigma \end{pmatrix} + \rho(\sigma) \begin{pmatrix} r \\ s \end{pmatrix}.$$

So the induced action on $v \in \mathbb{F}_p^2$ is

$$\sigma : v \mapsto A_\sigma v + b_\sigma,$$

$$\text{where } A_\sigma = \rho(\sigma|K_1) \in GL(2, \mathbb{F}_p) \text{ and } b_\sigma = \begin{pmatrix} r_\sigma \\ s_\sigma \end{pmatrix} \in \mathbb{F}_p^2.$$

□

2.3.3 A Group Theoretical Result

Proposition 2.3.7. *Let $H \leq AGL(2,\mathbb{F}_p)$ have the property that every $h \in H$ has a fixed point (in the natural action of $AGL(2,\mathbb{F}_p)$ on $\mathbb{F}_p^2$). Then H has a fixed point. Moreover it is enough to assume that every $h \in H \cap ASL(2,\mathbb{F}_p)$ has a fixed point.*

Lemma 2.3.8. *If H has an orbit of size n, $\{P_1, P_2, \ldots, P_n\}$ and $p \nmid n$ then H has a fixed point $P_0 = \frac{1}{n}(P_1 + P_2 + \ldots + P_n)$*

Proof of Lemma 2.3.8: Clear. □

2.3.4 Proof of Proposition 2.3.7

H acts on $\mathbb{F}_p^2$ since $H \leq AGL(2,\mathbb{F}_p)$. All elements of H have a (possibly different) fixed point. Define $H_0{=}H{\cap}ASL(2,\mathbb{F}_p)$. Define (A,v) ($A \in GL(2,\mathbb{F}_p)$ and $v \in \mathbb{F}_p^2$) to denote the element of $AGL(2,\mathbb{F}_p)$ which acts upon $x \in \mathbb{F}_p^2$ according to $x \to Ax + v$. Consider the group homomorphism $\phi : AGL(2,\mathbb{F}_p) \to GL(2,\mathbb{F}_p)$ mapping $(A,v) \mapsto A$. For any non-identity element $L \in \text{Ker}\phi$ then L is a translation so $L \notin H$ as L has no fixed point and so $\phi_{|H}$ has a trivial kernel. Hence
$H \cong \phi(H) \leq GL(2,\mathbb{F}_p)$
$\Rightarrow |H| \big| |GL(2,\mathbb{F}_p)| = (p^2-1)(p^2-p) = (p-1)^2 p(p+1)$
If p does not divide $|H|$ then the size of all orbits in $\mathbb{F}_p^2$ (which divide $|H|$) are coprime to p and so by lemma 2.3.8, there is a fixed point as required. If $p\big||H|$ then $p\big||H_0|$ (since $|H/H_0|\big|p-1$.) By Cauchy's Theorem, H_0 has an element h of order p. By assumption h has a fixed point $x \in \mathbb{F}_p^2$.

$$\langle h \rangle \leq Stab_H(x) \Rightarrow |Orb_H(x)| = \frac{|H|}{|Stab_H(x)|}, \text{ is coprime to p.}$$

Hence there is an H-orbit of size coprime to p, which by lemma 2.3.8 concludes the proof. □

2.3.5 A Remark to the proof of this theorem.

The crucial fact about H which we needed is that $ord_p(|H|) \leq 1$ so the Sylow-p-subgroup of H is cyclic. A cyclic Sylow-p-subgroup is necessary so that we can choose a generator $h \in H_0$ with fixed point $x \in \mathbb{F}_p^2$ and hence $|Orb_H(x)|$ is coprime to p.

2.3.6 Proof of Theorem 2.1.1

(This is an application of the Proposition 2.3.7.)

K_2/K is unramified away from p, and factors of the conductor of E by lemma 2.3.3. By Chebotarev, each $h \in H = Gal(K_2/K)$ has the form Frob($\mathfrak{Q}$) for infinitely many prime ideals $\mathfrak{Q} \lhd K_2 : \mathfrak{Q} \nmid p$ and $\mathfrak{Q} \nmid cond(E)$.

H acts on $\{P : pP = Q\}$. This means H has a fixed point $P \iff Q \in pE(K)$. Writing each element $h \in H$ as a Frobenius associated to a prime $\mathfrak{Q}$ it is clear that h has a fixed point in its action on $\{P \in E(K) : pP = Q\}$ if and only if it has a fixed point in its action on $\{\overline{P} \in E(\mathbb{F}_{\mathfrak{Q}}) : p\overline{P} = \lambda_{\mathfrak{Q}}(Q)\}$ it has if and only if $\lambda_{\mathfrak{Q}}(Q) \in pE(\mathbb{F}_{\mathfrak{Q}})$. This completes the proof.□

2.3.7 Proof of Theorem 2.1.2

Follows immediately from proof of Theorem 2.1.1 above noting that the Frobenius Density Theorem gives infinitely many such $\mathfrak{q}$.□

2.3.8 Proof of Theorem 2.1.4

If Q is in the kernel of all the maps

$$E(K) \to E(K)/pE(K) \to E(\mathbb{F}_{\mathfrak{q}})/pE(\mathbb{F}_{\mathfrak{q}})$$

for $\mathfrak{q} \notin S, N(\mathfrak{q}) \equiv 1 \pmod{p}$ then in the notation of the proof of Theorem 2.1.1 above, we have that each $h \in H \cap ASL(2, \mathbb{F}_p)$ has a fixed point since (from

$\det \rho = \chi$) we see that $\det(\rho(Frob(\mathfrak{q}))) \equiv 1 \pmod{p} \iff N(\mathfrak{q}) \equiv 1 \pmod{p}$ Hence Proposition 2.1.4 follows, using the last part of Proposition 2.3.7.□

2.4 Alternative proofs of the Local - Global Principle for points on Elliptic Curves.

After we proved Theorem 2.1.1 in 2001, several other papers came to our attention which proved the same (or similar) results independently in different contexts. We now discuss some of these.

Cassels and Flynn's book, "Prolegomena to a middlebrow arithmetic of curves of genus 2", [1, Chapter 6, section 9, page 61, "A Pathology"] says "we construct a curve C of genus 2 and an element A of its jacobian, both defined over $\mathbb{Q}$, such that (1) A is not divisible by 2 over $\mathbb{Q}$, but (2) A is divisible by 2 over every $\mathbb{Q}_p$ and over $\mathbb{R}$. It is not difficult to see that the analogous behaviour is impossible in genus 1."

The last sentence claims what our result says, with $K = \mathbb{Q}$, and $p = 2$ that a point on an elliptic curve over $\mathbb{Q}$ is divisible by 2 over $\mathbb{Q}$ if and only if it is divisible by 2 over all $\mathbb{Q}_p$ and over $\mathbb{R}$. Our result is more general, in that it replaces 2 by a general prime, and allows certain subsets of the $\mathbb{Q}_p$. Cassels and Flynn demonstrate here that our result cannot be extended to genus 2.

Our next result is from R. Dvornicich and U. Zannier, "Local-global divisibility of rational points in some commutative algebraic groups", [6]. The context here is of a commutative and connected algebraic group defined over a number field; this would include abelian varieties as a special case, and elliptic curves a special case of that. One of their results is:

Theorem 2.4.1. *Let E be an elliptic curve defined over a number field K. If a point $P \in E(K)$ is divisible by p in almost all $E(K_v)$, then it is divisible by p in $E(K)$.*

G.J. van der Heiden at Groningen (NL) also proves the same result in his paper [11] in which the main emphasis is on whether a similar result is true for Drinfeld modules (which it is not in general).

Chapter 3

p-Saturation of Points on an Elliptic Curve.

Definition 3.0.2. *We write $\hat{E}(K) = E(K)/Tor(E(K))$, with τ being the quotient map.*

Suppose we have s independent points, $P_1 \ldots P_s$, on an elliptic curve E of rank r over K. These could be obtained by 2-descent for example.

Let $G = \hat{E}(K)$, $s \leq r$, $H = \langle \tau(P_1), \ldots, \tau(P_s) \rangle \leq \hat{E}(K)$.

We have developed a computer program [1] which finds s independent points $P'_1, \ldots, P'_s$ where $\tau(P'_1), \ldots, \tau(P'_s)$ span a subgroup H' of $\hat{E}(K)$ with $[H' : H]$ finite and maximal. The program uses our algorithms which are described here and are either original or are improvements of those devised by Prof Cremona's previous student, Samir Siksek. Note that my method will clearly not find all of $\hat{E}(K)$ if $s < r$.

Definition 3.0.3. *Suppose p is a rational prime, and $L \leq G$. L is said to be p-saturated in G if $\nexists J : L \leq J \leq G$ with $[J : L] = p$.*

[1] See www.maths.nott.ac.uk/personal/pmxpm for the MAGMA implementation of the algorithms in this thesis.

Definition 3.0.4. *With the same notation, L is said to be saturated in G if $\nexists J : L \leq J \leq G$ with $[J : L]$ finite and bigger than* 1.

Remark 3.0.5. *Clearly, using the same notation, H is saturated iff it is $p-$ saturated $\quad\forall p$ where p is a rational prime.*

In later chapters, we use geometry of numbers arguments and often searching for points of low canonical heights to obtain an upper bound on $\{p : \langle P_1, \dots, P_s\rangle$ is not p-saturated$\}$. In this chapter we describe our algorithm for saturating at a given rational prime p and give examples.

To check p-saturation for given p, we need to prove there are no non-trivial solutions to:

$$pQ = \sum_{i=1}^{s} a_i P_i + \sum_{j=1}^{t} b_j T_j, \tag{3.1}$$

where $T_j : j \leq 2$ are a basis for the p-power torsion points of $E(K)$.

The direct method of solving equation 3.1 is to check all $\frac{p^{s+t}-1}{p-1}$ vectors $(\underline{a}, \underline{b})$: $0 \leq a_i, b_i \leq p-1$ representing all 1-dimensional subspaces of $\mathbb{F}_p^{s+t}$ and see if equation (3.1) has a solution.

The direct method is simple to understand and program[2], but it has a disadvantage that it takes too long for p or s large.

We define:

$$V_p = \big\{(\overline{\mathbf{a}}, \overline{\mathbf{b}}) \text{ with } \overline{\mathbf{a}} \in \mathbb{F}_p^s, \overline{\mathbf{b}} \in \mathbb{F}_p^t : \text{if } \mathbf{a} \equiv \overline{\mathbf{a}} \text{ (mod p) and } \mathbf{b} \equiv \overline{\mathbf{b}} \text{ (mod p) then } \sum_{i=1}^{s} a_i P_i + \sum_{j=1}^{t} b_j T_j \in p\hat{E}(K)\big\}.$$

It is clear that V_p is an $\mathbb{F}_p$- linear subspace of $\mathbb{F}_p^{s+t}$, and that $\langle P_1, \dots, P_s\rangle$ is p-saturated if and only if $V_p = \{0\}$.

[2] See section 3.4 below for how to check whether a given point in $E(K)$ actually lies in $pE(K)$ i.e. can be divided by p

Our approach is to seek group homomorphisms $\psi_n : \hat{E}(K) \to \mathbb{F}_p$. Then for all $(\overline{\mathbf{a}}, \overline{\mathbf{b}}) \in V_p$ we have

$$\sum \overline{a}_i \psi_n(P_i) + \sum \overline{b}_j \psi_n(T_j) = 0. \tag{3.2}$$

So $V_p \subseteq \text{Ker}\overline{\psi_n}$ where $\overline{\psi_n} : \mathbb{F}^{s+t} \to \mathbb{F}_p$ is the induced map.

If we can construct several such maps $\psi_1, \psi_2, \ldots$ then $V_p \subseteq \bigcap \text{Ker}(\overline{\psi_n})$. Ideally, each ψ_n cuts down the dimension of $\bigcap \text{Ker}(\psi_n)$ by 1 and after $s+t$ steps we will show that $V_p = 0$. In any case, we will reduce the number of possible vectors $(\underline{\mathbf{a}}, \underline{\mathbf{b}})$ to test down to $\frac{p^d-1}{p-1}$ where $d = \dim(\bigcap \text{Ker}(\psi_n))$.

3.1 Theory of using the Tate-Lichtenbaum Pairing to find group homomorphisms

We show how our homomorphisms ψ_n are defined using the Tate-Lichtenbaum pairing, and we identify the exact kernel of ψ_n which is used to prove that our method is an improvement on Siksek's method in Section 3.3.

The Tate-Lichtenbaum pairing uses the isomorphism that exists between $E(\mathbb{F}_q)$ and the class group of divisors of degree zero on E, by which $P \in E(\mathbb{F}_q)$ is mapped to the class $(P) - (\infty)$.

Proposition 3.1.1. *(Tate-Lichtenbaum pairing) For $p \big| N(\mathfrak{q}) - 1$, E an elliptic curve over $F_{\mathfrak{q}}$ for $\mathfrak{q} \lhd \mathfrak{O}(K)$ there is a non-degenerate bilinear pairing:*

$$E(\mathbb{F}_{\mathfrak{q}})[p] \times E(\mathbb{F}_{\mathfrak{q}})/pE(\mathbb{F}_{\mathfrak{q}}) \to \mathbb{F}_{\mathfrak{q}}^{*}/\mathbb{F}_{\mathfrak{q}}^{*p}$$

defined as follows:

Take points $P \in E(\mathbb{F}_{\mathfrak{q}})[p]$ and $P' \in E(\mathbb{F}_{\mathfrak{q}})$. Define D_P and $D_{P'}$ to be coprime divisors in the class of $(P) - (\infty)$ and $(P') - (\infty)$ respectively. Since $pP = O_E$ it follows that $p.D_P$ is the divisor of a function F_{D_P} on E. The Tate -Lichtenbaum *pairing is given by*

$$\alpha_p : (P, P') \mapsto F_{D_P}(D_{P'})^{\frac{N(\mathfrak{q})-1}{p}} \in \mathbb{F}_{\mathfrak{q}}^*/\mathbb{F}_{\mathfrak{q}}^{*p}.$$

Proof. Theorem from [8]. □

Equivalently to proposition 3.1.1, for each $T \in E(\mathbb{F}_{\mathfrak{q}})$ of order p there is a surjective homomorphism:

$$f_T : E(\mathbb{F}_{\mathfrak{q}}) \to \mathbb{F}_{\mathfrak{q}}^*/(\mathbb{F}_{\mathfrak{q}}^*)^p, \text{ where } P \mapsto \alpha_p(T, P)$$

with kernel containing $pE(\mathbb{F}_{\mathfrak{q}})$. If T_1 and T_2 are independent points of order p then f_{T_1} and f_{T_2} are independent i.e. neither is a power of the other.

