FINDING ELLIPTIC CURVES AND FAMILIES OF ELLIPTIC CURVES OVER Q OF LARGE RANK

BY GARIKAI CAMPBELL

A dissertation submitted to the

Graduate School—New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Mathematics

Written under the direction of

Jerrold B. Tunnell

and approved by

New Brunswick, New Jersey

January, 1999

ABSTRACT OF THE DISSERTATION

Finding Elliptic Curves and Families of Elliptic Curves over Q of Large Rank

by Garikai Campbell

Dissertation Director: Jerrold B. Tunnell

One of the most fundamental questions one can ask about elliptic curves is "what abelian groups arise as the group of an elliptic curve defined over the rationals?" By well known results of Mordell (generalized to other number fields by Weil) and of Mazur (similarly generalized by Merel), we know that the groups are finitely generated and that the torsion subgroups must be one of fifteen possible groups, with each possibility occuring. What is not known is how large the free part, more precisely the rank, of the group of an elliptic curve can be. Most believe that for every positive integer M, there exists an elliptic curve defined over $\mathbb{Q}$ whose group has rank greater than M. One other naturally related question for which there is not enough evidence to provide a reasonable conjecture is "for every positive integer M and possible torsion group T, is there an elliptic curve whose group has rank greater than M and whose torsion subgroup is T?" Even if we could answer these questions, we would still like to produce examples of such curves. This thesis reviews and extends some of the techniques used to produce elliptic curves and infinite families of elliptic curves defined over $\mathbb{Q}$ of large rank. While we do address the full breadth of this problem, we will pay particular attention to producing infinite families of elliptic curves with specified torsion.

Acknowledgements

I have completed this doctoral program with financial support from many sources. I would like to thank the Mellon Foundation, the General Electric Foundation, the National Science Foundation and the Rutgers University Minority Advancement Program.

I would like to also thank my advisor, Jerrold Tunnell, for suggesting this thesis problem, for all his help in attacking the problem and for all his support in getting past the times I was stuck!

In the last year I have had the opportunity to teach and complete my research at Swarthmore College as a Minority Scholar in Residence Fellow. This has been both an invaluable experience and a great pleasure. I have enjoyed the interaction and help from each of the professors. I would like to thank Charles James and Gene Klotz in particular, for bringing this fellowship to my attention and for encouraging me to apply.

I have also been involved with a number of summer programs which have helped in my development as a mathematician. Most notable is the PDP Program for which I would like to thank Uri Treisman, Leon Henkin and Carl Pomerance. Thank you all for encouraging me to pursue a PhD and for your continued support.

I believe that students learn the most from their interaction with other students and my graduate experience has been true to this. I would like to thank my fellow graduate students, Jenny Kelley, Naomi Klarreich, Terri Girardi and Luke Higgins in particular, for their support over the past few years.

I would also like to acknowledge and thank the support and inspiration of personal friends and family. Specifically I would like to thank my brothers Sekou and Britt Campbell, Peter Alfinito, John Byars, Martin Hunt, Bob Dougherty and C. Roy Epps. Others who I would like to acknowledge include Chris Towse, Susan Gooen, Rafael Irizarry, Ben Hansen and my many friends at NACME.

Dedication

To my parents, my wife and my children.

Thank you mom and dad for all the encouragement and support, but thank you most for being my first and greatest educators. Thank you Diana for sharing your love, strength, and dreams along this journey; I have been blessed to have you as guide and companion. Finally, I have been told that while it may seem like this journey is coming to an end, it is really only beginning and I agree. So, to my parents, to my wife and to my two sons, thank you for helping me to a great beginning and for keeping me excited about what is to come.

Table of Contents

Chapter 1

An Introduction to the Problem

1.1 Preliminaries

1.1.1 Statement of the Problem

A *curve* is a *projective* variety of dimension one. A *smooth curve* is one for which there exists a well defined, non-vanishing tangent at every point on the curve. Any smooth curve defined over a field K is described by a set of equations with coefficients in K. To be precise, let C be any curve. We call the *homogeneous ideal of* C, the ideal generated by

$$\{F \ \epsilon \ \overline{K}[x_0, x_1, ..., x_n] \mid F \text{ is homogeneous and } F(P) = 0 \text{ for all } P \ \epsilon \ C\}.$$

We denote this ideal by $I(C)$. If in fact this ideal can be generated by homogeneous polynomials in $K[x_0, x_1, ..., x_n]$, then the curve is said to be *defined over* K. The homogeneous ideal may be generated by many different sets of polynomials and we would like to distinguish between the curve and any particular representation of this ideal describing the curve. It is for this reason, we make the following definition. Let C be any curve and let $\{F_1, F_2, ..., F_m\}$ be a set of generators for $I(C)$. We call the set of equations $\{F_1 = 0, F_2 = 0, ..., F_m = 0\}$ a *projective model* for the curve C.

Very often, we will want to refer to some affine piece of a curve. We have the problem of distinguishing between the curve and a particular representation of the curve here as well. In this case, we want to be careful to remember that the curve is a projective variety even if we are representing some affine piece of the curve. And so, for any curve C, we again begin by letting $\{F_1, F_2, ..., F_m\}$ be a set of generators for the *homogeneous* ideal $I(C)$. Furthermore, for some fixed variable x and for each $j \ \epsilon \ \{1, 2, ..., m\}$, we let f_j be the dehomogenization of F_j with respect to x. We call the set of equations $\{f_1 = 0, f_2 = 0, ..., f_m = 0\}$ an *(affine) model* for the curve C.

For any curve $C \subset \mathbb{P}^n(\overline{K})$ defined over a field K, we define the $K-$*rational* points of C, denoted $C(K)$, to be $C \cap \mathbb{P}^n(K)$. A measure of the complexity of a curve is the *genus*, as defined in the Riemann-Roch Theorem. Perhaps, the most simple of the smooth curves are the conics. We will say that a *conic defined over* K is a smooth curve of genus zero defined over K. We have the easy but important theorem:

Theorem 1.1.1 *If C is a conic defined over K and $C(K)$ is not empty, then $C(K)$ is isomorphic to $\mathbb{P}^1(K)$.*

This theorem says that we can parameterize the solutions to any model of a conic, as long as there is at least one solution. Elliptic curves can be thought of as curves of complexity one level greater than conics. An *elliptic curve*, E, defined over a field K, is a smooth curve of genus one with at least one K-rational point. By contrast to our fairly complete understanding of conics, our understanding of elliptic curves is quite minimal.

If we attempt to parameterize the K-rational points on an elliptic curve in the way we parameterize the K-rational points on the conic, we discover that (in general) this is not possible. This leads quite naturally to the discovery that the set of $K-$rational points, $E(K)$, on an elliptic curve form an abelian group. A fundamental question we then ask is: what groups can $E(K)$ be? Mordell proved that if $K = \mathbb{Q}$, then

$$E(K) \cong \mathbb{T} \oplus \mathbb{Z}^r$$

with $\mathbb{T}$ a finite group. Weil proved that the group $E(K)$ is in fact finitely generated for any number field K. This fact has since been further extended to other fields (see [25, section III.6]); in particular, $E(\mathbb{Q}(t))$ is finitely generated.

Furthermore, Mazur proved that if $K = \mathbb{Q}$, then $\mathbb{T}$ is one of the following:

1. $\mathbb{Z}/n\mathbb{Z}$ where $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$
2. $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ where $n \in \{2, 4, 6, 8\}$

and that each occur as the torsion subgroup of some elliptic curve. Merel has since extended this theorem and proved the strong uniform boundedness conjecture: if K

is a number field, then the order of the torsion subgroup of $E(K)$ is bounded by a constant which depends only on the degree of K over $\mathbb{Q}$.

These theorems of Mordell, Weil, Mazur and Merel have brought us very far in answering the question of what groups $E(K)$ can be, but they do not answer it completely. In particular, we do not know what values of rank are possible for elliptic curves– not in the case of elliptic curves defined over a general field K, nor in the more specific case of $K = \mathbb{Q}$. A major open question in the study of elliptic curves is whether or not the rank is bounded. We present the following "folklore" conjecture:

Conjecture 1.1.2 *For any positive integer M, there exists an elliptic curve defined over $\mathbb{Q}$ such that the rank of $E(\mathbb{Q})$ is greater than M.*

A good deal of evidence has been collected, both experimental and theoretical, to support this conjecture. The analogous statement:

> *For any (allowable) group $\mathbb{T}$, there exists an elliptic curve E with torsion subgroup equal to $\mathbb{T}$ and rank at least M,*

does not have the same well established foundation. While the statement is certainly reasonable, it is also conceivable that the existence of certain torsion places restrictions on the rank of the elliptic curve.

Ideally, we would like to have a *constructive* proof of the conjecture and, if true, the statement as well– one which provides an *effective* method for producing *arbitrarily* large rank with or without some specified torsion. No such method currently exists and so we ask the slightly more tame question: how do we construct or find elliptic curves with *very* large rank with or without some specified torsion?

1.1.2 Prior Results

Experimental results define what we mean by "large rank" and so we begin by listing some of the highest known ranks of elliptic curves defined over $\mathbb{Q}$. The list is split into four standard categories.

	Curves		Infinite Families of Curves	
	Rank	Source	Rank	Source
unknown or trivial torsion	$r \geq 12$	Mestre [13]	$r \geq 11$	Mestre [14]
	$r \geq 21$	Nagao, Kouya [23]	$r \geq 12$	Mestre [15]
	$r \geq 22$	Fermigier [4]	$r \geq 13$	Nagao [19]
			$r \geq 14$	Kihara [7]
known torsion	$r_2 = 10$	Kretschmer [11]	$r_2 \geq 6$	Nagao [20]
	$r_2 \geq 14$	Fermigier [3]	$r_2 \geq 8$	Fermigier [3]
			$r_2 \geq 9$	Kihara [6]
			$r_{2\oplus 2} \geq 4$	Kihara [8]
			$r_{2\oplus 2} \geq 5$	Kihara [9]

In the known torsion categories a subscript of n or $2 \oplus n$ indicates that the torsion subgroup is known to contain the group $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, respectively. We will continue to use this notation to denote the rank of an elliptic curve with known torsion.

1.1.3 The Techniques

There are many techniques one can use to find elliptic curves of large rank and the list above reflects that. We restrict our attention to two of these techniques, the finite field method and the polynomial method, each of which can be attributed to Mestre. Each of these techniques follow the same general structure:

1. **Constructing Phase:** In this phase of the process, we produce a family of elliptic curves defined over the rationals which we believe to contain curves of high rank. In the case of the finite field method, we suspect that the curves we get during this phase have high rank based on a standard conjecture. In the case of the polynomial method, we construct curves with a prescribed number of points which we suspect to be linearly independent.

2. **Sieving Phase:** When trying to produce a single elliptic curve defined over the rationals of high rank, we take the family of curves produced in the previous

step and for each curve in that list, compute some value(s) associated to the curve. Based on these values, we choose which curves we would like to pass to the computing rank phase of the process.

3. **Computing Rank Phase:** Once we have a small list of curves which we *believe* to have high rank, we have to *verify* that they in fact do have high rank.

The latter two steps of this process are the same for each technique and we review them later in this chapter; where they differ is in the constructing phase. Therefore, we will focus on the extension and analysis of this phase of each technique. More specifically, we pay special attention to altering existing techniques to find elliptic curves of large rank with specified torsion.

1.1.4 New Results

Below is a list of some new results achieved by these extensions and analyses, together with where they are discussed:

	Curves		Infinite Families of Curves	
	Rank	Chapter (section)	Rank	Chapter (section)
known torsion	$r_3 \geq 4$	3.5.1	$r_3 \geq 3$	3.4.2
	$r_3 = 4$	2.3.2		
	$r_{2\oplus 6} = 3$	3.5.2	$r_{2\oplus 6} \geq 1$	3.4.3
	$r_{2\oplus 6} \geq 3$	3.5.2		
			$r_{2\oplus 2} \geq 5$	3.4.4
	$r_{2\oplus 4} \geq 3$	3.5.5	$r_{2\oplus 4} \geq 1$	3.4.5
	$r_{2\oplus 4} = 3$	3.5.5		
	$r_4 \geq 3$	3.5.5	$r_4 \geq 1$	3.4.5
	$r_4 = 3$	3.5.5		
	$r_4 \geq 2$	2.3.2		

In addition to the results listed above, we also include some discussion of the more general case of producing an infinite family of elliptic curves defined over $\mathbb{Q}$ without regard to torsion. This discussion leads to the discovery of some curves of rank at least 13 over $\mathbb{Q}(t)$.

1.2 Constructing Elliptic Curves

1.2.1 Weierstrass Form and Reduction

We begin the discussion with the following well known result.

Theorem 1.2.1 *For all elliptic curves, E, defined over the rationals*

1. *E is isomorphic to an elliptic curve of the form*

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

   An elliptic curve expressed in this way is said to be in Weierstrass form.

2. *Two curves in Weierstrass form are isomorphic if and only if there is a change of variables of the form:*

$$x = u^2x' + r$$
$$y = u^3y' + u^2sx' + t,$$

   where u, r, s and t are rational with $u \neq 0$.

3. *There exists a Weierstrass form for which the coefficients are integral and the absolute value of the discriminant is minimal.*

We will denote the minimal Weierstrass form of an elliptic curve E by E_{min} and similarly, the minimal discriminant of E_{min} as $\Delta_{E_{min}}$. Parts 1 and 2 of the theorem are essentially consequences of the Riemann-Roch theorem (see [24, sections II.5,III.3]). In section 4.1.2 we give an algorithm due to Laska for finding the minimal Weierstrass form.

Given an elliptic curve, E, in Weierstrass form, with integer coefficients and given a prime, p, we can reduce each of the coefficients of E modulo p. This new curve, E_p, can be considered to have coefficients in any field of characteristic p and in particular in the field of p elements, $\mathbb{F}_p$. We call the set of points defined over $\mathbb{F}_p$ on this new curve $E_p(\mathbb{F}_p)$. In some cases, E_p is not a smooth curve over $\mathbb{F}_p$. Recall that this occurs if and only if the prime p divides the discriminant of E. If E is in minimal Weierstrass form, we call these primes, *primes of bad reduction.* We call the primes that do not divide the minimal discriminant *primes of good reduction.* We will say that the curve E_p is the curve E *reduced* modulo p and we will call any curve E, defined over the rationals, which reduces to E_p modulo p, a *lift* of E_p.

1.2.2 The Finite Field Method

Let E be an elliptic curve and p be any prime. We denote the number of elements in $E_p(\mathbb{F}_p)$ by $\#E_p$. There is both theoretical and experimental evidence to suggest that elliptic curves, E, of large rank have the property that $\#E_p$ is large for many primes p. We will review this evidence when we discuss sieving later in this chapter. Let us now indicate how Mestre uses this evidence to search for elliptic curves of large rank.

The constructing phase of the algorithm is essentially composed of two steps. First, fix a finite set of primes, and for each prime p in this set, compute an E_p for which $\#E_p$ is maximum. There may be more than one curve E_p which satisfies this condition. Then, construct a list of curves in which each curve is a lift of each of the E_p.

Recall that we can quantify the maximum possible value of $\#E_p$ using Hasse's theorem:

Theorem 1.2.2 *Let p be any prime and E_p an elliptic curve defined over $\mathbb{F}_p$, then*

$$|p + 1 - \#E_p| \leq 2\sqrt{p}.$$

In particular, $\#E_p$ can be at most $\lfloor 2\sqrt{p} \rfloor + p + 1$.

A proof of Hasse's theorem can be found in [24, section V.1].

We make two remarks before continuing. First, the number $p + 1 - \#E_p$ comes up often enough that we define a_p to be $p+1-\#E_p$. Second, while *this* theorem does not guarantee the existence of a curve for which $\#E_p$ is $\lfloor 2\sqrt{p} \rfloor + p + 1$, Serre has proven

([27]) that in fact this is the case. However, if we take the maximum value of $\#E_p$ over curves containing some fixed non-trivial torsion, then this bound given by Weil may not be attained (see section 2.1).

1.2.3 The Polynomial Method

Mestre's polynomial method is distinct from any other method of finding elliptic curves of high rank because it is the only one which constructs elliptic curves with a prescribed number of points. The idea hinges on the following key theorem of Mestre ([14]):

Theorem 1.2.3 *For any field K, let $p(x) \in K[x]$, $p(x)$ monic with $\deg p(x) = 2n$, then there exist polynomials $g(x)$ and $r(x)$ such that*

1. $g(x), r(x) \in K[x]$,
2. $\deg g(x) = n$ *and* $\deg r(x) \leq n-1$, *and*
3. $p(x) = g(x)^2 - r(x)$.

We prove an analagous theorem, also due to Mestre, in section 3.2.1. Observe that for any root, α of the polynomial $p(x)$ in the above, we have that $g(\alpha)^2 = r(\alpha)$. Therefore, the curve $y^2 = r(x)$ contains the $2n$ points $(\alpha_i, g(\alpha_i))$, where the α_i are the roots of $p(x)$. Furthermore, if each of these roots is in the field K, then since $g(x) \in K[x]$, these $2n$ points are K-rational. So, to construct curves with $2n$ K-rational points, we simply need to choose $\alpha_i \in K, 1 \leq i \leq 2n$, and let $p(x)$ equal the product of $(x - \alpha_i)$.

We will write $\mathcal{A} = \{\alpha_1, \alpha_2, ..., \alpha_{2n}\}$ for some choice of roots and $r_{\mathcal{A}}(x)$ for the corresponding polynomial given by the theorem. Now, in order to use Theorem 1.2.3 and the previous observation, we need to investigate the relationship between a choice of $\mathcal{A}$ and:

1. the smoothness of $y^2 = r_{\mathcal{A}}(x)$,
2. the degree of $r_{\mathcal{A}}(x)$,
3. the isomorphism class of $y^2 = r_{\mathcal{A}}(x)$, and

4. the linear independence of the resulting points.

Mestre has proven that for an appropriate choice of $\mathcal{A}$, the resulting curve $y^2 = r_{\mathcal{A}}(x)$ is in fact an elliptic curve [14]. Furthermore, he has produced choices of $\mathcal{A}$ for which the resulting curve is an elliptic curve **and** the resulting points are linearly independent. While this shows that it is possible to prove some statements about the above relationships, we will often rely on experimental results to guide us to high rank elliptic curves.

The real strength of this method is that it can be used to not only construct elliptic curves over $\mathbb{Q}$, but that it is equally useful in constructing elliptic curves over different fields, and in particular over $\mathbb{Q}(t)$. This allows us to construct not only single elliptic curves with many points, but also *infinite families* of such elliptic curves. The idea is to construct an elliptic curve over $\mathbb{Q}(t)$ with high rank and then specialize to rational values of t to get elliptic curves defined over the rationals. Furthermore, by sieving through these curves using the same criteria as in Mestre's finite field method, we can try to pick out curves which have even larger rank over $\mathbb{Q}$ than they did over $\mathbb{Q}(t)$.

1.3 Sieving

Whenever we have a function on elliptic curves for which we understand (or reasonably believe) some relationship between the values of the function and the rank of the elliptic curve we can use it as a predictor of curves with high rank. For example if we can compute an upper bound on the rank of an elliptic curve, we can in the very least weed out curves of low rank. If we can refine the upper bound to be as sharp as possible, then it can be an even better predictor. We are not, however, restricted to using upper bounds. Below we describe two upper bounds and two sums which we use to sieve through lists of elliptic curves to isolate those that may have high rank.

1.3.1 Descent and Kretschmer's Bound

Kretschmer's bound comes from the classical process of descent. We begin by reviewing some facts about descent. The descent procedure was probably first used by Fermat to prove that the rank of the elliptic curve $x^4 + y^4 = z^4$ defined over the rationals is zero, but the proof of the Mordell-Weil Theorem gives us the modern form of descent. Recall that this proof consists of two major parts. Roughly, they are:

1. $E(\mathbb{Q})/mE(\mathbb{Q})$ is finitely generated (the weak Mordell-Weil theorem), and

2. there is a real valued *height function* on $E(\mathbb{Q})$ which bounds the number of points of a fixed height and which is "increasing" with respect to the multiplication by m map on $E(\mathbb{Q})$ for $m \geq 2$ (the descent theorem).