Hence the number of independent such maps is $0, 1, 2$ according to the p-rank of $|E(\mathbb{F}_{\mathfrak{q}}[p])|$. (See [19, Corollary 6.4 (b), page 89].)

3.1.1 Another equivalent definition of f_T

Given $T \in E(\mathbb{F}_{\mathfrak{q}})[p]$, we can define the function $F_T \in \mathbb{F}_{\mathfrak{q}}(E)$ up to multiplication by a constant by

$$div(F_T) = p(T) - p(\infty).$$

We define $f_T(P)$ for $P \in E(\mathbb{F}_{\mathfrak{q}})$ to be F_T evaluated on the divisor $(P) - (\infty) \in Pic^0(E)$ using the usual association of points on $E(K)$ with divisors in $Pic^0(E)$. We have that $f_T(P)$ is well-defined modulo $F_{\mathfrak{q}}^*/F_{\mathfrak{q}}^{*p}$ by this definition by Weil duality: i.e. we can choose any divisor D linearly equivalent to $(P)-(\infty)$ and f_T gives the same answer modulo $F_{\mathfrak{q}}^*/F_{\mathfrak{q}}^{*p}$ whether evaluated on D or on $(P)-(\infty)$.

To evaluate $f_T(P)$, choose a non-identity point $P' \in E(\mathbb{F}_{\mathfrak{q}})$ such that $P + P'$ and P' are both neither of T, 0_E. Since $(P'+P)-(P')-(P)+(\infty)$ is a principal divisor, $(P) - (\infty)$ and $(P + P') - (P')$ are linearly equivalent. Hence

$$f_T(P) = \frac{F_T(P+P')}{F_T(P')}$$

noting that this is well-defined in $F_{\mathsf{q}}^*/F_{\mathsf{q}}^{*p}$ by choice of P'.

There exists a p-isogeny ϕ_T to another elliptic curve E' [19, Proposition 4.12, page 78] with dual isogeny $\hat{\phi}_T$ such that

$$\phi_T : E \to E', \text{ with } \mathrm{Ker}(\phi_T) = \langle T \rangle \leq E(\mathbb{F}_{\mathsf{q}})$$

and

$$\hat{\phi}_T : E' \to E$$

with

$$\phi_T\hat{\phi}_T = [p]_{E'}, \text{ and, } \hat{\phi}_T\phi_T = [p]_E.$$

3.1.2 Identifying Kernel of Tate-Lichtenbaum maps

Lemma 3.1.2.

$$\mathrm{Ker}(f_T) = \hat{\phi}_T(E'(\mathbb{F}_{\mathsf{q}})) \leq E(\mathbb{F}_{\mathsf{q}}).$$

Proof. We will first show that $\exists g \in \mathbb{F}_{\mathsf{q}}(E') : f_T\hat{\phi}_T = g^p$. We may need to scale f to achieve this. This will prove that $\hat{\phi}_T(E'(\mathbb{F}_{\mathsf{q}})) \subseteq \mathrm{Ker}(f_T)$.

Choose $S \in E'(\overline{\mathbb{F}}_{\mathsf{q}})$ with $\hat{\phi}_T(S) = T$. Let $\{T_1', \ldots, T_p'\} = \mathrm{Ker}(\hat{\phi}_T(E'(\overline{\mathbb{F}}_{\mathsf{q}})))$.

Consider

$$\begin{aligned} div(f_T\hat{\phi}_T) &= \hat{\phi}_T^*(p(T) - p(\infty)) \\ &= p\Big(\sum_{i=1}^{p}((S \oplus T_i') - (T_i')\Big) \\ &= pD, \end{aligned}$$

where D is $\mathbb{F}_{\mathsf{q}}$-rational since the Galois action $G = \mathrm{Gal}(\overline{\mathbb{F}}_{\mathsf{q}}/\mathbb{F}_{\mathsf{q}})$ will permute the preimages of T (since both T and $\hat{\phi}_T$ are $\mathbb{F}_q$-rational) which are the $S+T_i'$ and so G takes D to itself.

$D = \sum_{i=1}^{p}(S \oplus T_i') - (T_i')$ is principal because

$$\begin{aligned} pS &= \phi_T(\hat{\phi}_T(S)) \\ &= \phi_T(T) = 0. \end{aligned}$$

So $D = div(g)$ for some $g \in \mathbb{F}_q(E')$.

$$\begin{aligned} div(f_T\hat{\phi}_T) &= p.div(g) = div(g^p), \\ f_T\hat{\phi}_T &= cg^p \text{ for constant } c. \end{aligned}$$

Scaling f_T gives

$$f_T\hat{\phi}_T = g^p$$

as required.

We next show that

$$[E(\mathbb{F}_q) : \hat{\phi}_T(E'(\mathbb{F}_q))] = 1 \text{ or } p.$$

We know from [19, Ex 5.4 page 145] that $|E(\mathbb{F}_q)| = |E'(\mathbb{F}_q)|$. Thus

$$\begin{aligned} [E(\mathbb{F}_q) : \hat{\phi}_T(E'(\mathbb{F}_q))] &= \frac{|E(\mathbb{F}_q)|}{|\hat{\phi}_T(E'(\mathbb{F}_q))|} \\ &= \frac{|E'(\mathbb{F}_q)||Ker\hat{\phi}_T(E'(\mathbb{F}_q))|}{|E'(\mathbb{F}_q)|} \\ &= |Ker\hat{\phi}_T(E'(\mathbb{F}_q))| \\ &= 1 \text{ or } p. \end{aligned}$$

As f_T is a Tate-Lichtenbaum map and hence non-degenerate, Ker(f_T) has index p and so Ker(f_T) $= \hat{\phi}_T(E'(\mathbb{F}_q))$ by the above result. □

3.2 Our application of the theory of Tate-Lichtenbaum maps.

In their paper, [9], Frey-Ruck-Muller use the Tate-Lichtenbaum pairing to reduce a discrete logarithm problem on an elliptic curve over a finite field to a discrete logarithm problem over a finite field. This is of use in work on Elliptic Curve Cryptosystems.

We however use the Tate-Lichtenbaum pairing to calculate the group homomorphisms ψ_n as defined at the beginning of this Chapter 3.

Theorem 3.2.1. *Suppose that $P_1, \ldots, P_r$ are p-saturated in $\hat{E}(K)$ Then, when we generate linear equations (3.2) for all prime ideals $\mathfrak{q} \lhd K : N(\mathfrak{q}) \leq N_0$ for N_0 incremented from 0, using the Tate-Lichtenbaum pairing, we shall prove our points are p-saturated in finite time.*

Proof. Define $\{\psi_{p,\mathfrak{q},y} : y \in 1, \ldots, y_0\}$ to be the maps $\beta\alpha_p : E(\mathbb{F}_\mathfrak{q}) \to \mathbb{F}_p$ derived from the Tate-Lichtenbaum pairing α_p composed with a discrete logarithm map $\beta : F_\mathfrak{q}^* / F_\mathfrak{q}^{*p} \to \mathbb{F}_p$. Here, y_0 is one of $0, 1, 2$ according to the $p-$rank of $E(\mathbb{F}_\mathfrak{q})[p]$. Since $\bigcap_y \mathrm{Ker}(\psi_{p,\mathfrak{q},y}) = pE(\mathbb{F}_\mathfrak{q})$ by proposition 3.1.1 it follows that the set of linear equations in $\{a_i, b_j\}$

$$\{\sum_i a_i \psi_{p,\mathfrak{q},y}(\lambda_\mathfrak{q}(P_i)) + \sum_j b_j \psi_{p,\mathfrak{q},y}(\lambda_\mathfrak{q}(T_j)) = 0 : y = 1, \ldots, y_0\} \tag{3.3}$$

is solved iff $\sum a_i \lambda_\mathfrak{q}(P_i) + \sum b_j \lambda_\mathfrak{q}(T_j) \in pE(\mathbb{F}_\mathfrak{q})$.

Taking N_0 as in corollary 2.1.3, we see that if we form our linear equations for all $\mathfrak{q}$ with $N(\mathfrak{q}) \leq N_0$ and with $N(\mathfrak{q}) \equiv 1 \bmod \mathrm{p}$ then for any simultaneous solutions $\{a_i, b_j\}$, we have $\sum a_i \lambda_\mathfrak{q}(P_i) + \sum b_j \lambda_\mathfrak{q}(T_j) \in pE(\mathbb{F}_\mathfrak{q})$ for all $\mathfrak{q}$ in this range, and so by the injection of corollary 2.1.3, $\sum a_i P_i + \sum b_j T_j \in pE(K)$. As we are in the p-saturated case, $a_i, b_j \in p\mathbb{Z}$, meaning that the only common solution to equations 3.3 taking all $\mathfrak{q}$ in this range is the trivial solution. Thus in finite time we prove $V_p = 0$ as required. □

In practice, we will apply this algorithm without knowing whether or not the given points are p-saturated. If the algorithm doesn't terminate after a very short time, then it is almost certain that the candidate generators are not p-saturated. The current linear equations can in this case be used to restrict possible solutions to Equation (3.1), which can be searched through as in the direct method.

Remark 3.2.2. *In the proof above,* $\bigcap_y \operatorname{Ker}(\psi_{p,\mathfrak{q},y}) = pE(\mathbb{F}_\mathfrak{q})$. *This is a subgroup of* $E(\mathbb{F}_\mathfrak{q})$ *of index* p^2 *when* $|E(\mathbb{F}_\mathfrak{q})[p]| = p^2$. *However,* $\operatorname{Ker}(\psi_{p,\mathfrak{q},y})$ *is a subgroup of index p as in lemma 3.1.2, so using just one homomorphism* $\psi_{p,\mathfrak{q},y}$ *in the algorithm would not suffice in this proof.*

3.2.1 Evaluating Tate-Lichtenbaum pairing to obtain the ψ_n

We explain here how to calculate the maps used in the proof of theorem 3.2.1.

We only consider $\mathfrak{q}$ where $E(\mathbb{F}_\mathfrak{q})$ has a p-torsion point, P.

We need to calculate the Tate-Lichtenbaum pairing for as many $\mathfrak{q} : N(\mathfrak{q}) \equiv 1 \quad mod \quad p$, as are necessary on the $r+s$ points in $\{P_i, T_j\}$. We believe that the most efficient way to do this is to use the idea in the Frey-Ruck-Muller paper [9].

3.2.2 Summary of method in Frey-Ruck-Muller paper [9] for evaluating Tate-Lichtenbaum pairing.

We choose $D_P = (P) - (\infty)$. We assume that $D_{P'}$ is prime to all prime divisors $(r.P)$ for $0 \leq r < p$. First a group law is defined on the set $\{r.P : 0 \leq r < p\} \times \mathbb{F}_\mathfrak{q}^*$:

$(r_1.P, a_1) \oplus (r_2.P, a_2) := ((r_1 + r_2).P, a_1 a_2 h(D_{P'}))$,

where h is a function whose divisor satisfies:

$div(h) = (r_1.P) + (r_2.P) - ((r_1 + r_2).P) - (\infty)$.

It can be shown that this is a group law, and that in particular:

$p \circledcirc (P, 1) = (0_E, F_{D_P}(D_{P'}))$.

Hence in this group by repeated doubling and adding, one can evaluate $F_{D_P}(D_{P'})$ in $O(\log p)$ steps.

3.3 Shortcomings of Siksek method for finding the group homomorphisms.

The Siksek method is as follows. Given $E(K)$, a prime ideal $\mathfrak{q}$, and rational prime p such that $|E(\mathbb{F}_{\mathfrak{q}})|$ is divisible by p, but not by p^2, we construct a group homomorphism $\tau : E(\mathbb{F}_{\mathfrak{q}}) \to \mathbb{F}_p^+$ with $P \in E(\mathbb{F}_{\mathfrak{q}})$ by

$$\tau(P) = \upsilon(\frac{|E(\mathbb{F}_{\mathfrak{q}})|}{p}P), \tag{3.4}$$

where υ is a discrete logarithm on $E(\mathbb{F}_{\mathfrak{q}})[p]$ to $\mathbb{F}_p^+$.

The method has the advantage that it is not necessary for $N(\mathfrak{q}) \equiv 1(\bmod p)$. In my implementation of this algorithm in MAGMA, I have encoded both the Siksek method of calculating homomorphisms as well as the Tate-Lichtenbaum pairing method. The Siksek method may not however, on its own, identify a set of $p-$saturated points as being $p-$saturated. I discuss this now.

Theorem 3.3.1. *Suppose we have $E(\mathbb{Q})$ with the following properties:*

1. *There exists a $p-$isogeny $\phi : E \to E'$, where E' and ϕ are defined over $\mathbb{Q}$.*
2. *The dual isogeny, $\hat{\phi}$ has kernel $\langle T' \rangle \leq E'(\mathbb{Q})$ of order p.*
3. *$E(\mathbb{Q})$ has rank 1 with generator P of the torsion-free group $\hat{E}(\mathbb{Q})$.*
4. *P is in the image of $\hat{\phi}(E'(\mathbb{Q}))$.*

Then $\tau(\lambda_q(P)) = 0$ for any q a rational prime coprime to p and with $\tau : E(\mathbb{F}_q) \to \mathbb{F}_p^+$, as in equation 3.4 and $\lambda_q : E(\mathbb{Q}) \to E(\mathbb{F}_q)$ is the reduction map.