Also recall, that while we can prove that $E(\mathbb{Q})/mE(\mathbb{Q})$ is finitely generated, the proof is ineffective in producing the generators of this group and that this is precisely what inhibits our finding generators for the whole group $E(\mathbb{Q})$. The descent procedure is precisely the technique we currently use to come as close as possible to finding the generators of $E(\mathbb{Q})/mE(\mathbb{Q})$. The procedure rests on the fact that there is an exact sequence:

$$0 \longrightarrow E(\mathbb{Q})/mE(\mathbb{Q}) \longrightarrow S^{(m)}(E/\mathbb{Q}) \longrightarrow \text{Ш}\,(E/\mathbb{Q})[m] \longrightarrow 0,$$

where $S^{(m)}(E/\mathbb{Q})$ is the Selmer group and Ш $(E/\mathbb{Q})$ is the Shafarevich-Tate group. The elements of the Selmer group correspond to twists of the elliptic curve E called *homogeneous spaces* which are everywhere locally soluble– have a solution over every completion of the rationals. The non-trivial elements of the Shafarevich-Tate group catalogue those homogeneous spaces that fail the Hasse principle– contain a solution over every completion of the rationals, yet do not contain a rational solution.

The descent procedure reduces the problem of finding the generators of $E(\mathbb{Q})/mE(\mathbb{Q})$ and hence of $E(\mathbb{Q})$ to computing the Selmer group and the Shafarevich-Tate group– finding a single rational point or proving that no such point exists on each of the homogeneous spaces. Given this, Kretschmer has proven the following ([11]):

Theorem 1.3.1 *Let p be a prime and $z^2 = g(x) = b_1\, x^4 + a\, x^2 + b_2$ define a homogeneous space, then we have*

1. *If p does not divide the discriminant of g, then $z^2 = g(x)$ is solvable in $\mathbb{Q}_p$.*

2. *Let* $\mu = \nu_p(a^2 - 4\,b_1\,b_2)$*. If* $\mu \geq 1$ *and* p *does not divide* $6\,b_1\,b_2$*, then* $z^2 = g(x)$ *is solvable in* $\mathbb{Q}_p$ *if and only if*

   (a) b_1 *or* b_2 *is a quadratic residue mod* p*, or*

   (b) μ *is even and*

$$(\tfrac{a}{p}) = \begin{cases} 1 & \textit{if } p \equiv 5, 7 \textit{ mod } 8 \\ -1 & \textit{if } p \equiv 1, 3 \textit{ mod } 8. \end{cases}$$

3. *If* p *divides* $b_1\,b_2$ *and not* $6\,a$*, then* $z^2 = g(x)$ *is solvable in* $\mathbb{Q}_p$ *if and only if*

   (a) p *does not divide* $\gcd(b_1, b_2)$*, or*

   (b) p *does divide* $\gcd(b_1, b_2)$ *and at least one of the following is true:* $\nu_p(b_1)$ *is even,* $\nu_p(b_2)$ *is even, or* $(\frac{a}{p}) = 1$*.*

We will denote an upper bound achieved using this theorem by k_E. Since this theorem requires that the homogeneous space be of the form $z^2 = b_1x^4 + ax^2 + b_2$, we find that we can only use this result for curves which contain a point of order 2. In section 4.3.2, we give a slightly more detailed account of the particular case of descent by 2-isogeny.

1.3.2 Bad Reduction and Mazur's Bound

Mazur gives another bound for the rank of elliptic curves defined over the rationals with nontrivial torsion. This bound is calculated solely from elementary information about the curve and in particular from information regarding primes of bad reduction.

Primes of bad reduction fall into two categories: additive and multiplicative. Let E be an elliptic curve in minimal Weierstrass form and let p be any prime dividing its discriminant. A prime is said to be of *additive reduction* if E_p has a node. Note that the name additive comes from the fact that the set of nonsingular points of $E_p(\overline{\mathbb{F}_p})$ form a group and this group is isomorphic to the additive group of $\overline{\mathbb{F}_p}$. A prime is said to be of *multiplicative reduction* if E_p has a cusp. The name multiplicative comes from the fact that the group of nonsingular points of $E_p(\overline{\mathbb{F}_p})$ is isomorphic to the multiplicative group of $\overline{\mathbb{F}_p}^*$.

Let $P = (x, y)$ be a point on the elliptic curve E in Weierstrass form. Mazur has proven that if P has prime order p and either $p \geq 3$, $p = 2$ with $x, y \in \mathbb{Z}$, or $p = 2$ with $\nu_2(x) = 2$ and $\nu_2(y) = 3$, we have $r_E \leq m_{E,p} = b + a - m - e - 1$, where a, b and m are defined as follows:

1. b is the number of primes of bad reduction (of all type).

2. a is the number of primes of additive reduction.

3. m is the number of primes of multiplicative reduction, s, satisfying:

   (a) p does not divide the exponent of s in $\Delta_{E_{min}}$ and

   (b) $s \not\equiv 1 \bmod p$.

4. $e = 0$ if $p \geq 3$ and $e = 1$ if $p = 2$ and there is a prime of multiplicative reduction not congruent to 1 modulo 4 satisfying condition 3(a).

Finally, we point out that we may also use $M_E = \min\{m_{E,p} \mid E \text{ has a point of order } p\}$ or $B_E = \min\{M_E, k_E\}$ as alternative bounds in this sieving method.

1.3.3 Mestre's and Nagao's Sums

While the sums we describe here are used in a way very similar to the upper bounds above, there are two significant differences. First, these sums can be computed for curves that have nontrivial torsion. Second, we believe by some theoretical arguments in addition to any experimental evidence that they are sharper estimates of rank.

Consider the sum:

$$S_E(N) = -\sum_{\substack{p \leq N \\ p \text{ prime}}} \frac{a_p - 2}{\#E_p} \log p.$$

This sum was first used by Mestre in the finite field method described in section 1.2.1. In fact, the theoretical evidence mentioned here is the same evidence supporting the idea that elliptic curves with large rank should have lots of points on their reduced models modulo p, for many primes p.

Now consider:

$$s_E(N) = -\frac{1}{N} \sum_{\substack{p \leq N \\ p \text{ prime}}} a_p \ \log p.$$

This sum was first used by Fermigier and generalized by Nagao to curves defined over $\mathbb{Q}(t)$.

The Birch, Swinnerton-Dyer conjecture does not formally imply that these sums give a good measure of the rank of an elliptic curve but rather, gives strong support to this idea. Recall that the L-series related to the elliptic curve E is the function

$$L_E(s) = \prod_{p|\Delta} (1 - a_p p^{-s})^{-1} \prod_{p \nmid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

Recall also that this function converges on the half plane $\mathrm{Re}(s) > 3/2$. A weak version of the Birch and Swinnerton-Dyer conjecture:

Conjecture 1.3.2 *For any elliptic curve E defined over the rationals, the L-series extends to an entire function and the order of vanishing of $L(s)$ at $s = 1$ is equal to r_E.*

We can now present a heuristic for why the Birch, Swinnerton-Dyer conjecture implies the sums $S_E(N)$ and $s_E(N)$ should be good indicators of rank for sufficiently large N. The conjecture first implies that we may write $L(s) = (s-1)^r_E \cdot g(s)$ with $g(1) \neq 0$. (In fact the full Birch, Swinnerton-Dyer Conjecture gives a precise value for $g(1)$ in terms of other data related to the elliptic curve. See [24, section C.16] for more details.) We then have that the logarithmic derivitave of $L(s)$ is

$$\frac{L'(s)}{L(s)} = r_E \frac{1}{(s-1)} + \frac{g'(s)}{g(s)}.$$

If we let $h(s) = g'(s)/g(s)$, we see that $h(s)$ is analytic near $s = 1$, so that

$$\lim_{s \to 1} \frac{L'(s)}{L(s)} = r_E \lim_{s \to 1} \frac{1}{(s-1)} + h(1).$$

It seems reasonable to believe that this limit goes to infinity faster for curves with larger rank.

Now consider the product, $L_E(s, N)$ defined as

$$L_E(s, N) = \prod_{p \leq N} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

This is simply the original L-series with two modifications– we cut off the product at N and ignore the difference between what happens for primes of good reduction and primes of bad reduction. We then have,

$$f(s,N) = \log L_E(s,N) = -\sum_{p\leq N} \log(1 - a_p p^{-s} + p^{1-2s}).$$

Therefore,

$$f'(s,N) = -\sum_{p\leq N} \frac{a_p p^{-s} - 2p^{1-2s}}{1 - a_p p^{-s} + p^{1-2s}} \ \log p.$$

We see that it is reasonable to think

$$\frac{L'(s)}{L(s)} \approx \lim_{N\to\infty} f'(s,N),$$

and hence that

$$\lim_{s\to 1} \frac{L'(s)}{L(s)} \approx \lim_{s\to 1} \lim_{N\to\infty} f'(s,N).$$

Now, if we could reverse the order of the limits, we would have that

$$\lim_{s\to 1} \frac{L'(s)}{L(s)} \approx \lim_{N\to\infty} f'(1,N).$$

Observe that $f'(1,N) = S_E(N)$. We might then expect that curves with larger rank have the property that the sum $S_E(N)$ converges to infinity faster than those with smaller rank. This is consistent with what occurs in practice. We discuss this particular sum further in section 2.1.2.

Note that we can rewrite $S_E(N)$ as

$$S_E(N) = \sum_{\substack{p\leq N \\ p \text{ prime}}} (1 - \frac{p-1}{\#E_p}) \log p\,.$$

This implies that this sum is larger when $\#E_p$ is large for many primes p. This in turn leads us to believe that $\#E_p$ is large for curves with large rank.

Consider the following result of Nagao:

Theorem 1.3.3 (NA3) *Let $\{c_p \mid p \text{ prime}\}$ be a bounded sequence of non-negative numbers. If one of the two series*

$$\frac{1}{N} \sum_{p\leq N} c_p \ \log p$$

or

$$\frac{1}{\pi(N)} \sum_{p\leq N} c_p$$

converges as $N \to \infty$, where $\pi(N)$ = the number of primes less than or equal to N, then so too does the other and they converge to the same limit.