Thus if setting $q = p$ does not generate a homomorphism which establishes $p-$saturation by the Siksek method, then $p-$saturation will never be established by this method.

Proof. Take q coprime to p. The $p-$isogenies on $E(\mathbb{Q})$ reduce to $p-$isogenies on $E(\mathbb{F}_q)$. Also for q coprime to p, then $E(\mathbb{Q})[p]$ maps injectively under λ_q to $E(\mathbb{F}_q)[p]$, see [19, Proposition 3.1 b), page 176]. As in the proof of lemma 3.1.2, $[E(\mathbb{F}_q) : \hat{\phi}(E'(\mathbb{F}_q))] = |\mathrm{Ker}\hat{\phi}(E'(\mathbb{F}_q))| = p$. We have that $\mathrm{Ker}(\tau)$ is of index p since image has order p. Since the Sylow-p-subgroup of $E(\mathbb{F}_q)$ has order p, there is a unique subgroup of index p and so $\mathrm{Ker}(\tau) = \hat{\phi}(E'(\mathbb{F}_q))$. Hence $\lambda_q(P) \in \mathrm{Ker}(\tau)$ as required. □

3.3.1 Examples of where Siksek method fails.

A $3-$saturation example.

We take the elliptic curve E:

$$y^2 + xy = x^3 - 24432x - 1471934$$

over $\mathbb{Q}$ which is in the Cremona Database on MAGMA, referenced "254A3".

This has a $3-$isogeny, ϕ, to a curve E'

$$y^2 + xy = x^3 - \frac{73391}{3}x - \frac{39634253}{27}$$

which is isomorphic to curve "254A2" from the Cremona Database.

The dual isogeny, $\hat{\phi}$ has kernel $\{(\frac{812}{3} : \frac{9881}{3} : 1), (\frac{812}{3} : \frac{-10693}{3} : 1), (0 : 1 : 0)\}$ of order 3.

The generators of the Mordell-Weil group of E and E' modulo torsion are $P = (-\frac{36131}{400} : \frac{361307}{8000} : 1)$ and $P' = (-\frac{4153}{48} : -\frac{1981}{192} : 1)$.

Since $\hat{\phi}(P') = P$, it follows that $P \in \hat{\phi}(E'(\mathbb{Q}))$.

Thus this example fulfils the conditions of our theorem. When we ran our programs with this example using Siksek's method, we indeed found that $3-$saturation was impossible to confirm with any reasonable range of auxiliary primes q. However, using Tate-Lichtenbaum maps we have demonstrated that the curve and points are $3-$saturated.

Some $2-$saturation examples.

Repeating our analysis with the following curves and their generators gives that these cannot be proved $2-$saturated with the Siksek method.

The curves are listed by their reference in the Cremona Database:

$$65A1, 82A2, 102A2, 112A1, 117A2, 128A1, 130A1.$$

3.4 Finishing off saturation manually.

This section uses the same method as [18]. If the saturation process has not been successful in proving $V_p = 0$ then it will leave us with a non-zero subspace $V'_p = \bigcap \mathrm{Ker}\psi_n$ of $\mathbb{F}_p^{r+s}$ containing V_p.

We define a projective subset of V'_p which we denote by S_p with the following properties:

1. if $(a_1, \ldots, a_r, b_1, \ldots, b_s) \in S_p$, then $|a_i|, |b_i| \leq (p-1)/2$ unless $p = 2$ in which case $a_i, b_i = 0$ or 1,
2. for every $(\overline{a_1}, \ldots, \overline{a_r}, \overline{b_1}, \ldots, \overline{b_s}) \in V_p \setminus \{0\}$, there exists exactly one $(a_1, \ldots, a_r, b_1, \ldots, b_s) \in S_p$ such that $(\overline{a_1}, \ldots, \overline{a_r}, \overline{b_1}, \ldots, \overline{b_s}) \equiv \beta(a_1, \ldots, a_r, b_1, \ldots, b_s)$ mod p) for some $\beta \in \mathbb{F}_p$.

It is clear that all that remains is to check for all $(a_1, \ldots, a_r, b_1, \ldots, b_s) \in S_p$, if

$$\sum_{i=1}^{r} a_i P_i + \sum_{j=1}^{s} b_j T_j = pQ \tag{3.5}$$

for some $Q \in E(K)$.

For each $(b_1, \ldots, b_{r+s}) \in S_p$ the equation 3.5 has up to p^2 solutions in $E(K)$ and a simple MAGMA function allows us to find these solutions via the division polynomial.

In our algorithm, if there is no solution to equation (3.5) then our points are $p-$ saturated and the algorithm terminates. Otherwise we choose a solution, Q. We are then able to replace one of the P_i with Q and can then repeat the whole algorithm at p to see if our points are now $p-$saturated. This process will finish in finite time because the index of $\langle P_1, \ldots, P_r \rangle$ in its saturation is finite and with each round of the algorithm, the index decreases by a factor p.

3.5 Special case of saturation at $p = 2$

In Cremona's paper [3], 2-saturation is covered and he has a proof that his method will prove 2-saturation in finite time for 2-saturated inputs. The method relies on discrete calculations, finding roots of cubics and evaluating quadratic characters modulo primes. Our method generalises this to arbitrary primes p.

3.6 Examples of proving Saturation at a given rational prime

3.6.1 Curve of rank at least 24 over $\mathbb{Q}$

This example was found by the N.S.A using methods that they have not disclosed. Our points were obtained by applying LLL-reduction to the points in the release.

$$y^2 + xy + y = x^3 - 120039822036992245303534619191166796374x$$

$$+ 504224992484910670010801799168082726759443756222911415116$$

with 24 independent points:

$(20050245580548130 68 : -164803715883430851082348882 52 : 1)$,

$(-4690836759490453344 : -3104988352578580151474452480 4 : 1)$,

$(4700156326649806635 : -6622116250158424945781859743 : 1)$,

$(6785546256295273860 : -1456180928830978521107520473 : 1)$,

$(6823803569166584943 : -1685950735477175947351774817 : 1)$,

$(7788809602110240789 : -6462981622972389783453855713 : 1)$,

$(27385442304350994620556 : 4531892554281655472841805111276996 : 1)$,

$(54284682060285253719/4 : -29660878815798901619218209042 7/8 : 1)$,

$(-94200235260395075139/25 : -3756324603619419619213452459781/125 : 1)$,

$(-34636610553318417246 47/576 : -4390335413918676900411140472877 93/13824 : 1)$,

$(-668406593403350697063 7/676 : -4730722530661906698041726571924 57/17576 : 1)$,

$(-956077386192640344198/2209 : -24483267624430969872659074691076 61/103823 : 1)$,

$(-27067471797013364392578/2809 : -41209761684451154341938868 51218259/148877 : 1),$

$(-25538866857137199063309/3721 : -71949622899374712699671287 29589169/226981 : 1),$

$(-10263250117602590518943 31/108241$

$: -1000895294067489857736110963003267773/35611289 : 1),$

$(9351361230729481250627334/1366561$

$: -286974960574863577747537233930 6204832/1597509809 : 1),$

$(1010087863587943289733 9615/1423249$

$: -530496577627696645106690094148938 7801/1697936057 : 1),$

$(1149965586821102262534 0735/17522596$

$: -151343576334154118826523024142682 6478043/73349586856 : 1),$

$(1103522536650810025178 11734/21353641$

$: -461706833308406671405570254542647784288/98675175061 : 1),$

$(414280096426033094143668538257/285204544 :$

$2666421389247913106639634997876030198338 72421/4816534339072 : 1),$

$(361017122906998280429300 87436/4098432361$

$: -2995258855766764520463389153587111670142292/262377541318859 : 1),$

$(4544246340850352421546018 3165/5424617104$

$: -3716041581470144108721590695554670156388869/399533898943808 : 1),$

$(9838860133447007076785874 82584/141566320009$

$: -1266158183877179304491616259603976057 41940953/53264752602346277 : 1),$

$(1124614335716851053281176544216033/152487126016$

$: -37714203831317877163580088877209977295481388540127/59545612760743936 : 1).$

We give below the calculations to prove that this set of points is saturated at

$p = 3$. At each rational prime q with $\#E(F_q)$ divisible by p, we use either the Siksek method or the Tate-Lichtenbaum method of finding a homomorphism ψ_n. These are applied to the 24 points to generate a row of a 24x24 matrix in $\mathbb{Z}/3\mathbb{Z}$. Note that two rows of the matrix are derived for $q = 43$, where the Tate-Lichtenbaum method has been used. The program checks that new rows are independent of previous rows.

```
p=  3  q=  37  #E(Fq)=  48  new row  1  =
[ 0, 1, 0, 2, 2, 1, 2, 1, 1, 1, 2, 2, 1, 0, 1, 2, 1, 1, 2, 1, 1, 0, 1, 1 ]
p=  3  q=  43  #E(Fq)=  54  new row  2  =
[ 0, 0, 0, 2, 1, 1, 1, 2, 2, 2, 1, 0, 2, 0, 0, 2, 2, 1, 2, 1, 2, 1, 0, 1 ]
p=  3  q=  43  #E(Fq)=  54  new row  3  =
[ 2, 1, 1, 1, 1, 0, 0, 1, 1, 2, 0, 2, 2, 0, 2, 0, 0, 0, 1, 1, 2, 0, 0, 0 ]
p=  3  q=  47  #E(Fq)=  60  new row  4  =
[ 0, 1, 0, 0, 2, 2, 2, 1, 1, 2, 0, 2, 1, 0, 2, 2, 2, 2, 0, 0, 1, 0, 2, 1 ]
p=  3  q=  61  #E(Fq)=  72  new row  5  =
[ 0, 1, 2, 0, 0, 2, 0, 1, 2, 2, 1, 1, 1, 2, 1, 0, 1, 0, 1, 2, 1, 2, 2, 0 ]
p=  3  q=  71  #E(Fq)=  87  new row  6  =
[ 1, 2, 2, 1, 2, 2, 2, 1, 2, 2, 2, 0, 0, 0, 2, 2, 2, 0, 1, 1, 2, 1, 0, 0 ]
p=  3  q=  113  #E(Fq)=  123  new row  7  =
[ 1, 0, 1, 0, 1, 1, 0, 1, 2, 0, 0, 0, 2, 1, 0, 2, 1, 0, 1, 0, 0, 0, 1, 1 ]
p=  3  q=  127  #E(Fq)=  135  new row  8  =
[ 2, 2, 1, 0, 1, 0, 2, 0, 0, 0, 1, 0, 2, 2, 0, 1, 1, 0, 2, 2, 1, 1, 1, 1 ]
p=  3  q=  131  #E(Fq)=  147  new row  9  =
[ 1, 0, 2, 1, 2, 1, 2, 2, 1, 2, 2, 2, 0, 2, 1, 2, 0, 0, 2, 1, 1, 0, 2, 2 ]
p=  3  q=  163  #E(Fq)=  174  new row  10  =
[ 1, 2, 2, 1, 0, 0, 2, 2, 2, 2, 1, 1, 1, 0, 1, 1, 2, 1, 2, 1, 0, 1, 0, 2 ]
p=  3  q=  179  #E(Fq)=  204  new row  11  =
[ 1, 1, 2, 2, 1, 0, 2, 0, 0, 0, 2, 1, 0, 1, 1, 0, 1, 0, 0, 1, 2, 1, 2, 2 ]
p=  3  q=  181  #E(Fq)=  204  new row  12  =
[ 0, 1, 2, 0, 2, 2, 1, 0, 2, 0, 0, 0, 1, 2, 0, 2, 2, 2, 0, 1, 0, 1, 2, 1 ]
p=  3  q=  211  #E(Fq)=  237  new row  13  =
[ 1, 1, 2, 1, 0, 2, 0, 2, 1, 2, 2, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 2 ]
p=  3  q=  223  #E(Fq)=  246  new row  14  =
[ 1, 0, 0, 2, 1, 1, 0, 2, 2, 1, 0, 0, 2, 2, 2, 2, 1, 1, 2, 0, 1, 2, 1, 1 ]
p=  3  q=  233  #E(Fq)=  264  new row  15  =
[ 1, 0, 2, 2, 1, 1, 0, 0, 1, 0, 2, 2, 1, 2, 2, 1, 0, 1, 1, 2, 2, 1, 0, 1 ]
p=  3  q=  251  #E(Fq)=  267  new row  16  =
[ 0, 1, 2, 2, 1, 2, 0, 1, 2, 2, 1, 0, 0, 1, 0, 2, 2, 1, 0, 2, 1, 0, 1, 0 ]
p=  3  q=  263  #E(Fq)=  264  new row  17  =
[ 1, 0, 1, 2, 0, 0, 1, 2, 2, 2, 0, 2, 1, 0, 0, 2, 2, 1, 1, 2, 0, 2, 2, 1 ]
p=  3  q=  281  #E(Fq)=  264  new row  18  =
[ 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 2, 1, 1, 2, 1, 2, 1, 2, 1, 1, 1, 2, 1, 2 ]
p=  3  q=  307  #E(Fq)=  315  new row  19  =
[ 2, 2, 0, 0, 2, 1, 2, 2, 0, 1, 0, 1, 0, 2, 0, 1, 0, 1, 0, 2, 2, 1, 1, 0 ]
p=  3  q=  311  #E(Fq)=  330  new row  20  =
[ 1, 0, 0, 2, 1, 2, 0, 0, 2, 2, 0, 2, 0, 0, 1, 1, 0, 1, 2, 0, 0, 0, 2, 0 ]
p=  3  q=  317  #E(Fq)=  336  new row  21  =
[ 0, 1, 2, 0, 2, 2, 1, 0, 2, 1, 0, 1, 0, 0, 2, 1, 1, 0, 2, 2, 0, 2, 0, 2 ]
p=  3  q=  347  #E(Fq)=  375  new row  22  =
[ 0, 1, 1, 1, 2, 0, 2, 2, 2, 2, 0, 2, 2, 2, 0, 0, 2, 0, 2, 1, 0, 0, 0, 2 ]
p=  3  q=  359  #E(Fq)=  384  new row  23  =
[ 1, 0, 1, 0, 1, 2, 1, 1, 1, 2, 1, 2, 1, 1, 1, 2, 1, 0, 0, 2, 0, 0, 0, 0 ]
p=  3  q=  373  #E(Fq)=  393  new row  24  =
[ 1, 1, 1, 2, 2, 0, 2, 0, 1, 2, 0, 2, 0, 2, 2, 1, 0, 0, 2, 0, 0, 0, 0, 1 ]
saturation complete at p = 3.
```

Further results for this curve are in section 6.4.3

3.6.2 Curve of rank at least 2 over a number field.

The curve is over number field K given by:

$$K = \mathbb{Q}[\theta] \text{ where } \theta^5 + 5\theta^3 + 5\theta - 1 = 0$$

with equation:

$$\begin{aligned} E : y^2 = x^3 + (-30\theta^3 - 100\theta + 30)x^2 + (500\theta^4 - \\ 600\theta^3 + 500\theta^2 - 1700\theta + 300)x + (4000\theta^4 \\ - 28000\theta^3 - 57000\theta + 11000) \end{aligned}$$

and points:

$$\begin{aligned} &(-25\theta^4 + 10\theta^3 - 125\theta^2 + 25\theta - 10 : 275\theta^4 - 25\theta^3 + 1425\theta^2 - 50 : 1), \\ &(-20\theta^4 + 90\theta^3 - 20\theta^2 + 180\theta - 30 : 800\theta^4 + 200\theta^3 + 1200\theta^2 - 200\theta : 1). \end{aligned}$$

This curve and set of points is from a paper by Halberstadt and Kraus [10]. In their paper they needed to demonstrate that this example is saturated.