We present a proof of this theorem (different from the one given by Nagao) in section 2.2.1. Given this result, we may consider (under the appropriate conditions) the sum $s_E(N)$ as an average of the values $-a_p$:

$$s_E(N) = \frac{1}{\pi(N)} \sum_{\substack{p \leq N \\ p \text{ prime}}} (\#E_p - p - 1).$$

It is now clear that this sum should also be large when the rank is large. Furthermore, Nagao has also shown that we can extend the idea of this average to curves $\mathcal{E}$ defined over $\mathbb{Q}(t)$ and in some cases actually prove that this "extended" average converges to the rank of the elliptic curve $\mathcal{E}$ ([22]).

1.4 Computing Rank

The section above explains how we go about isolating curves that have a good chance of having large rank, but after isolating these curves, we are still left with the task of actually verifying that what we suspect is true is in fact true. We compute the rank of an elliptic curve by finding points on the curve which are linearly independent in the Mordell-Weil group.

If the curve has a point of finite order we can in theory use descent to find linearly independent points on an elliptic curve. It is, however, often difficult if we are doing anything other than a 2-descent for elliptic curves defined over the rationals. Also, we again can only use this technique on curves that have a rational point of finite order.

It is, therefore, necessary that we also be able to find points on the curve by simply searching (plugging in an x value and testing to see if any of the corresponding y values lie in the same field) and then find the largest subset of linearly independent points from them. Recall that we can compute this linearly independent subset by computing the determinant of the matrix of heights. A more detailed discussion of this process appears in section 4.2.1.

Chapter 2

The Finite Field Method

2.1 Finding a Single Elliptic Curve

2.1.1 The Original Method in Detail

Mestre begins with a particular model for an elliptic curve:

$$E : y^2 + y = x^3 + a_4\,x + a_6.$$

This model is particularly nice since distinct pairs a_4, a_6 determine distinct isomorphism classes. In other words, if $a_4 \neq a_4'$ or $a_6 \neq a_6'$, then the elliptic curve $y^2+y = x^3+a_4\,x+a_6$ is not isomorphic to the elliptic curve $y^2+y = x^3+a_4'\,x+a_6'$. This fact is an immediate consequence of theorem 1.2.1.

Next, we choose a finite set of primes P. In Mestre's original implementation of this technique, he chooses the set of all primes less than or equal to some fixed prime p_0, but one can use any finite set of primes.

For each prime in the set P, we compute the pairs of values (a_4, a_6) which give a maximum value of $\#E_p$. As mentioned earlier, Serre has shown that there exists some pair of values for which $\#E_p$ equals $\lfloor 2\sqrt{p} \rfloor + p + 1$ ([27]). Also as mentioned, there can be more than one pair which attains this maximum value and for primes larger than 7, this appears to always occur. Denote this set of pairs by C_p.

We let $M_P = \prod\limits_{p\,\epsilon\,P} p$ and use the chinese remainder theorem to calculate the set of pairs

$$C_{M_P} = \{(a_4, a_6) \mid 0 \leq a_4, a_6 < M_P\,;\ \text{for each } p\ \epsilon\ P,\ (a_4 \bmod p\,,\ a_6 \bmod p)\ \epsilon\ C_p\}.$$

Finally, we construct a list of curves

$$C = \{y^2 + y = x^3 + a_4\,x + a_6 \mid (a_4 \bmod M_P\,,\ a_6 \bmod M_P)\ \epsilon\ C_{M_P}\},$$

with a_4 negative and a_6 chosen to make the discriminant of the curve small (in absolute value). The former condition exists purely for experimental reasons– curves with this property have tended to have higher rank. The latter condition is for aesthetic reasons– whenever we find a curve with a given property, it is nice to find the curve with the smallest conductor that has that property.

Once the list C has been constructed, we may use any of the applicable sieving methods discussed earlier. Mestre originally used the sum $S_E(N) - S_E(p_0)$ and found several curves of rank at least 6, 7, 8 and 9 one curve of rank at least 12. Note that for each curve in the list C, the value of $S_E(p_0)$ will be the same. This is clearly true by construction. Hence we may use the sum $S_E(N)$ instead of $S_E(N) - S_E(p_0)$ as Mestre does.

2.1.2 Varying the Parameters

After varying the parameters in this method– changing the set of primes P, increasing the lower bound for $S_E(N)$ and $s_E(N)$, computing these sums for greater values of N and increasing the size of C by increasing the number of curves per equivalence class of C_{M_P}– we made two observations.

First, since these changes did not seem to improve or worsen the probability of finding a high rank elliptic curve, the finite field method does not appear to be well suited for finding curves with "very" high rank. (For example, rank as high as those found using the polynomial method which we describe in the next chapter.) Observe that if the number of curves over $\mathbb{F}_p$ which attain the maximum $\lfloor 2\sqrt{p} \rfloor + p + 1$ is at least 2 for all $p \geq 7$, then the size of C_{M_P} grows exponentially with each new prime, p, added to P. Experimentally, we find that this number of curves is an increasing function of p. Furthermore, M_P grows exponentially as well (recall that this is equivalent to the prime number theorem); so, not only do the number of curves in C grow rapidly, but the coefficients of each curve grow rapidly as well. Therefore, if it is the case that the number of primes necessary to find curves of large rank using this method increases with rank (which is experimentally true), then it would be unreasonable to expect that this method alone would be able to produce elliptic curves of "very" high rank.

The second observation we made was regarding the growth of the sum $S_E(N)$. $S_E(N)$ appears to be $O(\log(N))$. More importantly, if we let

$$G_E(N) = \frac{1}{\log N - 2} S_E(N),$$

then it seems to be the case that $(r_E - \lim_{N\to\infty} G_E(N)) < \frac{3}{2}$. For the first 10,000 curves in Cremona's list, we found that for sufficiently large N ($N \approx 15^5$), $G_E(N)$ was between r_E and $r_E - 1.3$. In each of the curves found using this finite field method, we found that the difference between $G_E(p_{500})$, where p_{500} is the 500th prime, and the number of linearly independent points found on the curve was less than 1. Similar results hold for curves found by Fermigier and Nagao (see [4, page 361]).

2.2 More on Sums

2.2.1 Sums over Primes

The goal of this section will be to prove theorem 1.3.3. First, we recall and sketch a proof of Abel's Identity.

Theorem 2.2.1 (Abel's Identity) *For any sequence $g(n)$, $n \in \mathbb{N}$, let*

$$G(x) = \sum_{0<n\leq x} g(n),$$

and let F be in $C^1([a,b])$ with $0 < a < b$. Then we have

$$\sum_{a<n\leq b} g(n)F(n) = G(b)F(b) - G(a)F(a) - \int_a^b G(x)F'(x)\, dx.$$

Sketch of Proof:

$$\sum_{a<n\leq b} g(n)F(n) = \int_a^b F(x)\, dG(x),$$

where the right hand side of the equation is a Riemann-Stieljes integral. Now integrate by parts to get the theorem.

We now restate and present a proof, different from the one given by Nagao in [22], of theorem 1.3.3.

Theorem 2.2.2 *Let $\{c_p \mid p \text{ prime}\}$ be a bounded sequence of non-negative numbers. If one of the two series*

$$\frac{1}{N}\sum_{p\le N} c_p \ \log p$$

or

$$\frac{1}{\pi(N)}\sum_{p\le N} c_p$$

converges as $N \to \infty$, where $\pi(N)$ = the number of primes less than or equal to N, then so too does the other and they converge to the same limit.

Proof: Let

$$g(n) = \begin{cases} c_p & \text{if } n \text{ equals the prime } p \\ 0 & \text{otherwise,} \end{cases}$$

and let

$$G(x) = \sum_{1<n\le x} g(n).$$

Then, by Abel's identity, we have

$$\sum_{1<p\le N} c_p \ \log p = \log N \cdot G(N) - \int_1^N \frac{G(x)}{x} dx.$$

If we divide this equation through by N and observe that $G(x) = 0$ for $x < 2$, we get

$$\frac{1}{N}\sum_{1<p\le N} c_p \ \log p = \frac{\log N}{N} G(N) - \frac{1}{N}\int_2^N \frac{G(x)}{x} dx.$$

Since the c_p are positive and bounded, for some positive constant M, we have the inequality $0 \le G(x) \le M \cdot \pi(x)$ where $\pi(x)$ is the number of primes between 1 and x. The prime number theorem gives us the following two equalities:

$$\lim_{N\to\infty} -\frac{M}{N}\int_2^N \frac{\pi(x)}{x} dx = 0$$

and

$$\lim_{N\to\infty} \frac{\log N}{N} G(N) = \lim_{N\to\infty} \frac{1}{\pi(N)} G(N),$$

which proves the theorem.

2.2.2 Applications to $s_E(N)$ and $G_E(N)$

As mentioned in the introduction, this theorem gives a basis upon which to think of the sum $s_E(N)$ as an average of the values $-a_p$. Unfortunately, the sequence $\{-a_p\}$ is not in general a bounded, nonnegative sequence and so the theorem does not apply. However, for elliptic curves for which we can prove that the sequence above satisfies the conditions of the theorem, we can replace the sum $s_E(N)$ with the sum

$$s'_E(N) = -\frac{1}{\pi(N)} \sum_{\substack{p \le N \\ p \text{ prime}}} a_p \, .$$

If $0 \le -a_p \le M$ for some constant M then we have,

$$s'_E(N) \le \frac{1}{\pi(N)} \sum_{\substack{p \le N \\ p \text{ prime}}} M = M.$$

This means that $s'_E(N)$ is a bounded increasing sequence and hence converges. By theorem 1.3.3 then, we have that $s_E(N)$ converges and converges to the same value. In sections 3.2.5 and 3.4.6, we give some results of Nagao in which these results become relevant.

Similarly, we cannot in general apply theorem 1.3.3 to the sum $G_E(N)$, since we do not always have that $\{-\frac{a_p-2}{\#E_p}\}$ is a bounded, nonnegative sequence. We have in this case as well, a sum,

$$G'_E(N) = -\sum_{\substack{p \le N \\ p \text{ prime}}} \frac{a_p - 2}{\#E_p},$$

which can replace $G_E(N)$ when the sequence $\{-\frac{a_p-2}{\#E_p}\}$ satisifies the conditions of theorem 1.3.3. Differing from the situation above, this alone does not give us that the sum converges.

2.3 Finding Curves with Nontrivial Torsion

2.3.1 Modifying the Method

Just as we can vary the set of primes and the sum used to sieve, we can also vary the model of the elliptic curve we use in the finite field method. If we use one of

Tate's normal forms for curves containing a point of finite order in place of $y^2 + y = x^3 + a_4\,x + a_6$, we can use the finite field method to find curves with nontrivial torsion of high rank. Furthermore, we can now use the upper bounds discussed earlier during the sieving phase of the technique. In some cases, computing the upper bound allows us to give the exact rank of curves rather than just a lower bound on the rank.

Let $E_0 = E(A, B)$ be the elliptic curve $y^2 + y = x^3 + A\,x + B$ defined over $\mathbb{Q}(A, B)$ and for any a and b rational, let $E(a, b)$ be the specialization of the curve to $y^2 + y = x^3 + a\,x + b$ defined over $\mathbb{Q}$. Let $S_p(0)$ be the set of reduced curves

$$\{E(a, b)_p \mid 0 \leq a, b \leq p, E(a, b) \text{ an elliptic curve defined over } \mathbb{Q}\}.$$

Furthermore, let $W_p(0)$ be the maximum value $\#E(a, b)_p$ over all curves in $S_p(0)$. If we let $w_p = \lfloor 2\sqrt{p} \rfloor + p + 1$, we have $(w_p - W_p(E_0)) = 0$ for all primes, p. Serre has generalized this statement for curves of higher genus and for curves defined over other finite fields ([27]). We have found that this seems to also generalize in a different way. First, we define $E_{\mathbb{T}}$ to be the Tate normal form of the elliptic curve with torsion $\mathbb{T}$, with E_0 being the curve for $E_{\{0\}}$. This curve is defined over some function field over $\mathbb{Q}$. Let $S_p(\mathbb{T})$ be the set of reduced curves

$$\{E_p \mid E \text{ is a specialization of } E_{\mathbb{T}}\}.$$

If we set $W_p(\mathbb{T})$ to be the maximum value $\#E_p$ over all curves E in $S_p(\mathbb{T})$, then we conjecture the following.

Conjecture 2.3.1 *Let $\mathbb{T}$ be one of the possible subgroups for an elliptic curve defined over $\mathbb{Q}$. For any prime, p,*

$$(w_p \;-\; W_p(\mathbb{T})) < |\mathbb{T}|,$$

except when $\mathbb{T} = \mathbb{Z}/2\mathbb{Z}$ and $p = 2$. Furthermore, for each integer $k \;\epsilon\; \{0, 1, ..., |\mathbb{T}| - 1\}$, there exists a prime p_0 with $(w_p \;-\; W_p(\mathbb{T})) = k$.

(It is also possible that each value of k is obtained infinitely often, though our calculations were not performed for enough primes to include this as part of the conjecture.) We present the following calculations as evidence of this conjecture:

	Value of $(w_p - W_p(\mathbb{T}))$												
$\mathbb{T}$	0	1	2	3	4	5	6	7	8	9	10	11	total # of primes
$\mathbb{Z}/2\mathbb{Z}$	16	13	1										30
$\mathbb{Z}/3\mathbb{Z}$	11	13	6										30
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	10	9	6	4									30
$\mathbb{Z}/4\mathbb{Z}$	52	54	49	45									200
$\mathbb{Z}/6\mathbb{Z}$	33	36	36	38	31	26							200
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$	37	38	32	24	19	21	13	16					200
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	16	17	16	20	18	20	16	18	21	16	14	8	200

Each row in the table above shows the distribution of the difference $(w_p - W_p(\mathbb{T}))$ for a given torsion group. For the curves whose Tate normal form is parameterized by two variables, the distribution is over the first 30 primes and for the curves parameterized by one variable, the distribution is over the first 200 primes.

It is not yet clear, why this phenominon occurs, but it does loosely imply that it is more difficult to produce large rank elliptic curves using this method as the size of the desired torsion subgroup grows. This holds true in practice as is illustrated by the few curves of large rank produced in the following section and in section 3.5.

2.3.2 Curves with Nontrivial Torsion

We present two curves with nontrivial torsion and moderate rank. Each of these curves were found by performing the finite field method using the Tate normal form in place of the form used by Mestre originally. In the case of the curve with a point of order three, we searched for curves with corresponding sum $G_E(p_{500})$ at least 3 and with the bound given by Mazur at least 3. We found several curves of rank 3 and one curve of rank exactly 4. This curve is known to have rank precisely 4 because we were able to find four linearly independent points and because Mazur's bound for this curve is 4. This curve is listed below, together with independent points on the minimal Weierstass model. We also indicate the point of order 3.

Tate Form	Minimal Form	x : Order	rank	Generators (x)
[-109,0,421,0,0]	[1,0,1, -2963740, 1963602390]	$[990, -285] : 3$	4	[-1957,17397], [-1115,62865], [-1082,63022], [509,23973]

Similarly, we were able to find a curve of rank 2 with a point of order 4. We found this curve by again searching for curves with a high corresponding sum $G_E(p_{500})$. However, in this case, we searched for curves with the additional constraint that the bound given by Kretschmer was at least 3. Once a curve was found that satisfied these conditions a descent was performed to find points on the curve. Section 4.2.3 describes this descent in more detail. While we found many curves of rank at least one, the elliptic curve below was the only curve found to have rank strictly larger than 1.

Tate Form	Minimal Form	x : Order	rank	Generators (x)
[1,-26273, -26273,0,0]	[1,1,1, -230098934, -1343368714654]	$[-8758, 17515] : 4$	2 or 3	[41552, 7779230], [84035/4, 13991581/8]

Note that we can compute the sign of the functional equation and assuming the Birch, Swinnerton-Dyer conjecture, compute the rank more precisely. This is discussed in more detail in section 4.2.4.

Chapter 3

The Polynomial Method

3.1 The Quartic Model

3.1.1 Alternate Models of Elliptic Curves

Given theorem 1.3.2, we could have defined an elliptic curve defined over K to be the set of points in projective two space satisfying

$$Y^2Z + a_1\,XYZ + a_3\,YZ^2 = X^3 + a_2\,X^2Z + a_4\,XZ^2 + a_6\,Z^3$$

provided this curve is smooth. We do not have to add the provision that the curve contain a K-rational point since every curve in Weierstrass form contains the point $[0, 1, 0]$ called the *point at infinity*. It is often useful, however, to recognize other models of elliptic curves. This motivated our more general definition of elliptic curves as smooth curves of genus 1. The projective model above is an example of a degree three, homogeneous polynomial in three variables. It is in fact the case that any smooth, degree three, homogeneous polynomial in three variables containing at least one K-rational point describes an elliptic curve defined over K.

A less commonly used description of an elliptic curve is the set of points in projective three space satisfying both

$$X_0X_3 = X_1^2$$

and

$$X_2^2 = a_4\,X_3^2 + a_3\,X_3X_1 + a_2\,X_0X_3 + a_1\,X_1X_0 + a_0\,X_0^2,$$

where $a_4 \neq 0$. Dehomogenizing at the variable X_0, we see that one affine model for this curve is

$$y^2 = a_4\,x^4 + a_3\,x^3 + a_2\,x^2 + a_1\,x + a_0.$$

For this reason, we will refer to this model of an elliptic curve as *the quartic model* and the points with $X_0 \neq 0$ *the affine points*. If $X_0 = 0$, then it must be that $X_1 = 0$ and we see that the points $[0, 0, \sqrt{a_4}, 1]$ and $[0, 0, -\sqrt{a_4}, 1]$ are points on the curve. We call these points the *points at infinity* for this model of the curve. By dehomogenizing at either X_0 or X_3, we observe that this curve is smooth at each of its points, including the points at infinity, if and only if the function $f(x) = a_4\,x^4 + a_3\,x^3 + a_2\,x^2 + a_1\,x + a_0$ has no double roots. If $f(x)$ has no double roots, then the curve is smooth and has genus 1. Therefore, if the coefficients of $f(x)$ lie in a field K and the curve contains a k-rational point, then this model describes an elliptic curve defined over K. Furthermore, if a_4 is a square in K, then the two points at infinity are K-rational.

These two more general models above give us greater flexibility when trying to construct elliptic curves of high rank, but it is still necessary to be able to work with the Weierstrass form of an elliptic curve we construct. As mentioned in the remarks following theorem 1.2.1, the Riemann-Roch theorem can be used to prove that every elliptic curve can be put into Weierstrass form. In section 4.1.1, we present a discussion of why this is necessary and give the transformation which maps the quartic model to a curve in Weierstrass form.

3.1.2 Divisors

If an elliptic curve, E, is in Weierstrass form, we can take any rational point to be the identity and the rational points on the curve, $E(\mathbb{Q})$, form a group with the usual chord and tangent method. Unless otherwise stated, we take the unique point at infinity on a curve in Weierstrass form to be the identity. A similar *geometric* group law can be defined for curves presented in the quartic model.

The construction of this group law follows the same construct as for the group law for curves in Weierstrass form. For this reason, we first recall some facts about divisors. A *divisor* for the elliptic curve E defined over a field K, is a formal finite integer sum of points on E. Equivalently, it is an element in the free ableian group generated by the points on E. Every divisor is of the form:

$$D = \sum_{P \,\epsilon\, S} n_P\,(P),$$

where the n_P are integers and S is some finite set of points in $E(\overline{K})$. We use the notation (P) when using divisors to make the distinction between a divisor and a sum in the group $E(\overline{K})$. The *degree* of a divisor of the form above is defined to be

$$\deg(D) = \sum_{P \,\epsilon\, S} n_P.$$

The set of all divisors for an elliptic curve E, called the *divisor group of* E and denoted $\mathrm{Div}(E)$, is a group. The set of divisors of degree 0, denoted $\mathrm{Div}^0(E)$, is a subgroup.