We saturate at $p = 5$. The sieving for curves over number fields works exactly the same as over $\mathbb{Q}$ except that we look through the ideals that are prime factors of the rational primes q.

```
p= 5
p=  5  q=  7  Q = Prime Ideal of R: (7,11+t)
  #E(FQ)=  10  new row  1  =  [ 1, 1 ]
p=  5  q=  43  Q =  Prime Ideal of R: (43,76+t)
  #E(FQ)=  50  new row  2  =  [ 1, 4 ]
saturation complete at p = 5.
```

Chapter 4

Calculation of Upper Bound for the Difference between Naive and Canonical Height.

I enclose the results here from a joint paper in progress, [2], co-authored by Cremona, Siksek and myself. Siksek originally derived a method for calculating an upper bound for the difference between naive and canonical heights of points on an elliptic curve in his thesis [17]. We implemented that method as part of our saturation algorithm. We observed inefficiencies in the method, in particular whether the local contributions to the bound at finite primes could be obtained simply from the Kodaira symbol. Siksek also had thought of this - see concluding remarks of [18, p.1536]. After a meeting of the three of us, Siksek then drew on our examples and experience of how the method could be improved and worked out the details of calculating local contributions from Tate's Algorithm and it is this work I summarise here.

4.1 Statement of the Difference in Heights Bound Theorem.

The following notation is relevant to non-archimedean valuations v.

k_v	the residue field corresponding to v,
$\mathfrak{O}_v$	ring of integers in K_v,
q_v	the cardinality of the residue field k_v.

Let E be an elliptic curve given by the Weierstrass equation

$$E: \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{4.1}$$

where $a_1, \ldots, a_6$ are in the ring of integers $\mathfrak{O}_K$ of K. We define the usual associated constants (see [19, page 46]) as follows.

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned}$$

Let

$$\begin{aligned} f(P) &= 4x(P)^3 + b_2x(P)^2 + 2b_4x(P) + b_6 \\ g(P) &= x(P)^4 - b_4x(P)^2 - 2b_6x(P) - b_8. \end{aligned} \tag{4.2}$$

Define the function $\Phi_v : E(K_v) \to \mathbb{R}$ by

$$\Phi_v(P) = \begin{cases} 1 & \text{if } P = O, \\ \frac{\max\{|f(P)|_v, |g(P)|_v\}}{\max\{1, |x(P)|_v\}^4} & \text{otherwise.} \end{cases} \tag{4.3}$$

It is easy to see that Φ_v is a continuous and hence bounded function on $E(K_v)$

Kodaira type of $E_v^{\min}$ at v	Tamagawa index c_v	α_v
any	1	0
$\mathrm{I_m}$, m even	2 or m	$m/4$
$\mathrm{I_m}$, m odd	m	$(m^2-1)/4m$
III	2	$1/2$
IV	3	$2/3$
I_0^*	2 or 4	1
I_m^*	2	1
I_m^*	4	$(m+4)/4$
IV^*	3	$4/3$
III^*	2	$3/2$

(the boundedness follows immediately from the fact that $E(K_v)$ is compact with respect to the v-adic topology). Define

$$\epsilon_v^{-1} = \inf_{P\in E(K_v)} \Phi_v(P), \qquad \delta_v^{-1} = \sup_{P\in E(K_v)} \Phi_v(P), \tag{4.4}$$

where the exponents -1 have been chosen to simplify the formulae appearing later. In [18, Lemma 2.3, page 1508] it is shown that ϵ_v exists (i.e. the infimum is not 0) and satisfies $\epsilon_v \geq 1$. A similar argument shows that δ_v exists.

We define naive height $h(P) : P \in E(K)$ in Chapter 5. The canonical height $\hat{h}(P)$ is defined by

$$\lim_{N\to\infty} 4^{-N}h([2^N]P).$$

For each non-archimedean valuation v, let $E_v^{\min}$ be a minimal model for E over K_v, and let $\Delta_v^{\min}$ be the discriminant of $E_v^{\min}$. Thus we can take $E_v^{\min} = E$ and $\Delta_v^{\min} = \Delta$ for almost all non-archimedean valuations v, and they are always equal if the model E is global minimal. For non-archimedean valuations v define the constants α_v according to the Kodaira type of $E_v^{\min}$ and the Tamagawa index c_v as in the table above.

Theorem 4.1.1. *For all $P \in E(K)$,*

$$\frac{1}{3[K:\mathbb{Q}]}\sum_{v\in M_K^\infty} n_v \log \delta_v \leq h(P) - \hat{h}(P) \leq \frac{1}{3[K:\mathbb{Q}]}\sum_{v\in M_K^\infty} n_v \log \epsilon_v$$
$$+\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^0}\left(\alpha_v + \frac{1}{6}\mathrm{ord}_v(\Delta/\Delta_v^{\min})\right)\log(q_v).$$

Definition 4.1.2. *We refer to the upper bound in the above theorem as the Cremona-Prickett-Siksek bound (C.P.S.) in this thesis.*

The following theorem is a byproduct of the proof of Theorem 4.1.1. In essence it says that the bounds are sharper if we restrict ourselves to points that have everywhere good reduction. This result has proved highly useful in the bounding of the saturation index bound in Chapter 6.

Theorem 4.1.3. *Suppose $P \in E(K)$. If $P \in E_0(K_v)$ for all non-archimedean valuations v then*

$$\frac{1}{3[K:\mathbb{Q}]}\sum_{v\in M_K^\infty} n_v \log \delta_v \leq h(P) - \hat{h}(P) \leq \frac{1}{3[K:\mathbb{Q}]}\sum_{v\in M_K^\infty} n_v \log \epsilon_v.$$

4.2 The Real Contributions

To be able to compute the bounds in our Theorem 4.1.1 we need a method for determining δ_v and ϵ_v for archimedean valuations v. In this section we give such a method for real valuations v. Thus suppose that v is a real valuation; in other words, there is an embedding $\sigma : K \to \mathbb{R}$ such that $|a|_v = |\sigma(a)|$ for all $a \in K$. To ease the notation, we will henceforth think of all elements of K as lying in $\mathbb{R}$ via this embedding σ.

Write

$$\begin{aligned} f(x) &= 4x^3 + b_2x^2 + 2b_4x + b_6, \\ g(x) &= x^4 - b_4x^2 - 2b_6x - b_8. \end{aligned}$$

and let

$$F(x) = x^4 f(1/x), \qquad G(x) = x^4 g(1/x).$$

Define

$$\begin{aligned} D &= \{x \in [-1,1] : f(x) \geq 0\}, \\ D' &= \{x \in [-1,1] : F(x) \geq 0\}. \end{aligned}$$

The following lemma is elementary.

Lemma 4.2.1. *Define constants d, d' by*

$$\begin{aligned} d &= \inf_{x \in D} \max\{|f(x)|, |g(x)|\}, \\ d' &= \inf_{x \in D'} \max\{|F(x)|, |G(x)|\}, \end{aligned}$$

and constants e, e' by

$$\begin{aligned} e &= \sup_{x \in D} \max\{|f(x)|, |g(x)|\}, \\ e' &= \sup_{x \in D'} \max\{|F(x)|, |G(x)|\}. \end{aligned}$$

Then $\epsilon_v = \min(d, d')^{-1}$ and $\delta_v = \max(e, e')^{-1}$. where ϵ_v and δ_v are as defined in 4.4.

It is clear that D, D' can be written as finite unions of disjoint closed intervals. Moreover the problem of determining δ_v and ϵ_v has been reduced to the problem of determining d, d', e, e'. This is straightforward by the following lemma.

Lemma 4.2.2. *If f, g are continuous real functions and I is a closed interval then the infimum and supremum of the continuous function* $\max\{|f(X)|, |g(X)|\}$ *over the interval I are attained at two of the following points*

(i) an end point of I,

(ii) at one of the roots of f, g, $f+g$, $f-g$ in the interval I,

(iii) at a turning point of one of the functions f, g.

4.3 The Complex Contributions

In this section we consider the determination of δ_v and ϵ_v for complex archimedean valuations v. As in the previous section, think of all elements of K as lying in $\mathbb{C}$ via a suitable embedding.

Let $f,\ g,\ F,\ G$ be as in the previous section, and now let $D = \{z \in \mathbb{C} : |z| \leq 1\}$ be the unit disc. The following lemma is elementary.

Lemma 4.3.1. *Define constants $d,\ d'$ by*

$$\begin{aligned} d &= \inf_{z\in D} \max\{|f(z)|, |g(z)|\}, \\ d' &= \inf_{z\in D} \max\{|F(z)|, |G(z)|\}, \end{aligned}$$

and constants $e,\ e'$ by

$$\begin{aligned} e &= \sup_{z\in D} \max\{|f(z)|, |g(z)|\}, \\ e' &= \sup_{z\in D} \max\{|F(z)|, |G(z)|\}. \end{aligned}$$

Then $\epsilon_v = \min(d, d')^{-1}$ and $\delta_v = \max(e, e')^{-1}$.

Write $z = x + iy$ and $f = f_1 + if_2,\ g = g_1 + ig_2$ where $f_i,\ g_i$ are real polynomials in $x,\ y$.

Lemma 4.3.2. *The supremum of the function $\max\{|f(z)|, |g(z)|\}$ on the region D is attained at a point $z = x + iy$ that satisfies one of the following pairs of simultaneous equations:*

- $f_1^2 + f_2^2 = g_1^2 + g_2^2, \qquad x^2 + y^2 = 1,$
- $y\frac{\partial(f_1^2+f_2^2)}{\partial x} - x\frac{\partial(f_1^2+f_2^2)}{\partial y} = 0, \qquad x^2 + y^2 = 1,$
- $y\frac{\partial(g_1^2+g_2^2)}{\partial x} - x\frac{\partial(g_1^2+g_2^2)}{\partial y} = 0, \qquad x^2 + y^2 = 1.$

The infimum of the function $\max\{|f(z)|, |g(z)|\}$ on D is attained at a point $z = x + iy$ satisfying one of the above pairs of simultaneous equations or at a *point $z = x + iy$ belonging to the interior $x^2 + y^2 < 1$ and satisfying these two simultaneous equations:*

$$f_1^2 + f_2^2 = g_1^2 + g_2^2, \qquad \frac{\partial(f_1^2 + f_2^2)}{\partial x}\frac{\partial(g_1^2 + g_2^2)}{\partial y} - \frac{(f_1^2 + f_2^2)}{\partial y}\frac{(g_1^2 + g_2^2)}{\partial x} = 0.$$

To compute $d,\ d',\ e,\ e'$ and hence $\epsilon_v,\ \delta_v$ we need to solve pairs of polynomial equations in two variables. These can be solved using elimination theory. Once these pairs of equations are solved we need to discard any solutions that do not belong to D.

4.4 Silverman's bound

Silverman gives an upper bound [20] on the difference between the naive and canonical height of points on $E(K)$. This is quick to calculate on a computer, and so we have implemented both the Silverman and the C.P.S. bound and take the lowest upper bound of the two.

Theorem 4.4.1. *(Silverman) Let $E(K)$ be an elliptic curve given by a Weierstrass equation (4.1). Let Δ be the discriminant of the equation (4.1) and let j be the $j-$invariant of E. Further let*

$$2^* = \begin{cases} 2 & \textit{if } b_2 \neq 0, \\ 1 & \textit{if } b_2 = 0. \end{cases}$$

Define 'height of E' by

$$\mu(E) = \frac{1}{12}h(\Delta) + \frac{1}{12}h_\infty(j) + \frac{1}{2}h_\infty(\frac{b_2}{12}) + \frac{1}{2}\log(2^*)$$

where for $t \in K$,

$$h_\infty = \frac{1}{[K:\mathbb{Q}]}\sum_{v \in M_K^\infty} n_v \log(\max(1, |t|_v))$$

Then for all $P \in E(\overline{K})$,

$$h(P) - \hat{h}(P) \leq \frac{1}{12}h(j) + 2\mu(E) + 1.922.$$

Proof. See [20]. □

4.5 Examples and Numerical Comparisons

Our examples only illustrate calculation of the C.P.S. upper bound, as the lower bound has no application in this thesis.

Example 1. Consider the (randomly chosen) curve

$$E: \qquad y^2 = x^3 + (1+5i)x + (3+i)$$

over the field $K = \mathbb{Q}(i)$.

We seek an upper bound for $h - \hat{h}$ using our Theorem 4.1.1. The discriminant of the curve is

$$1280 + 4448i = -i(1+i)^{10}(40 + 139i),$$

where the last factor is prime. Since the discriminant was not divisible by any 12–th powers we saw that the curve is global minimal. Our computer program gave us the C.P.S. (Cremona, Prickett, Siksek) upper bound derived from implementing this chapter of

$$h(P) - \hat{h}(P) \leq 0.1149$$

for all $P \in E(K)$. Silverman's bounds for the same curve are

$$h(P) - \hat{h}(P) \leq 5.7584.$$

Example 2. Consider the curve E from Halberstadt and Kraus [10] which we have already used in section 3.6.2.

$$\begin{aligned}y^2 = x^3 &+ (-30\theta^3 - 100\theta + 30)x^2 + (500\theta^4 - 600\theta^3 + 500\theta^2 \\ &- 1700\theta + 300)x + (4000\theta^4 - 28000\theta^3 - 57000\theta + 11000)\end{aligned}$$

over Number Field K given by

$$K = \mathbb{Q}[x]/(x^5 + 5x^3 + 5x - 1).$$

The Silverman bound is 11.4279 for the difference of heights, and this was calculated very quickly.

The C.P.S (Cremona, Prickett, Siksek) upper bound on the other hand took longer to calculate, since it was necessary to calculate Groebner bases for the complex and real prime valuations.

There are four complex valuations and one real valuation. The C.P.S upper bound for all points was calculated to be 15.7283, larger than the Silverman bound.

Next, we calculated the C.P.S. upper bound for the height difference for everywhere good reduction points. This was calculated to be 0.8850 since only archimedean primes contribute and most of the contribution in the previous case was from the non-archimedean primes. These two runs took $\frac{1}{2}$ hour to execute.

Chapter 5

Searching for points on E(K) of bounded naive height

Our aim is to describe an algorithm which finds all points on $E(K)$ of bounded logarithmic naive height $\leq b$, given $b \in \mathbb{R}^{+}$.

Using the method of chapter 4 to bound the difference d between naive and canonical height, we will then have found all points of $E(K)$ of bounded canonical height $\leq b - d$ if that quantity is positive. The lower bound on the canonical height of points is used in chapter 6 as a vital part of our Saturation Algorithm.

We require the following notation in addition to that defined in section (1.2).

For each non-archimedean or archimedean valuation, v we define $n_v = [K_v : \mathbb{Q}_v]$ where K_v is the completion of K by this valuation.

We write M_K^0 and M_K^∞ for the sets of non-archimedean and archimedean valuations on K respectively, with M_K denoting their union.

The standard definition (see [19, pp.207] of naive logarithmic height of the point

$P = (x : y : 1)$ on $E(K)$ is:

$$h(P) = h(x) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \max\{0, \log |x|_v\} \tag{5.1}$$

with associated naive height:

$$H(x) = \exp(h(x)) = \prod_{v \in M_K} \max\{1, |x|_v\}^{\frac{n_v}{[K:\mathbb{Q}]}}$$

and I also define

$$H^{\infty}(x) = \prod_{v \in M_K^{\infty}} \max\{1, |x|_v\}^{\frac{n_v}{[K:\mathbb{Q}]}},$$

$$H^{0}(x) = \prod_{v \in M_K^{0}} \max\{1, |x|_v\}^{\frac{n_v}{[K:\mathbb{Q}]}},$$

with

$$H(x) = H^{\infty}(x) H^{0}(x).$$

For non-archimedean valuations we define for consistency,

$$|x|_v = N(\mathfrak{p})^{\frac{-\mathrm{ord}_{\mathfrak{p}}(x)}{n_v}}.$$

For real archimedean valuations, v, take corresponding embedding $\alpha : K \hookrightarrow \mathbb{R}$ and define

$$|x|_v = \| x^{\alpha} \|_{\mathbb{R}},$$

where $\| \, . \, \|_{\mathbb{R}}$ is the absolute value. For complex archimedean valuations, v, take corresponding embedding $\alpha : K \hookrightarrow \mathbb{C}$ and define

$$|x|_v = \| x^{\alpha} \|_{\mathbb{C}},$$

where $\| \, . \, \|_{\mathbb{C}}$ is the absolute value.

Suppose $h(P) = h(x) \leq b$ for $b \in \mathbb{R}^{+}$. Let $B = \exp(b[K:\mathbb{Q}])$. Hence $H(x)^{[K:\mathbb{Q}]} \leq B$.

It follows that

$$|x|_v \leq B^{\frac{1}{n_v}} \quad \forall v. \tag{5.2}$$

Now, $H(x) \geq H^0(x)$ since $H^\infty(x) \geq 1$ and so $H^0(x)^{[K:\mathbb{Q}]} \leq B$. But taking $(x) = \mathfrak{a}\mathfrak{b}^{-1}$, $(\mathfrak{a}, \mathfrak{b} \lhd \mathfrak{O}_K$ coprime ideals) it is clear that $H^0(x)^{[K:\mathbb{Q}]} = N(\mathfrak{b})$ and $N(\mathfrak{b}) \leq B$.

We search for all such ideals $\mathfrak{b} : N(\mathfrak{b}) \leq B$, assisted by the fact that $\mathfrak{b}$ is a perfect square ideal since it is the denominator ideal of the x coordinate of a point. We find corresponding ideals $\mathfrak{c}$ such that $\mathfrak{b}.\mathfrak{c} = (d)$ for principal ideals $(d), d \in \mathfrak{O}_K$. Hence for any $P : h(P)$ =$h((x:y:1))$= $h(x) \leq b$, it follows that $(x) = \mathfrak{a}\mathfrak{c}(d)^{-1}$ for some $\mathfrak{a}$,$\mathfrak{c}$, and d chosen by our algorithm.

For each archimedean valuation v_j there is a corresponding injection $\sigma_j : K \hookrightarrow \mathbb{C}$, considering $\mathbb{R}$ as a subset of $\mathbb{C}$ for the real archimedean valuations.

Taking each d in turn from our list, and letting $g_j = x^{\sigma_j} d^{\sigma_j}$ we have

$$\| g_j \|_{\mathbb{C}} \leq B \| d^{\sigma_j} \|_{\mathbb{C}},$$
$$g_j = \sum t_i \pi_i^{\sigma_j},$$

where π_i is an integral basis for $\mathfrak{c}$ and $t_i \in \mathbb{Z}$. Writing $t = (t_i)$ and $P = (\pi_i^{\sigma_j})$ and $g = (g_j)$ gives us that

$$tP = g.$$

P is clearly invertible since σ_j are independent and injective and the π_i are independent.

Hence we can write

$$t = gP^{-1}.$$

This is the crux of our algorithm. For each d in our list and corresponding $\mathfrak{c}$, we construct P. We have the bound on g that $\| g_j \|_{\mathbb{C}} \leq B \| d^{\sigma_j} \|_{\mathbb{C}}$.

Hence

$$\| t_j \|_{\mathbb{C}} = \| \sum_i g_i P_{i,j}^{-1} \|_{\mathbb{C}} \leq \sum_i \| g_i \|_{\mathbb{C}} \| P_{i,j}^{-1} \|_{\mathbb{C}} \leq B \sum_i \| d^{\sigma_i} \|_{\mathbb{C}} \| P_{i,j}^{-1} \|_{\mathbb{C}} .$$

Thus we can consider each integer vector t with this bound, and hence determine each g and hence each possible x.

Lastly for each point $P = (x : y : 1)$ found using the algorithm, we check that $h(P) \leq b$ using Equation (5.1).

5.1 Example of searching for points.

Let E be an elliptic curve taken from Serf's thesis [15],

$$y^2 + 2xy + \frac{1}{2}(-\sqrt{5} - 3)y = x^3 - 2x^2 + \frac{1}{2}(\sqrt{5} + 1)x + \frac{1}{2}(-\sqrt{5} - 1)$$

defined over number field

$$K = \mathbb{Q}(\sqrt{5})$$

We searched for points of naive height less than or equal to 1. This implied searching for points with denominators given by ideals of norm bounded above by $\exp(2) = 7.389$.

No denominator ideals were found, and so we searched over the algebraic integers only, which gave the following points:

Point	Naive Height
$(\frac{1}{2}(\sqrt{5}+5) : \sqrt{5}+1 : 1)$	0.805
$(\frac{1}{2}(\sqrt{5}+1) : 0 : 1)$	0.241
$(0 : 1 : 1)$	0
$(\frac{1}{2}(-\sqrt{5}+1) : \sqrt{5} : 1)$	0.241
$(\frac{1}{2}(\sqrt{5}+3) : \frac{1}{2}(\sqrt{5}+1) : 1)$	0.481

$(0 : 1 : 1)$ is the point with smallest canonical height (0.212)with naive height bounded above by 1 and $(\frac{1}{2}(-\sqrt{5}+1) : \sqrt{5} : 1)$ is the everywhere good reduction point (see Chapter 6) with smallest canonical height given these constraints.

5.2 Using searching for points in our Saturation Algorithm

In conjunction with the upper bound on the difference between naive and canonical heights from Chapter 4, we now have an algorithm for finding the finite sets[1]:

- $\{P \in E(K) : \hat{h}(P) \leq c\}$,
- $\{P \in E_{gr}(K) : \hat{h}(P) \leq c\}$,

and hence for determining $\lambda, \lambda_{gr} > 0$ such that:

- $\{P \in E(K) : 0 < \hat{h}(P) < \lambda\} = \emptyset$,
- $\{P \in E_{gr}(K) : 0 < \hat{h}(P) < \lambda_{gr}\} = \emptyset$.

This means that a saturation index bound can be calculated as in Chapter 6.

[1] We define $E_{gr}(K)$ in Chapter 6, section 6.2.1.

Chapter 6

The Saturation Algorithm

Definition 6.0.1. *The index of saturation of* $L = \langle P_1, \ldots, P_s \rangle \leq \hat{E}(K)$ *is* $[\overline{L} : L]$ *where* $\overline{L}$ *is the saturation of* L*.*

We calculate a bound on the index of saturation (saturation index bound) by geometry of numbers arguments. Three methods for calculating it are given in this section and we use whichever is the lowest of the three answers in our programs. Chapter 4 is a prerequisite for this work, for relating bounds on naive height to bounds on canonical height.

6.1 Full Search to find Saturation Index Bound

The following subsection is an abbreviated version of [18, section 3]. I include lemmas without proofs.

Define $\hat{E}(K) = E(K)/Tor(E(K))$ where $Tor(E(K)$ is the torsion subgroup of $E(K)$. Suppose $P_1, \ldots, P_r$ generate a sublattice of $\hat{E}(K)$ which has index of saturation, n. Suppose $n > 1$. We define the height pairing matrix of $P_1, \ldots, P_r$ as:

$$H(P_1, \ldots, P_r) = (\langle P_i, P_j \rangle)_{i,j=1,\ldots,r},$$

where for all $P, Q \in E(K)$:

$$\langle P, Q\rangle := \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)).$$

Definition 6.1.1. *The regulator, $R(P_1, \ldots, P_s)$, is defined to be the absolute value of the determinant of the height pairing matrix $H(P_1, \ldots, P_s)$. The regulator $R(M) = R(Q_1, \ldots, Q_t)$ where M is a sublattice of points on $\hat{E}(K)$, of rank t with a basis $Q_1, \ldots, Q_t$.*

Remark 6.1.2. *Clearly whichever basis is chosen in Definition 6.1.1 will give the same regulator since two bases are related by a matrix of determinant ±1.*

Remark 6.1.3. *Note that if $L' \supseteqq L$ and $[L' : L] < \infty$ then*

$$R(L) = [L' : L]^2 R(L').$$

Taking $L = \langle P_1, \ldots, P_s\rangle$ if the index of saturation is n then it follows by remark 6.1.2 that

$$R(\overline{L}) = \frac{1}{n^2} R(L).$$

Lemma 6.1.4. *(Hermite, Minkowski and others) Suppose*

$$f(\mathbf{x}) = \sum_{i,j=1}^{w} f_{i,j} x_i x_j, \tag{6.1}$$

where $(f_{i,j})$ is a symmetric positive definite matrix with determinant

$$D = det(f_{i,j}) > 0. \tag{6.2}$$

Then there exists a positive constant γ_w such that

$$\inf_{\mathbf{m} \neq 0 \; integral} f(\mathbf{m}) \leq \gamma_w D^{\frac{1}{w}}. \tag{6.3}$$

Moreover we can take

$$\gamma_1^1 = 1, \gamma_2^2 = \frac{4}{3}, \gamma_3^3 = 2, \gamma_4^4 = 4,$$
$$\gamma_5^5 = 8, \gamma_6^6 = \frac{64}{3}, \gamma_7^7 = 64, \gamma_8^8 = 2^8,$$

and for $w \geq 9$

$$\gamma_w = (\frac{4}{\pi})\Gamma(\frac{w}{2}+1)^{\frac{2}{w}}.$$

Lemma 6.1.5. *Let E be an elliptic curve defined over a number field K. Let $L = \langle P_1, \ldots, P_w \rangle$, a sublattice of $\hat{E}(K)$ of rank w. Let $R(\overline{L})$ be the regulator of the saturation of L. If the rank w is ≥ 1 then there exists a point Q in $\overline{L}$ of infinite order such that*

$$\hat{h}(Q) \leq \gamma_w R(\overline{L})^{\frac{1}{w}}.$$

Theorem 6.1.6. *Let E be an elliptic curve defined over a number field K. Suppose that $E(K)$ contains no point Q of infinite order with canonical height $\hat{h}(Q) \leq \lambda$ where λ is some positive real number. Suppose that $P_1, \ldots, P_w$ generate a sublattice of $E(K)$ of rank $w \geq 1$. Then the index of saturation, n of $P_1, \ldots, P_w$ in $\hat{E}(k)$ satisfies*

$$n \leq R(P_1, \ldots, P_w)^{\frac{1}{2}}(\frac{\gamma_w}{\lambda})^{\frac{w}{2}}, \tag{6.4}$$

where

$$\gamma_1^1 = 1, \gamma_2^2 = \frac{4}{3}, \gamma_3^3 = 2, \gamma_4^4 = 4,$$
$$\gamma_5^5 = 8, \gamma_6^6 = \frac{64}{3}, \gamma_7^7 = 64, \gamma_8^8 = 2^8,$$

and for $w \geq 9$

$$\gamma_w = (\frac{4}{\pi})\Gamma(\frac{w}{2}+1)^{\frac{2}{w}}.$$

6.1.1 Example.

We have calculated a saturation index bound for the sublattice H of points on

$$y^2 + \frac{1}{2}(\sqrt{5}+3)y = x^3 + \sqrt{5}x^2 + \frac{1}{2}(-\sqrt{5}-1)x + \frac{1}{2}(-\sqrt{5}-1)$$

over

$$K = \mathbb{Q}(\sqrt{5})$$

where H is spanned by

$$(0 : \frac{1}{2}(-\sqrt{5}-1) : 1)\ ,\ (\frac{1}{2}(-\sqrt{5}+1) : \frac{1}{2}(-\sqrt{5}-3) : 1)$$

using the methods of this section.