A divisor D is defined over the field K if for every element, σ, in the galois group of $\overline{K}$ over K, we have

$$D = D^\sigma = \sum_{P \,\epsilon\, S} n_P\,(P^\sigma).$$

The group of divisors defined over K is denoted $\mathrm{Div}_K(E)$. Similarly, the group of divisors defined over K of degree 0 is denoted $\mathrm{Div}_K^0(E)$.

A divisor is called *principal* if it is of the form:

$$D = \sum_{P \,\epsilon\, E} \mathrm{ord}_P(f)\,(P),$$

for some function $f \,\epsilon\, \overline{K}(E)^*$, where $\mathrm{ord}_P(f)$ is the order of vanishing or pole of the function f at the point P. In this case, we write $D = \mathrm{div}(f)$ and call D the divisor of f. Every principal divisor has degree 0 and so it makes sense to consider the quotient of the group $\mathrm{Div}^0(E)$ by the subgroup of prinicipal divisors. This quotient group is called the degree 0 part of the divisor class group and is denoted $\mathrm{Pic}^0(E)$. Similarly, we denote the quotient group of $\mathrm{Div}_K^0(E)$ by its subgroup of principal divisors by $\mathrm{Pic}_K^0(E)$. Note that the principal divisors that are defined over K are the divisors of functions $f \,\epsilon\, K(E)^*$.

Consider the following theorem. (We note that the proof, together with a more in depth discussion of divisors may be found in sections II.3 and III.3 of [24].)

Theorem 3.1.1 *Let E be an elliptic curve defined over K with identity O and let $D = \sum n_P\,(P)$ be a divisor defined over K (with the sum being over some finite set of points $S \subset E(K)$). Then we have that*

1. *$Pic^0_K(E) \cong E(K)$ and*

2. *D is principal if and only if D has degree 0 and*

$$\sum_{P \,\epsilon\, S} n_P\, P \;=\; O$$

as a sum in $E(K)$.

3.1.3 The Group Law

We now present the group law on the quartic model of an elliptic curve, E, defined over K. We assume, that the curve is of the form:

$$X_0 X_3 = X_1^2$$
and
$$X_2^2 = a^2\, X_3^2 + b\, X_3 X_1 + c\, X_0 X_3 + d\, X_1 X_0 + e\, X_0^2,$$

with $a, b, c, d, e \;\epsilon\; K$. This gives that the two points at infinity $O = [0, 0, -a, 1]$ and $O' = [0, 0, a, 1]$ are in fact K-rational. Furthermore, we choose O to be the identity of the group. We let

$$L_{[\alpha,\beta,\gamma,\delta]}(X_0, X_1, X_2, X_3) = \alpha\, X_0 \;+\; \beta\, X_1 \;+\; \gamma\, X_2 \;+\; \delta\, X_3,$$

and

$$l_{x_0} = X_1 \;-\; x_0\, X_0.$$

Each of these linear curves intersects the elliptic curve E in 4 points (counting multiplicity). In particular, if $R = [1, x_0, y_0, x_0^2]$ is an affine point on the curve, $l_{x_0} = 0$ intersects E at the points O, O', R and $T = [1, x_0, -y_0, x_0^2]$. Furthermore, for some points P and Q (neither of which equal to O), the linear curve $L_{[\alpha,\beta,1,-a]}(X_0, X_1, X_2, X_3) = 0$ intersects the curve at the points P, Q, R and O' when $\beta = (ax_0^2 - \alpha - y_0)/x_0$. If P and Q are K-rational, then the function $f = L/l \;\epsilon\; K(E)^*$ and

$$\mathrm{div}(f) = (P) + (Q) - (T) - (O).$$

By theorem 3.1.1, we have that $T = P + Q$ in the group $E(K)$.

If we dehomogenize at X_0, we can observe the *geometry* of this group law. We see that the curve $L = 0$ defines a parabola and $l = 0$ defines the vertical line $x = x_0$. If we have two K-rational points P and Q (again both not O), we can solve $y^2 = ax^2+\beta x+\alpha$, for β and α such that the parabola contains the points P and Q. If $P = Q$, then we simply require that the parabola be tangent at the point P. This parabola then intersects the elliptic curve E in one other K-rational point, R. If the point is affine, then the sum of P and Q is the reflection of this point across the x-axis, T.

If in the above, the point R is not affine, then we have the two following possibilities. If $R = O$ then the zeroes of L are P, Q, O and O' each with multiplicity one. Since the function X_0 has a double zero at O and at O', we have that $\mathrm{div}(L/X_0) = (P) + (Q) - (O) - (O')$. Therefore, in this case, $P + Q = O'$. Furthermore, the condition that O and O' be on $L = 0$ implies that Q must be the reflection of P across the x-axis. If $R = O'$, then the zeroes of L are P and Q each with multiplicity one and O' with multiplicity two. Therefore, we have that $\mathrm{div}(L/X_0) = (P) + (Q) - 2(O)$ and so $P = -Q$.

3.2 Constructing Curves over $\mathbb{Q}(t)$

3.2.1 Two Polynomial Constructions

There are two constructions due to Mestre which produce elliptic curves with a prescribed number of points on the curve. Each of these constructions follow the same general principal. The first construction is a consequence of theorem 1.2.2, restated below:

Theorem 3.2.1 *For any field K, let $p(x) \in K[x]$, $p(x)$ monic with $\deg p(x) = 2n$, then there exist polynomials $g(x)$ and $r(x)$ such that*

1. $g(x), r(x) \in K[x]$,
2. $\deg g(x) = n$ *and* $\deg r(x) \leq n-1$, *and*
3. $p(x) = g(x)^2 - r(x)$.

The second construction is a consequence of the similar theorem:

Theorem 3.2.2 *For any field K, let $p(x) \in K[x]$, $p(x)$ monic with $\deg p(x) = 3n$, then there exist polynomials $g(x), r_1(x)$ and $r_2(x)$ such that*

1. $g(x), r_1(x), r_2(x) \ \epsilon \ K[x]$,

2. $\deg g(x) = n, \deg r_1(x) \leq \ n-1$ *and* $\deg r_2(x) \leq n-1$, *and*

3. $p(x) = g(x)^3 + g(x)\, r_1(x) + r_2(x)$.

Proof: If

$$p(x) = x^{3n} + ... + a_1\, x + a_0,$$

then

$$p(\frac{1}{x}) = \frac{1 + a_{3n-1}\, x + ... + a_1\, x^{3n-1} + a_0\, x^{3n}}{x^{3n}}.$$

Let $p_1(x)$ be the numerator of $p(\frac{1}{x})$ and let $h(x)$ be the Taylor expansion of $p_1(x)^{\frac{1}{3}}$ about $x = 0$. Let $g(\frac{1}{x})$ equal the terms of $\frac{h(x)}{x^n}$ with non-positive exponent. Then,

$$g(\frac{1}{x}) = \frac{1 + b_{n-1}\, x + ... + b_1\, x^{n-1} + a_0\, x^n}{x^n}.$$

Let $g_1(x)$ be the numerator of $g(\frac{1}{x})$. Since, $h(x)^3 = p_1(x)$, $g_1(x)^3$ agrees with $p_1(x)$ to at least the degree n term. This implies that $p(x) - g(x)^3$ is at most a degree $2n - 1$ polynomial. If we then divide $p(x) - g(x)^3$ by $g(x)$, let $r_1(x)$ be the quotient polynomial and let $r_2(x)$ be the remainder polynomial, then we get the theorem.

Now observe that for any root α of $p(x)$, we have

$$g(\alpha)^2 = r(\alpha)$$

in the first theorem and

$$g(\alpha)^3 + r_1(\alpha)\, g(\alpha) + r_2(\alpha) = 0$$

in the second. So if we replace $g(x)$ in each of the equations with y, then in the first case we have, that the curve defined by

$$y^2 = r(x),$$

contains the point $(\alpha, g(\alpha))$ for any root α of $p(x)$. Similarly, in the second case, we have that the curve defined by

$$y^3 + r_1(x)\, y + r_2(x) = 0$$

contains the equivalently defined points. Furthermore, since $g(x) \epsilon K[x]$, if a root, α, of $p(x)$ is in K, then the resulting point, $(\alpha, g(\alpha))$, on the curve is K-rational.

Mestre's idea is to choose $2n$ or $3n$ roots of $p(x)$ for some n and then use one of these theorems to construct the curve

$$y^2 = r(x) \quad \text{or} \quad y^3 + r_1(x)\,y + r_2(x) = 0.$$

If the roots are chosen properly, then the curves defined by the equations above will be elliptic curves.

In particular, if we let $n = 6$ and choose the 12 roots of $p(x)$ in the first theorem, then the degree of $r(x)$ is no greater than 5. Mestre showed that there were possible choices of 12 roots for which $r(x)$ in this construction is of degree 4. If in this case, $r(x)$ has no double roots, then we have that $y^2 = r(x)$ describes an elliptic curve. Similarly, if we let $n = 4$ and again choose the 12 roots of $p(x)$, then in the second theorem, the degrees of $r_1(x)$ and of $r_2(x)$ are each less than or equal to 3. Mestre also showed that there were possible choices of 12 roots for which $r_1(x)$ in this construction is of degree 2. If the resulting curve $y^3 + r_1(x)\,y + r_2(x) = 0$ is smooth, then this too describes an elliptic curve.