This curve is taken from [15],[5].

The Silverman bound for all points is 5.982 and the C.P.S bound for all points is 0.284.

A lower bound on the canonical height of points is 0.016 found by searching up to naive height $b = 0.3$. Note this is equal to $0.3 - 0.284$ since no points were found with smaller canonical height.

The regulator of the two points given is 0.059.

This gives a saturation index bound of $17 = \lfloor 0.059^{0.5} \times (\frac{2}{0.016 \times \sqrt{3}}) \rfloor$.

6.2 Calculation of Index of Everywhere Good Reduction Subgroup.

The height bounds calculated in Chapter 4 are generally much smaller for points with good (non-singular) reduction at all non-archimedean primes. Thus we have reduced the saturation problem to considering only the subgroup of points with such good reduction, hence taking advantage of these small bounds when we calculate an index of saturation bound. The initial stage is to calculate the index of the everywhere good reduction subgroup.

6.2.1 Notation and background.

We use the notation in section 1.1, together with the following:

Let $v \in M_K$ be a valuation.

Let $E^0(K_v)$ be the connected component of $E(K_v)$. For v a complex valuation, (or if v is a real valuation with $\sigma : K \to \mathbb{R}$ being the associated real embedding, and $\sigma(\Delta) < 0$) then this is all of $E(K_v)$. If v is real and $\sigma(\Delta) > 0$ then $[E(\mathbb{R}) : E^0(\mathbb{R})] = 2$. Otherwise, for v non-archimedean, $E^0(K_v) = \{P \in E(K_v) : P \text{ has good reduction at } v\}$.

We define $C_v = E(K_v)/E^0(K_v)$, the component group at v.

Proposition 6.2.1. *The group $E(K)/E^0(K)$ is finite. If E has split multiplicative reduction then it is cyclic. In all other cases it has order at most 4.*

Proof. See [19, Corollary 15.2.1 p.359]. □

Definition 6.2.2. *The Tamagawa number, $c_v = |C_v|$.*

If E has good reduction at v then $E(K_v) = E^0(K_v)$ and so $C_v = 0$ giving $c_v = 1$.

Remark 6.2.3. $c_v < \infty$ *for all* $v \in M_K$ *and* $c_v = 1$ *for almost all* $v \in M_K$.

Definition 6.2.4. $E_{gr}(K) = E(K) \cap_{v \in M_K} E^0(K_v)$. *This is the subgroup of points on $E(K)$ of good reduction at all valuations.*

Definition 6.2.5. *If H is a sublattice of $E(K)$ then we define $H_{gr} = H \cap E_{gr}(K)$.*

It is clear from the above that by the definition of $E_{gr}(K)$,

$$E(K)/E_{gr}(K) \hookrightarrow \bigoplus_{v \in M_K} E(K_v)/E^0(K_v), \tag{6.5}$$

and that $\bigoplus_{v \in M_K} E(K_v)/E^0(K_v)$ is a finite abelian group of order $\Pi_v c_v$.

6.2.2 Calculating $[\overline{H} : \overline{H}_{gr}]$.

We have the diagram of inclusions:

$$\begin{tikzcd}
& \overline{H} \arrow[dl, dash] \arrow[dr, dash] & \\
H \arrow[dr, dash] & & \overline{H}_{gr} \arrow[dl, dash] \\
& H_{gr} &
\end{tikzcd}$$

Given the curve $E(K)$ and the set of s points $P_1, \ldots, P_s \in E(K)$ which span the subgroup H of $E(K)$, we need to calculate $[\overline{H} : \overline{H}_{gr}]$.

Definition 6.2.6. *A Tamagawa prime for $E(K)$ is a rational prime dividing $\Pi_v c_v$.*

We need to assume that the index of saturation $[\overline{H} : H]$ is not divisible by any Tamagawa primes. It is easy to ensure this via saturation at all Tamagawa primes using the method of Chapter 3 on the individual primes. This is possible as Tamagawa primes are in practice small.

It follows from (6.5) that

$$\overline{H}/\overline{H}_{gr} \hookrightarrow \bigoplus_v C_v.$$

Also,

$$|[H : H_{gr}]| \Big| |[\overline{H} : \overline{H}_{gr}]|$$

by the second isomorphism theorem, and since H is saturated at all Tamagawa primes, and only these primes divide the order of $\overline{H}/\overline{H}_{gr}$, it follows that

$$|[H : H_{gr}]| = |[\overline{H} : \overline{H}_{gr}]|.$$

Since we have generators of H we can use MAGMA to calculate the index of the gr-subgroup. We do this by constructing a matrix M with rows referenced by the points $P_1, \ldots, P_s$ and columns by the valuations v_j for which C_v is non-trivial.

As we have observed, C_v is usually cyclic but for the other possibility that $C_v = C_2 \times C_2$ we need two columns for that valuation v in our matrix.

We define μ_v as the natural map

$$\mu_v : H \to C_v.$$

We can choose a map $\nu_v : C_v \hookrightarrow \mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. With this choice fixed, we can represent the image of a point P_i under μ_{v_j} as one element of $\mathbb{Z}/m\mathbb{Z}$ for some integer m or as two elements of $\mathbb{Z}/2\mathbb{Z}$.

6.2.3 Brief description of method of calculating $\nu_{v_j}\mu_{v_j}$

In the case $C_v \ncong C_2 \times C_2$, and hence is cyclic, the key is to find a point G whose image under μ_{v_j} generates $\mu_v(H)$. We do this iteratively by choosing G_t in turn whose image generates the images of all of $P_1, \ldots, P_t : t \leq s$.

Having at stage t pre-calculated G_{t-1} and the order of its image, γ_{t-1}, we calculate π_t, the order of $\mu_{v_j}(P_t)$, by testing multiples of P_t to see if they lie in $E_{gr}(K)$. Taking chosen multiples of G_{t-1} and P_t we can construct points R_t and S_t with images $\mu_{v_j}(R_t), \mu_{v_j}(S_t)$ of coprime order ρ_t and σ_t, with $\rho_t \sigma_t = \gamma_{t-1}\pi_t$. We can then use the extended Euclid's algorithm to calculate a new G_t whose image $\mu_{v_j}(G_t)$ generates images $\mu_{v_j}(R_t), \mu_{v_j}(S_t)$ and hence $\mu_{v_j}(G_{t-1}), \mu_{v_j}(P_t)$. Thus in particular, G_t generates $\langle \mu_{v_j}(P_1), \ldots, \mu_{v_j}(P_t) \rangle$ as required.

In the case $C_v \cong C_2 \times C_2$, we take the points giving the first two different non-zero images as the generators G_1 and G_2. Then all other points give images equal to that given by one of $0, G_1, G_2, G_1 + G_2$ and we can represent these images in terms of those of the generators.

In both cases, having obtained our generators it is an easy matter to take a discrete log of the images of points $P_1, \ldots, P_s$ with respect to our generators. This gives a map from $H \to \mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as required.

¿From the μ_v we obtain the homomorphism $H \to \oplus C_v$ as $\oplus \mu_v$. Hence $[H : H_{gr}]$ is the order of the image of this.

MAGMA is able to calculate this order, having inbuilt functions to calculate the order of a group with prescribed generators.

6.2.4 Note on use of the index in our algorithms.

We need both the index of the Everywhere Good Reduction Subgroup defined above and also the index of the subgroup that has good reduction at all non-archimedean valuations but not necessarily at archimedean valuations. The latter is easily calculated by repeating the above analysis but replacing M_K, the set of valuations of K with M_K^0 the set of non-archimedean valuations of K.

6.2.5 Example.

We again use the curve E of rank at least 24 over $\mathbb{Q}$ produced by the N.S.A:

$$\begin{aligned} y^2 + xy + y = x^3 &- 120039822036992245303534619191166796374x \\ &+ 504224992484910670010801799168082726759443756222911415116 \end{aligned}$$

The set of 24 independent points that we use is listed in section 3.6.1. They span H, a subgroup of $E(\mathbb{Q})$. We calculate the index $[\overline{H} : \overline{H}_{gr}]$:

Bad primes	2	3	5	11	13	17	29	31	41	p_{10}[1]	p_{11}[2]
Tamagawa Numbers	2	9	2	6	2	2	2	3	2	1	1
Kodaira Symbols	I_2	I_9	I_2	I_6	I_2	I_2	I_2	I_3	I_2	I_1	I_1
P_1	1	1	1	2	1	1	1	0	0	0	0
P_2	1	7	1	2	0	0	1	0	0	0	0
P_3	0	5	1	0	1	0	0	1	0	0	0
P_4	0	1	1	4	1	0	0	2	1	0	0
P_5	0	3	1	3	1	1	1	1	0	0	0
P_6	0	5	1	5	1	0	0	2	1	0	0
P_7	0	6	1	2	1	0	0	2	0	0	0
P_8	0	8	1	3	0	1	1	2	1	0	0
P_9	0	7	1	4	1	1	0	1	0	0	0
P_{10}	1	3	0	2	0	1	1	1	1	0	0
P_{11}	0	0	0	4	1	1	1	2	1	0	0
P_{12}	0	1	0	3	0	1	1	1	0	0	0
P_{13}	1	4	0	0	1	1	0	2	0	0	0
P_{14}	1	2	1	1	0	1	0	2	1	0	0
P_{15}	1	6	1	1	1	1	0	2	0	0	0
P_{16}	0	8	1	5	0	0	0	1	1	0	0
P_{17}	1	3	0	1	1	1	0	2	0	0	0
P_{18}	1	1	1	0	1	1	1	2	0	0	0
P_{19}	0	2	0	4	1	0	0	1	0	0	0
P_{20}	0	2	1	2	0	0	1	1	1	0	0
P_{21}	1	2	1	4	0	1	1	2	0	0	0
P_{22}	0	4	0	4	0	1	1	1	1	0	0
P_{23}	1	0	0	0	0	1	1	2	0	0	0
P_{24}	1	4	1	5	1	1	2	1	2	0	0

We include for completeness the matrix recording whether each of the 24 points

[1] 458619970494582607679296750333015081

[2] 264240973182971699094661154229360236070105974082503

are in the good reduction subgroup over the real valuation $v_{\mathbb{R}}$ only or not.

Image of point in $C_{v_{\mathbb{R}}}$																							
1	0	0	0	1	1	0	0	1	1	0	0	1	0	0	1	1	1	0	0	1	1	0	1

We calculated that $[\overline{H} : \overline{H}_{gr}] = 10368$, excluding and $= 20736$ including the archimedean primes when calculating the Everywhere Good Reduction Subgroup. The exponent of the groups is 18.

Remark 6.2.7. *The program ran in seconds although for this example, the bad primes had to be calculated previously by factorising the discriminant, a factorisation that takes many hours on our computer. We anticipate that if our method is applied to curves with large discriminant, factorising that discriminant may prove a stumbling block.*

6.3 Search of Everywhere Good Reduction Subgroup to calculate Saturation Index Bound.

The theory of Section 6.1 can be amended in a straightforward way to restrict to just everywhere good reduction points. The advantage of these is that the upper bound on the difference between naive and canonical heights is much less since there are no contributions from finite primes.

We use the notation of Subsection 6.2.

Suppose we have the diagram of inclusions:

$$\begin{tikzcd}
 & \overline{H} \arrow[dl, dash] \arrow[dr, dash] & \\
H \arrow[dr, dash] & & \overline{H}_{gr} \arrow[dl, dash] \\
 & H_{gr} &
\end{tikzcd}$$

where $H = \langle P_1, \dots, P_s \rangle$ is the subgroup generated by the points that are known on the curve.

We ensure as in Section 6.2 that $m = [\overline{H} : H]$ is not divisible by Tamagawa primes by saturating H at these primes.

Thus we know that $n = [\overline{H} : \overline{H}_{gr}]$, which is a product of Tamagawa primes, is coprime to $[\overline{H} : H]$. It follows that $[\overline{H} : H] = [\overline{H}_{gr} : H_{gr}]$.

Proposition 6.3.1. *The index of saturation (n) is bounded above as follows*

$$n = [\overline{H} : H] = [\overline{H}_{gr} : H_{gr}] \leq [\overline{H} : \overline{H}_{gr}] R(P_1, \dots, P_s)^{\frac{1}{2}} (\frac{\gamma_s}{\lambda_{gr}})^{\frac{s}{2}}.$$

Note that $\overline{H}_{gr}$ is chosen to have good reduction with respect to all non-archimedean valuations only. This is because the difference in heights bound calculated in section 4 tends to be much lower for points with such good reduction.

The quantity on RHS of the above inequality is a saturation index bound.

Proof. The result follows using Equation 6.4 in Theorem 6.1.6, noting that the sublattice H_{gr} has regulator $[\overline{H} : \overline{H}_{gr}]^2 R(P_1, \dots, P_s)$. □

6.3.1 Example.

We apply the method of this subsection to the elliptic curve defined by

$$y^2 = x^3 - 379340164x + 2858976058624$$

over $\mathbb{Q}$ obtained from Cremona. We wish to saturate the subgroup H of the Mordell-Weil group spanned by the following independent points

$$(11550 : -135632 : 1), (11830 : 164248 : 1), (9086 : -402976 : 1),$$
$$(11116 : -125636 : 1), (14000 : 540568 : 1), (7728 : 623672 : 1),$$
$$(1456 : 1519784 : 1), (-19712 : 1636208 : 1).$$

The index of good reduction for H $(= [\overline{H} : \overline{H}_{gr}])$ was found to be 1 excluding and including the real valuation.

The Silverman bound for all points is 17.9748,

The C.P.S. bound for all points is 6.8712, whilst the C.P.S. bound for everywhere good reduction points is 3.8856.

After searching for points up to naive logarithmic height 13, we obtained a lower bound on the canonical height of points with everywhere good reduction at non-archimedean primes of 6.1288 ($\gamma_8 = 2.0000$.)

This gives a saturation index bound of $3 = \left\lfloor 1 \times 113614.5942^{0.5} \times (\frac{2.0000}{6.1288})^{\frac{8}{2}} \right\rfloor$.

In a few seconds of computer time we established that the subgroup spanned by these points is saturated by saturating at primes 2 and 3 using the method of Chapter 3.

6.4 Finding a Saturation Index Bound without any searching.

In this section we only consider $E(K)$ over K which are totally real. Otherwise this method cannot be applied. This method is joint work with Samir Siksek.

Our method gives a lower bound on the canonical height of good reduction points on $E(K)$ without searching for points. The problem with searching is that sometimes it may take too long, whereas this method is very fast to execute on a computer. However the method may return a negative real number for the bound, which although giving a true statement does not help us. We ran the method of this section on the curves from Cremona's Tables [4] in the below table to gain insight into the method.

conductor range	number of curves	proportion giving positive bound
1 – 8000	27250	54%
8000 – 12000	15438	61%
12000 – 20000	32859	64%

This analysis of these $70,000$ curves leads us to believe that our method is a useful complement to the other techniques in this thesis.

Our canonical height and local heights will be double those in Silverman's book [21].

Theorem 6.4.1. *Let K be a totally real field and let E be a Weierstrass elliptic curve with coefficients $a_1, \dots, a_6 \in \mathfrak{O}_K$. Suppose that the point $P \in E(K)$ satisfies $P \in E^0(K_v)$ for all valuations v including the archimedean ones. For each archimedean valuation, v, fix (compatible) isomorphisms $K_v \cong \mathbb{R}$ and $\overline{K_v} \cong \mathbb{C}$. Consider the isomorphisms:*

$$E(\mathbb{C}) \cong \frac{\mathbb{C}}{\mathbb{Z}\omega_{v,1} + \mathbb{Z}\omega_{v,2}} \cong \frac{\mathbb{C}}{\mathbb{Z} + \mathbb{Z}\tau_v},$$

where $\omega_{v,1}$ = least positive real period, $\omega_{v,2}$ = least period $\notin \mathbb{Z}\omega_{v,1}$, and τ_v = point in fundamental domain for $SL(2,\mathbb{Z})$ equivalent to $\omega_{v,2}/\omega_{v,1}$.

Define

$$\begin{aligned} q_v =& e^{2\pi i \tau_v}, \\ M^\infty_{K,\leq} =& \{v \in M^\infty_K : |\omega_{v,1}| \leq |\omega_{v,2}|\}, \\ M^\infty_{K,>} =& \{v \in M^\infty_K : |\omega_{v,1}| > |\omega_{v,2}|\}. \end{aligned}$$

Then it follows that

$$\begin{aligned} \hat{h}(P) \geq & \frac{1}{6}\log|\mathrm{Norm}_{K/\mathbb{Q}}\Delta| - 2\log 2 + \frac{1}{[K:\mathbb{Q}]}\sum_{v \in M^\infty_{K,\leq}} \left(\frac{\pi \mathrm{Im}(\tau_v)}{3} - \frac{4|q_v|}{1-|q_v|} \right) \\ & + \frac{1}{[K:\mathbb{Q}]}\sum_{v \in M^\infty_{K,>}} \left(\frac{-\pi \mathrm{Im}(\tau_v)}{6} - \frac{2(1+|q_v|^2)}{1-|q_v|} \right). \end{aligned}$$

Proof. Recall that [21, Chapter VI]:

$$\hat{h}(P) = \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K} n_v\lambda_v(P) = \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^0} n_v\lambda_v(P) + \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^\infty} \lambda_v(P).$$

Here $n_v = 1$ for all archimedean places since K is totally real. We will bound the non-archimedean and archimedean sums separately. Recall that P has everywhere good reduction. Then

$$\lambda_v(P) = \log\max\{1, |x(P)|_v\} - \frac{1}{6}\log|\Delta|_v \geq \frac{-1}{6}\log|\Delta|_v.$$

for all non-archimedean v (see [21, Theorem VI.4.1]). Hence

$$\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K^0} n_v\lambda_v(P) \geq -\frac{1}{6}\log\prod_{v\in M_K^0}|\Delta|_v^{n_v} = \frac{1}{6}\log|\mathrm{Norm}_{K/\mathbb{Q}}\Delta|$$

using the product formula. The rest follows from the lower bounds for the non-archimedean contributions given in the following lemma. □

Lemma 6.4.2. *Let E be an elliptic curve defined over $\mathbb{R}$. Let τ be the period of E belonging to the usual fundamental domain in the lattice $E \cong \frac{\mathbb{C}}{\mathbb{Z}+\mathbb{Z}\tau_v}$. Let $q = e^{2\pi i\tau}$. If $P \in E^0(\mathbb{R})$ then*

$$\lambda_{\mathbb{R}}(P) \geq \frac{\pi\mathrm{Im}(\tau)}{3} - 2\log 2 - \frac{4|q|}{1-|q|} \geq -0.49.$$

Proof. Let z be the image of P under the isomorphism $E(\mathbb{C}) \to \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$. Now the local height function

$$\lambda_{\mathbb{R}} : \frac{\mathbb{C}}{\mathbb{Z}+\mathbb{Z}\tau} \to \mathbb{R}$$

is given by

$$\lambda(z) = -B_2\left(\frac{\mathrm{Im}(z)}{\mathrm{Im}(\tau)}\right)\log|q| - 2\log|1-u| - 2\sum_{n\geq 1}\log|(1-q^n u)(1-q^n u^{-1})|,$$

where $B_2(T) = T^2 - T + 1/6$, and $u = e^{2\pi iz}$ and $q = e^{2\pi i\tau}$ (see [21, Theorem VI.3.4]).

To prove the Lemma we want to calculate or estimate each of the terms in the formula for $\lambda(z)$ above:

6.4.1 Case I: Real Weierstrass period of $E(K)$ has smallest or equal modulus

In this case,

$$\tau = \frac{\omega_2}{\omega_1}$$

lies in the fundamental domain. Since $P \in E^0(\mathbb{R})$, and z is a real multiple of the image of P under $E \cong \frac{\mathbb{C}}{\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2}$ therefore $Im(z) = 0$. Hence, $Im(\tau)$ is either ≥ 1 if ω_2 is pure imaginary or $\geq \frac{\sqrt{3}}{2}$ otherwise.

First: $-B_2\left(\frac{\mathrm{Im}(z)}{\mathrm{Im}(\tau)}\right) \log |q| = \frac{\pi \mathrm{Im}\tau}{3}$.

Second: u is on the unit disc and hence $|1-u| \leq 2$. Hence $-2\log|1-u| \geq -2\log 2$.

Third: Note that

$$|(1-q^n u)(1-q^n u^{-1})| = |1 - q^n(u+u^{-1}) + q^{2n}| \leq 1 + 2|q|^n + |q|^{2n} = (1+|q|^n)^2.$$

Since τ is in the usual fundamental domain, it follows that $\mathrm{Im}(\tau) \geq \sqrt{3}/2$. Hence $0 < |q| \leq e^{-\pi\sqrt{3}}$. In particular, as $|q| < 1$ we see that

$$\log|(1-q^n u)(1-q^n u^{-1})| \leq 2\log(1+|q|^n) \leq 2|q|^n.$$

Finally

$$-2\sum_{n\geq 1} \log|(1-q^n u)(1-q^n u^{-1})| \geq \frac{-4|q|}{1-|q|}.$$

The Lemma follows at once in this case from these three estimates and the above inequalities for $\mathrm{Im}(\tau)$ and $|q|$.

6.4.2 Case II: Real Weierstrass Period of E(K) has greatest modulus

Here we do not know that $Im(z) = 0$ and have no inequalities for $Im(\tau)$ but we can still bound our expressions. We may assume that z lies in the fundamental domain given by periods 1 and τ.

Since $\mathrm{Im}(z) \leq \mathrm{Im}(\tau)$, hence $|u| \geq |q|$. It follows immediately that, $|u + u^{-1}| \leq |q + q^{-1}|$.

First: Since $B_2(x) \geq -\frac{1}{12}$, it follows that $-B_2\left(\frac{\mathrm{Im}(z)}{\mathrm{Im}(\tau)}\right)\log|q| \geq -\frac{\pi \mathrm{Im}\tau}{6}$.

Second: u is on the unit disc and hence $|1-u| \leq 2$. Hence $-2\log|1-u| \geq -2\log 2$.

Third: Note that

$$|(1-q^n u)(1-q^n u^{-1})| = |1 - q^n(u+u^{-1}) + q^{2n}| \leq (1+|q|^{n+1})(1+|q|^{n-1}).$$

Hence:

$$-2\sum_n \log|(1-q^n u)(1-q^n u^{-1})| \geq \frac{-2(1+|q|^2)}{(1-|q|)}.$$

The Lemma follows at once in this case from these three inequalities.

□

6.4.3 Example 1.

We again use the curve E of rank at least 24 over $\mathbb{Q}$ produced by the N.S.A:

$$y^2 + xy + y = x^3 - 120039822036992245303534619191166796374x$$
$$+ 504224992484910670010801799168082726759443756222911415116$$

The set of 24 independent points that we use is listed in section 3.6.1. They span H, a subgroup of $E(\mathbb{Q})$.

Our programs calculated: $[\overline{H} : \overline{H}_{gr}] = 10368$ over all archimedean valuations in $M^0_{\mathbb{Q}}$.

$[\overline{H} : \overline{H}_{gr}] = 20736$ over all valuations in $M_{\mathbb{Q}}$.

The C.P.S bound for all points is 16.644 and for e.g.r. points only is 0.926.

The Silverman bound is 71.279.

The lower bound on canonical height of g.r points over all of $M_{\mathbb{Q}}$ derived from method of this subsection is 39.315.

The lower bound on canonical height of g.r. points over all of $M^0_{\mathbb{Q}}$ derived from searching for points is 11.074.

The lower bound on canonical height of all points was not possible to calculate as the corresponding C.P.S bound is too high.

The saturation index bound N given by the above is given by

$$N \leq 20736 \times (1.049 \times 10^{26})^{0.5} \times (\frac{6.734}{39.315})^{12} = 1.354 \times 10^{8}.$$

Unfortunately, this thesis does not provide a practical method to saturate these points on $E(\mathbb{Q})$ since the saturation index bound is too high to saturate at all primes p lower than it in a reasonable time.

Nonetheless this example demonstrates that the method of bounding the index of saturation without searching does form another useful tool to achieve saturation of points on curves.

6.4.4 Example 2.

We apply the method of this section to the elliptic curve defined by

$$y^2 = x^3 + 2429469980725060x^2 + 275130703388172136833647756388x$$

over $\mathbb{Q}$.

We wish to saturate subgroup H of the Mordell-Weil group spanned by the following points:

$$
\begin{aligned}
&(4859338299729438 : 416471863148635757166984 : 1),\\
&(-1655376807922479 : 408139823161823125040037 : 1),\\
&(-13783163903211906/25 : 2559282848641379326053672/125 : 1),\\
&(2189707338529593 : 150832925221536994856391 : 1),\\
&(117386244964836 : -8209204785115731247572 : 1),\\
&(3501548111333769 : -271445468504099342225871 : 1),\\
&(179104002703038 : 11530632350958995292984 : 1),\\
&(2189707338529593/4 : -258329262728233934936469/8 : 1),\\
&(-24962853836057298/121 : -8189783230960490403311592/1331 : 1),\\
&(-22466568452451 5682/121 : -5092060590625302734827 0104/1331 : 1),\\
&(-168194075588658 : -42064757738349510 36168 : 1),\\
&(46011795801039 3006/25 : 3321874585040076783675570 96/125 : 1),\\
&(-1528299258985359 : -410412130127644817397 33 : 1),\\
&(-13139608245811133778/11881 : 4695311564704258650327711 5928/1295029 : 1).
\end{aligned}
$$

The curve and points are from work of Stephane Fermigier [7]. At rank 14, the curve has the highest proved rank of any curve. Other curves such as the N.S.A. curve (3.6.1) earlier have higher but unknown rank.

The index of good reduction for H $(= [\overline{H} : \overline{H}_{gr}])$ is found to be 1024 excluding and including the real valuation.

The Silverman bound for all points is 85.133,

The C.P.S. bound for all points is 45.273, whilst the C.P.S. bound for everywhere good reduction points is 10.513.

After searching for points up to naive logarithmic height 14, we obtained a lower bound on the canonical height of points with everywhere good reduction at non-archimedean primes of 3.4868 ($\gamma_{14} = 4.3036$) using the method of section 6.3.