3.2.2 Setting up the Construction

We now present one particular way to use theorem 3.1.1 to construct elliptic curves over the field $\mathbb{Q}(t)$. In section 4.3.1 we indicate why we choose this construction over one using theorem 3.1.2. We let $\mathcal{A}$ be the set $\{a_1 + t, a_1 - t, ..., a_6 + t, a_6 - t\}$, where $a_i \epsilon \mathbb{Q}$ for each i. If we let

$$p_{\mathcal{A}}(x) = \prod_{\alpha_i \,\epsilon\, \mathcal{A}} (x - \alpha_i),$$

then by theorem 3.1.1 there exist polynomials $g_{\mathcal{A}}(x)$ and

$$r_{\mathcal{A}}(x) = r_{5,\mathcal{A}}(t)\,x^5 + r_{4,\mathcal{A}}(t)\,x^4 + ... + r_{0,\mathcal{A}}(t)$$

such that

$$p_{\mathcal{A}}(x) = g_{\mathcal{A}}(x)^2 - r_{\mathcal{A}}(x).$$

We will call the 12 points on the curve $y^2 = r_{\mathcal{A}}(x)$ arising from this procedure, the twelve *constructed points.*

Note that when $t = 0$, we have $p_{\mathcal{A}}(x)$ is a perfect square. Therefore, when $t = 0$, $r_{\mathcal{A}}(x)$ is identically zero. Furthermore, $p_{\mathcal{A}}(x)$ is even in t and so both $g_{\mathcal{A}}(x)$ and $r_{\mathcal{A}}(x)$ are even in t as well. This gives that $r_{\mathcal{A}}(x)$ is a multiple of t^2. Also, for this choice of roots, the set of rationals $\{a_1, a_2, ..., a_6\}$ completely determines $p_{\mathcal{A}}(x), g_{\mathcal{A}}(x)$ and $r_{\mathcal{A}}(x)$. Given these remarks, we define A to be the point $(a_1, a_2, ..., a_6) \ \epsilon \ \mathbb{Q}^6$, and we let

$$\begin{aligned}
&p_A(x) = p_{\mathcal{A}}(x),\\
&g_A(x) = \tfrac{g_{\mathcal{A}}(x)}{t^2},\\
&r_A(x) = \tfrac{r_{\mathcal{A}}(x)}{t^2} \text{ and}\\
&r_{j,A}(t) = \tfrac{r_{j,\mathcal{A}}(t)}{t^2} \text{ for each } j, 0 \le j \le 5.
\end{aligned}$$

Not all choices of A give an elliptic curve. The greatest challenge is choosing the roots so that $r_{5,A}(t)$ is identically zero. The zeroes of $r_{5,A}(t)$, considered now as a polynomial in a_1, a_2, a_3, a_4, a_5 and a_6, form a surface in $\mathbb{Q}^6$. Currently, there is no simple description of the rational points on this surface or a parameterization of some subset known to give elliptic curves of high rank. In the next two sections we describe how to *discover* points on this surface that lead to elliptic curves of high rank.

3.2.3 Differentiating Choices of Roots

Our goal is to produce curves of high rank and so we will first require that the roots we choose be distinct. Therefore, we demand that no two of the a_i in A be equal. Our goal is also to produce many non-isomorphic examples of elliptic curves of large rank. Therefore, we need to be able to determine when two choices of A giving elliptic curves, actually give isomorphic elliptic curves. Working toward that end, we give two definitions.

Definition 3.2.3 *Suppose $A = (a_1, a_2, ..., a_6)$ and $B = (b_1, b_2, ..., b_6)$ are such that $r_{5,A}$ and $r_{5,B}$ are zero. Then we say $A \sim B$ if there exist α and β in $\mathbb{Q}$, $\alpha \neq 0$ and $\sigma \ \epsilon \ S_6$ (the symmetric group on six letters), such that for each i,*

$$a_i = \alpha\, b_{\sigma(i)} + \beta.$$

Definition 3.2.4 *Let $\mathcal{S}$ be defined as the set of $A = [a_1, a_2, ..., a_6] \ \epsilon \ \mathbb{P}^5[\mathbb{Z}]$ such that*

1. $r_{5,A}(t) = 0$,

2. $a_1 = 0$,

3. $\gcd(a_1, a_2, ..., a_6) = 1$ *and*

4. $a_1 < a_2 < \cdots < a_6$.

We now prove two propositions which summarize how to determine when two choices of roots produce the same curve.

Propostion 3.2.5 *If $A = [a_1, a_2, ..., a_6]$ and $B = [b_1, b_2, ..., b_6]$ are elements of $\mathcal{S}$, then $A \sim B$ if and only if $a_i = b_6 - b_{7-i}$ for each $i = 1, 2, ..., 6$.*

Proof: If $a_i = b_6 - b_{7-i}$ for each $i = 1, 2, ..., 6$ then clearly, we have that $A \sim B$.

Now note that $a_1 = b_1 = 0$ and assume $A \sim B$. We then have an α and a β in $\mathbb{Q}$ with $\alpha \neq 0$, and a $\sigma \ \epsilon \ S_6$ such that

$$a_i = \alpha b_{\sigma(i)} + \beta \text{ for each } i.$$

$\sigma(i_0) = 1$ for some i_0 and so $a_{i_0} = \alpha \cdot 0 + \beta = \beta$. Also, $0 = \alpha b_{\sigma(1)} + a_{i_0}$ so

$$\alpha = -\frac{a_{i_0}}{b_{\sigma(1)}}.$$

Therefore,

$$a_i = a_{i_0} \cdot (1 - \frac{b_{\sigma(i)}}{b_{\sigma(1)}}).$$

Now since $a_i > 0$ for $i > 0$, we have that $(1 - \frac{b_{\sigma(i)}}{b_{\sigma(1)}}) > 0$ for $i > 1$. This implies that $b_{\sigma(i)} < b_{\sigma(1)}$ for $i > 1$. Therefore, $b_{\sigma(1)} = b_6$. Similarly, by rewriting the equivalence relation as

$$b_{\sigma(i)} = b_6 \cdot (1 - \frac{a_i}{a_{i_0}}),$$

we have that $a_{i_0} = a_6$. So now we have

$$a_i = a_6 - \frac{a_6}{b_6} b_\sigma.$$

Since the greatest common divisor of the a_i and of the b_i must each be 1, it must be that $a_6 = b_6$, so that $a_i = b_6 - b_{\sigma(i)}$. Finally since $a_1 < a_2 < \ldots < a_6$ and $b_1 < b_2 < \ldots < b_6$, $\sigma(i) = 7 - i$.

Propostion 3.2.6 *If $A \sim B$, and $r_{5,A}(t) = r_{5,B}(t) = 0$, $y^2 = r_A(x)$ and $y^2 = r_B(x)$ are elliptic curves, then they are isomorphic elliptic curves.*

Proof: Clearly, changing the order of the roots has no effect on $p(x)$ and therefore no effect on $g(x)$ or $r(x)$. Now consider the possibility that $A = \lambda B$. Then if we substitute λt for t in the polynomial $p_A(\lambda x)$, we get $\lambda^{12} p_B(x)$ and so we have isomorhic curves. Similarly, if A is a translation of B by a constant d, then the polynomial $p_A(x - d) = p_B(x)$.

These two propositions allow us to restrict our attention to a choice of roots represented by an element of $\mathcal{S}$.

3.2.4 Conditions on $r_A(x)$

If we find an A for which $r_{5,A}(t) = 0$ and $r_A(x)$ has no double roots, then $y^2 = r_A(x)$ defines an elliptic curve. (Note that in practice, the curves are always smooth.) Let us suppose that we have such an A. This elliptic curve will have at least the twelve constructed points derived from the roots given by A. We now discuss some conditions on $r_A(x)$ which allow us to construct and to identify more points on $y^2 = r_A(x)$.

Propostion 3.2.7 $\deg(r_{j,A}(t)) \leq 8 - 2\lceil \frac{j}{2} \rceil$ *for* $0 \leq j \leq 5$.

Proof: Recall that $r_{j,A}(t)$ is even in t and so this condition on the degree is equivalent to $\deg(r_{j,A}) \leq 8 - j$ for $0 \leq j \leq 5$. This in turn is equivalent to the condition

$$\deg(r_{j,\mathcal{A}}) \leq 10 - j \text{ for } 0 \leq j \leq 5.$$

Observe that the coefficient of x^n in $p(x)$ is a polynomial of degree less than or equal to $12 - n$, so we have immediately that $\deg(r_{j,\mathcal{A}}) \leq 12 - j$. Furthermore, $p_A(x)$ is a perfect square at $t = \infty$ and so we have that $r_{\mathcal{A}}(x) = 0$ at $t = \infty$. Therefore, $\deg(r_{j,A}) \leq 10 - j$.

We in fact found experimentally that more is true. Let us denote the coefficient of t^n for any polynomial, f, in t as $c_n(f)$. We conjecture the following:

Conjecture 3.2.8 *For any choice of A, $\deg(r_{j,A}(t)) \leq 6 - 2\lceil \frac{j}{2} \rceil$ for $0 \leq j \leq 5$,*

$$-2c_2(r_{4,A}) = c_4(r_{2,A}) = -2c_6(r_{0,A}),$$

$$\text{and}$$

$$c_2(r_{3,A}) = -c_4(r_{1,A}).$$

This conjecture held true for every A we tested.

If we let $\omega(x)$ be the polynomial $r_A(x)$ evaluated at $t = 0$, then we have the following proposition.

Propostion 3.2.9 *Let $A \,\epsilon\, \mathcal{S}$ and suppose $r_A(x)$ satisfies conjecture 3.2.8. Let $s(t) \,\epsilon\, \mathbb{Q}[t]$ with $d = \deg(s)$, $\alpha = c_d(s)$ and $\beta = c_0(s)$.*

1. *If $d = 0$, then*

$$r_A(s(t)) = r_A(\beta) = c_6(r_{0,A})\, t^6 + \cdots + \omega(\beta).$$

2. *If $d = 1$ and $\alpha = \pm 1$, then*

$$r_A(s(t)) = \mu_4(\beta)\, t^4 + \mu_3(\beta)\, t^3 + \mu_2(\beta)\, t^2 + \mu_1(\beta)\, t^1 + \omega(\beta),$$

   for some functions $\mu_i(x) \,\epsilon\, \mathbb{Q}[x]$. Furthermore, if we define the function f as

$$f = 4 \cdot \mu_4 \cdot \mu_3 \cdot \mu_2 - \mu_3^2 - 8 \cdot \mu_4^2 \cdot \mu_1,$$

   then

   (a) *$\deg(f)$=7 and*

   (b) *$f(a_i) = 0$ for each $a_i \,\epsilon\, A$.*

3. *If $d = 1$ and $\alpha \neq \pm 1$, then*

$$r_A(s(t)) = c_2(r_{4,A})(\alpha^2 - 1)^2\, t^6 + \cdots + \omega(\beta).$$

4. If $d > 1$, then

$$r_A(s(t)) = \alpha^4 c_2(r_{4,A})\, t^{4d+2} + \cdots + \omega(\beta).$$

Proof: To verify that in each case $r_A(s(t))$ is as stated above, simply plug $s(t)$ into a general polynomial satisfying conjecture 3.2.8. This also verifies that the degree of f is 7.