However the method of this section gives a lower bound on the canonical height of points with everywhere good reduction at all primes of 30.4940 which is a vastly better bound for our purposes.

This gives a saturation index bound of $13375 = 1024 \times (1.372 \times 10^{14})^{0.5} \times (\frac{4.3036}{30.494})^{\frac{14}{2}}$.

In 1.5 days of computer time we established that the subgroup spanned by these points is saturated, by saturating at all rational primes up to 13375 using the method of Chapter 3.

Chapter 7

Examples of uses of programs.

7.1 Proving sets of points independent.

We give here a complementary use of our saturation algorithm as described in Chapter 3 to give a method of proving that points $P_1, \ldots, P_s$ on elliptic curve $E(K)$ are independent, i.e. that if

$$\sum a_i P_i = 0$$

for $a_i \in \mathbb{Z}$, then every $a_i = 0$.

In Chapter 3, we found methods of proving that there were no non-trivial solutions to equation (3)

$$(3) \qquad pQ = \sum_{i=1}^{s} a_i P_i + \sum_{j=1}^{t} b_j T_j,$$

where $T_j : j \leq 2$ are a basis for the $p-$power torsion points of $E(K)$.

The difference between our application of equation (3) here and in Chapter

3 is that here we do not assume that the P_i are independent when we solve the equation. (Recall that in Chapter 3 we solve equation (3) by calculating homomorphisms $\psi : E(K) \to \mathbb{F}_p$.)

Theorem 7.1.1. *Suppose for given E/K and given $P_1, \ldots, P_s$ we choose p such that there are no $p-$torsion points on E/K (always possible because Torsion Subgroup is finite) and such that equation (3) has no non-trivial solutions (not always possible [1]). Then $P_1, \ldots, P_s$ are independent.*

Proof. Suppose $P_1, \ldots P_s$ are dependent. Then we can choose

$$\sum a_i P_i = 0$$

with not all $a_i = 0$, $a_i \in \mathbb{Z}$ and also with $\sum a_i$ minimal.

Suppose also that equation(3) has no non-trivial solutions. Thus p divides all a_i. Let $b_i = \frac{a_i}{p} \in \mathbb{Z}$. The point $\sum b_i P_i$ is a p-torsion point and must hence be the 0 by choice of p. Hence we have

$$\sum b_i P_i = 0$$

with not all $b_i = 0$, $b_i \in \mathbb{Z}$ but $\sum b_i < \sum a_i$ which gives a contradiction. □

This method of proving points independent is composed of discrete calculations, whereas the alternative method of calculating the regulator of the points involves judging whether a real value is non-zero, thus requiring knowledge of the error in the Canonical Height function.

The condition of equation (3) having no non-trivial solutions is a stronger condition than $P_1, \ldots P_s$ being independent. For these reasons, both this method and the regulator method do not always prove that independent points are independent.

[1] e.g. take any E/K, $P_1 = P_2 = P \in E(K)$ and $p = 2$ then $2Q = P_1 + P_2$ has solution $Q = P$

We now demonstrate our method and compare it with the regulator method. All three examples are run on curves from Serf's thesis [15].

7.1.1 Example 1

For the elliptic curve

$$y^2 + (-\sqrt{5}+1)xy = x^3 + (-\sqrt{5}-2)x - 1$$

we found these points

$$\begin{aligned}&(\frac{1}{8}(3\sqrt{5}-9) : \frac{1}{8}(-5\sqrt{5}+6) : 1),\\ &(-1 : -\sqrt{5} : 1),\\ &(-9\sqrt{5}+18 : -41\sqrt{5}+90 : 1)\end{aligned}$$

to be independent in 0.43 seconds by our method and in 1.36 seconds by the regulator method.

7.1.2 Example 2

For the elliptic curve

$$y^2 - 2xy + 2y = x^3 + \frac{1}{2}(\sqrt{5}+1)x^2 + \sqrt{5}x - 2$$

we found these points

$$\begin{aligned}&(\frac{1}{8}(-3\sqrt{5}-9) : \frac{1}{8}(-4\sqrt{5}-23) : 1),\\ &(-1 : \frac{1}{2}(-\sqrt{5}-3) : 1),\\ &(-13\sqrt{5}+28 : \frac{1}{2}(167\sqrt{5}-379) : 1)\end{aligned}$$

to be independent in 0.429 seconds by our method and in 1.32 seconds by the regulator method.

7.1.3 Example 3

For the elliptic curve

$$y^2 - 2xy + (-\sqrt{5} + 1)y = x^3 + \frac{1}{2}(-\sqrt{5} - 5)x^2 + \frac{1}{2}(\sqrt{5} - 3)x$$

we found these points

$$\begin{aligned}&(\frac{1}{8}(3\sqrt{5} - 1) : \frac{1}{8}(2\sqrt{5} + 5) : 1),\\ &(\frac{1}{2}(\sqrt{5} - 1) : \frac{1}{2}(3\sqrt{5} - 5) : 1),\\ &(\frac{1}{2}(-23\sqrt{5} + 51) : \frac{1}{2}(141\sqrt{5} - 315) : 1)\end{aligned}$$

to be independent in 0.51 seconds by our method and in 1.48 seconds by the regulator method.

7.2 Searching for points of bounded naive height

We searched for points on the curve from Serf's thesis [15]

$$y^2 + 2xy + \frac{1}{2}(-\sqrt{5} - 3)y = x^3 - 2x^2 + \frac{1}{2}(\sqrt{5} + 1)x + \frac{1}{2}(-\sqrt{5} - 1)$$

over

$$K = \mathbb{Q}(\sqrt{5})$$

up to naive height bound 1.30. This took time 19.6 seconds.

The program determined that no denominators were needed in the search; only algebraic integers needed to be searched.

The least canonical height of a point with naive height less than 1.30 is 0.21174 for point $(0, 1)$, and the least canonical height of a point of everywhere good reduction at non-archimedean valuations with naive height less than 1.30 is 0.38176 for the point $(\frac{1}{2}(-\sqrt{5} + 1), \sqrt{5})$.

Secondly, we searched for points on another curve from Serf's thesis [15]:

$$y^2 + 2xy - 2\sqrt{2}y = x^3 + (-\sqrt{2}+1)x^2 + (-2\sqrt{2}-2)x + (-2\sqrt{2}+2)$$

up to naive height bound 1.30. This took time 26.6 seconds.

The program searched for points with denominator 2.

The least canonical height of a point with naive height less than 1.30 was 1.1639 for the everywhere good reduction point at non-archimedean valuations $(\sqrt{2}+1 : \sqrt{2}-2 : 1)$.

7.3 Calculation of bounds on difference between naive and canonical height.

1. We used the elliptic curve from Halberstadt and Kraus, [10] defined by

$$\begin{aligned} y^2 = x^3 &+ (-30\alpha^3 - 100\alpha + 30)x^2 + \\ &(500\alpha^4 - 600\alpha^3 + 500\alpha^2 - 1700\alpha + 300)x + \\ &(4000\alpha^4 - 28000\alpha^3 - 57000\alpha + 11000) \end{aligned} \tag{7.1}$$

   over

$$K = \mathbb{Q}(\alpha)$$

   where α is a root of $t^5 + 5t^3 + 5t - 1 = 0$

   The time taken to calculate height bounds was 874.9 seconds. The C.P.S. bound for egr points is 0.885 and was for all points 15.728. The Silverman bound is 11.428.

2. We used the elliptic curve defined by

$$y^2 = x^3 - 9217x + 300985$$

over $\mathbb{Q}$.

The Silverman bound is 11.441, the C.P.S. bound for egr points is 0.000, and the C.P.S. bound for all points is 0.462.

3. We used the elliptic curve defined by

$$y^2 = x^3 - 240604x + 45804256$$

over $\mathbb{Q}$.

The Silverman bound is 13.425, the C.P.S. bound for egr points is 2.534 and the C.P.S. bound for all points is 3.747.

4. We used the elliptic curve defined by

$$y^2 = x^3 - 4954801x + 4270189489$$

over $\mathbb{Q}$.

The Silverman bound is 16.156, the C.P.S. bound for egr points is 3.134, and the C.P.S. bound for all points is 3.596.

7.4 Calculation of Everywhere Good Reduction Index.

1. We used the elliptic curve from Serf's thesis [15] given by

$$y^2 = x^3 + (-\sqrt{13}+2)x^2 + (-\sqrt{13}+2)x + (\sqrt{13}-2).$$

$E(K)$ has rank 2 and we considered the sublattice given by the points

$$(\frac{1}{2}(\sqrt{13}-3) : -1 : 1),$$
$$(\sqrt{13}+1 : -\sqrt{13}-4 : 1).$$

The programs took 9 seconds to calculate the EGR indices for this sublattice. Both the EGR index at archimedean valuations and the EGR index at all valuations were found to be 3.

2. We used the elliptic curve from Serf's thesis [15] given by

$$y^2 = x^3 + (-\sqrt{3} - 2)x^2 - 3x + (3\sqrt{3} - 2)$$

over

$$K = \mathbb{Q}(\sqrt{3}).$$

$E(K)$ has rank 2 and we considered the sublattice given by the points

$$\begin{aligned}
&(-\sqrt{3} - 2 : 5\sqrt{3} + 10 : 1),\\
&(\frac{1}{121}(-1405\sqrt{3} + 1756) : 1/1331(-77612\sqrt{3} + 169325) : 1).
\end{aligned}$$

The programs took 3 seconds to calculate the EGR indices for this sublattice. Both the EGR index at archimedean valuations and the EGR index at all valuations was found to be 1.

7.5 Saturation.

We saturated the elliptic curve, E, cited by Thomas Kretschmer in [13, page 633] given by

$$y^2 + xy = x^3 - 5818216808130x + 5401285759982786436$$

over $\mathbb{Q}$.

The curve, E, was also used in Samir Siksek's thesis [17] to demonstrate calculations of an upper bound on naive height minus canonical height. He gave eight independent points on the curve which when 3-saturated give these points:

$(1145136 : 489626526 : 1), (987594 : 785948706 : 1), (1284264 : -218219910 : 1),$

$(1573410 : 376054914 : 1), (1365048 : 51389034 : 1), (1467138 : -152933892 : 1),$

$(1368480 : -45144546 : 1), (1437384 : -90242214 : 1).$

John Cremona proved that E has rank 8 by using 2-descent.

By using the method of section 6.4, which involves no searching for points, we obtained a saturation index bound of 509. Lastly, E was proved saturated by saturating for all primes p up to 509. The process took 5 minutes. Since E has rank 8, the set of 8 independent points above was hence proved to be a basis for $E(K)/E_{Tors}(K)$.

This example demonstrates how the method of section 6.4 can be essential to achieve saturation. In this example, searching for points takes too long to be practical.

Bibliography

[1] J. Cassels, E.V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, C.U.P.

[2] J.E.Cremona, M.J.Prickett, S.Siksek, *Bounds for the difference between Naive and Canonical Height.*, in preparation.

[3] J.E.Cremona, *On the computation of Mordell-Weil and 2-Selmer Groups of Elliptic Curves*,Rocky Mountain Journal of Mathematics, Vol 32 (2002). pages 953–967.

[4] J.E.Cremona *Tables of Elliptic Curves*,
http://www.maths.nott.ac.uk/personal/jec/ftp/data

[5] J.E.Cremona and P.Serf, *Computing the rank of elliptic curves over real quadratic fields of class number* 1., Mathematics of Computation, Vol. 68, no 227 (1999), pages 1187–1200.

[6] R. Dvornicich and U. Zannier, *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France 129 (2001), no. 3, pages 317–338.

[7] S. Fermigier *Exemples de courbes elliptiques de grand rang sur* $\mathbb{Q}(t)$ *et sur* $\mathbb{Q}$ *possédant des points d'ordre* 2 (1996),C.R. Acad. Sci. Paris Sér. I Math.,Vol. 322, pages 949–957.

[8] Gerhard Frey , Hans-Georg Ruck, Mathematics of Computation, *A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves.* Volume 62, Issue 206 (Apr.1994), 866.

[9] Gerhard Frey, Michael Muller, Hans-Georg Ruck,*The Tate Pairing and the Discrete Logarithm applied to Elliptic Curve Cryptosystems.* IEEE Transactions on Information Theory. Vol 45, No 5 July 1999.

[10] E. Halberstadt and A Kraus, *Une conjecture de V.A. Lebesgue* Journal of the London Mathematical Society, (to appear.)

[11] G.J. van der Heiden, *Local-global problem for Drinfeld Modules.*, Journal of Number Theory, Volume 104, Issue 2, February 2004. pages 193-209.

[12] G.J.Janusz, *Algebraic Number Fields* Graduate Studies in Mathematics, 1996, Vol. 7, American Mathematical Society, page 217.

[13] T.J. Kretschmer, *Construction of Elliptic Curves with Large Rank* Math. Comp. 46 (1986), pages 627-635.

[14] M.J.Prickett and J.E.Cremona *MAGMA implementation of Saturation of Mordell-Weil Groups of Elliptic Curves over Number Fields.*, http://www.maths.nott.ac.uk/personal/pmxpm

[15] P.Serf,*The rank of elliptic curves over real quadratic fields of class number* 1., Ph.D. thesis, Universitat de Saarlandes, 1995.

[16] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*,Invent. Math., Volume 15, No.4, 1972, pages 259-331.

[17] Samir Siksek, *Descents on Curves of Genus 1.* PhD Thesis. Exeter. 1995.

[18] S. Siksek, *Infinite descent on elliptic curves*, Rocky Mountain Journal of Mathematics **25**, number 4 (Fall 1990), pages 1501–1538.

[19] J.H. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, 1986.

[20] J.H. Silverman, *The Difference between the Weil Height and the Canonical Height on Elliptic Curves*, Math. Comp. **55** (1990), pages 723-743.

[21] J. H. Silverman,*Advanced topics in the Arithmetic of elliptic curves*, GTM 151, Springer-Verlag, 1994.