It remains to show that f vanishes on A. Let $\mu(\beta, t) = r_A(t + \beta)$. We then have that

$$\mu(\beta, t) = \mu_4(\beta)\, t^4 + \mu_3(\beta)\, t^3 + \mu_2(\beta)\, t^2 + \mu_1(\beta)\, t^1 + \omega(\beta).$$

By theorem 3.1.1, there is a polynomial $u(t)$, such that $\mu(\beta, t) = u(t)^2 - v(t)$ with $\deg(v) \leq 1$. The numerator of the coefficient of t in v is the function f. Since $\mu(a_i, t)$ is a square for each $a_i \,\epsilon\, A$, we have that $v(t) = 0$ on A. Therefore, f is 0 on A.

The proposition gives some necessary conditions for there to be additional $Q[t]$ points on the curve $y^2 = r_A(x)$. We summarize these conditions in the corollary below.

Corollary 3.2.10 *Let $A \,\epsilon\, \mathcal{S}$ and $s(t) \,\epsilon\, \mathbb{Q}[t]$. Suppose $r_A(x)$ satisfies conjecture 3.2.8.*

1. *If $r_A(\beta)$ is a square, then β must be a zero of $\omega(x)$.*

2. *If $r_A(\pm t + \beta)$ is a square, then there is only one possible value of β outside of A.*

3. *If $r_A(s(t))$ is a square and $c_0(s) = \beta$, then $\omega(\beta)$ must be a square.*

4. *If $c_2(r_{4,A})$ is not a square, then all points in $\mathbb{Q}[t] \times \mathbb{Q}[t]$ on $y^2 = r_A(x)$ have x-coordinate equal to $a_i \pm t$, $a_i \,\epsilon\, A$.*

Proof: By proposition 3.2.9,

$$r_A(\beta) = c_6(r_0, A)\, t^6 + \cdots + \omega(\beta).$$

Since, r_A is even in t, this can only be a square if the constant term is 0.

If $r_A(\pm t + \beta)$ is a square, then the function f defined in proposition 3.2.9 must be 0 at β. Since $f(a_i) = 0$ for each of the six values of A and $\deg(f) = 7$, we have part 2.

Parts 3 and 4 of the corollary follow easily from parts 3 and 4 of proposition 3.2.9.

Finally, we add that if $c_2(r_{4,A})$ is a square, then we can always parameterize the points on $r_{4,A}(t) = b^2$. If $c_2(r_{4,A}) = a^2$ the parameterization is

$$t = \frac{c_0(r_{4,A}) - m^2}{2 \cdot m \cdot a}, \ m \ \epsilon \ Q.$$

This gives

$$b = \frac{m^2 + c_0(r_{4,A})}{2 \cdot m}.$$

Therefore, whenever $c_2(r_{4,A})$ is a square, we can make a change of variables so that there are two points at infinity on the curve $y^2 = r_A(x)$. In this case we will always choose one of the points at infinity to be the identity of the Mordell-Weil group. Therefore, whenever, we have $c_2(r_{4,A})$ a square, we will refer to one of the points at infinity as the identity.

3.2.5 Nagao's Sum

The sums $s_E(N)$, $S_E(N)$ and $G_E(N)$ introduced earlier are defined for elliptic curves defined over the rationals. We would like to have a similar sum for estimating the rank of an elliptic curve defined over $\mathbb{Q}(t)$. Nagao has developed just such a sum ([22]). Let E be an elliptic curve defined over $\mathbb{Q}(t)$ and let E_{t_0} be the curve specialized at the specific value t_0. Let $a_p(t_0)$ be the value a_p for the curve E_{t_0} and consider the sum

$$A_p(E) = \frac{1}{p} \sum_{t_0 \epsilon \mathbb{F}_p} a_p(t_0).$$

This sum is simply an average of the values a_p for each possible specialization of the curve E. Now consider the sum

$$H_E(N) = -\frac{1}{N} \sum_{\substack{p \leq N \\ p \text{ prime}}} A_p(E) \log p.$$

As mentioned earlier, under the right conditions this sum is "equivalent" to

$$H'_E(N) = -\frac{1}{\pi(N)} \sum_{\substack{p \leq N \\ p \text{ prime}}} A_p(E).$$

By equivalent we mean as in the statement of theorem 1.3.3. We can then interpret the sum $H_E(N)$ as an average of the values $-a_p$ over all specializations and over all primes less than or equal to N.

Nagao has shown that for some elliptic curves defined over $\mathbb{Q}(t)$, the sum $H_E(N)$ does in fact converge to the rank of the elliptic curve. This gives strong evidence to suggest that this sum is a good predictor of rank.

3.3 Constructing Curves of Rank 13 over $\mathbb{Q}(t)$

3.3.1 Finding Elements of $\mathcal{S}$

Before we can use any of the information in the preceding section to find curves with *more* than the 12 constructed points, we need to find some six-tuples, A, which lie in $\mathcal{S}$. Our initial procedure for finding $A \,\epsilon\, \mathcal{S}$ went as follows. Let

$$A = [0, a_2, a_3, a_4, a_5, \varepsilon]$$

and write $r_5(A)$ as a polynomial in ε. For each integral root, ε, of this polynomial, test to see if ε is relatively prime to the a_i. By carrying out this procedure for many choices of a_i, we observed that a small number of A which produced an elliptic curve, had the form

$$A = [0, a, a + \gamma, b, c, c + \gamma].$$

These particular A stood out because, Nagao's rank 13 curve over $\mathbb{Q}(t)$ was derived from an A of this form: $[0, 25, 57, 104, 116, 148]$. For A of this form, we found by direct calculation that $r_5(A)$ is a degree 3 polynomial in γ with $\gamma = b - c - a$ a root. If we let $\gamma = b - c - a$, then $A = [0, a, b - c, b, c, b - a]$. If we translate the elements of this A by $-\frac{b}{2}$ and reorder, then we see that A is equivalent to the vector

$$A' = [\frac{b}{2}, -\frac{b}{2}, a - \frac{b}{2}, \frac{b}{2} - a, c - \frac{b}{2}, \frac{b}{2} - c].$$

From this representation, we see that $r_{A'}(x)$ is even in x and so $r_5(A')$=0. However, 6 of the twelve constructed points are negatives of the other 6.

We then let

$$h(\gamma) = \frac{r_5(A)}{\gamma + c - b + a}.$$

This is a degree 2 polynomial in γ, with the discriminant a cubic in a. This led to the following proposition which is proved by simply working out the calculation.

Propostion 3.3.1 *Let*

$$A = [0, a, a + \gamma, 2^8 b - 2^4 b^2, 2^7 b, 2^7 b + \gamma],$$

let $h(\gamma)$ *be as defined above and let* $d_0 = (b - 16) \cdot 2^8 \cdot b^2$*.* $h(\gamma)$ *is of degree 2 in* γ *and the discriminant of* h *is*

$$d = d_0^2 \cdot (a^3 + f_2(b)\, a^2 + f_1(b)\, a + f_0(b)),$$

where

$$f_2(b) = 17b^2 - 672b + 2304,$$
$$f_1(b) = 32b^4 - 5376b^3 + 131072b^2 - 589824b \text{ and}$$
$$f_0(b) = 256b^6 - 12288b^5 + 475136b^4 - 7864320b^3 + 37748736b^2.$$

Therefore, for each value δ *on the curve defined by*

$$\delta^2 = a^3 + f_2(b)\, a^2 + f_1(b)\, a + f_0(b)),$$

we can factor $h(\gamma)$ *over* $\mathbb{Q}$*. The two roots of* h *give rise to the two choice of roots* *described by*

$$
\begin{aligned}
A \quad = \quad & [0, a^3 - 256\, b\, a^2 + 16384\, b^2\, a, \\
& a^3 - 256\, b\, a^2 + (32\, b^4 - 1024\, b^3 + 24576\, b^2)\, a + \\
& (512\, b^6 - 20480\, b^5 + 262144\, b^4 + (32\, \delta\ - 1048576)\, b^3 - 512\, \delta\, b^2), \\
& (-16\, b^2 + 256\, b)\, a^2 + (4096\, b^3 - 65536\, b^2)\, a + \\
& (-262144\, b^4 + 4194304\, b^3), \\
& 128\, b\, a^2 - 32768\, b^2\, a + 2097152\, b^3, \\
& 128\, b\, a^2 + (32\, b^4 - 1024\, b^3 - 24576\, b^2)\, a + (512\, b^6 - 20480\, b^5 \\
& +262144\, b^4 + (32\, \delta\ + 1048576)\, b^3 - 512\, \delta\, b^2)] \\
& \textit{and} \\
A' \quad = \quad & [0, a^3 - 256\, b\, a^2 + 16384\, b^2\, a, \\
& a^3 - 256\, b\, a^2 + (32\, b^4 - 1024\, b^3 + 24576\, b^2)\, a + \\
& (512\, b^6 - 20480\, b^5 + 262144\, b^4 + (-32\, \delta\ - 1048576)\, b^3 + 512\, \delta\, b^2), \\
& (-16\, b^2 + 256\, b)\, a^2 + (4096\, b^3 - 65536\, b^2)\, a + \\
& (-262144\, b^4 + 4194304\, b^3), \\
& 128\, b\, a^2 - 32768\, b^2\, a + 2097152\, b^3, \\
& 128\, b\, a^2 + (32\, b^4 - 1024\, b^3 - 24576\, b^2)\, a + (512\, b^6 - 20480\, b^5 \\
& +262144\, b^4 + (-32\, \delta\ + 1048576)\, b^3 + 512\, \delta\, b^2)].
\end{aligned}
$$

for which $r_5(A) = 0$ *and* $r_5(A') = 0$.

3.3.2 Examples

By searching, through A of the form given by the preceding section with the added condition that $c_2(r_{4,A})$ be a square, we have found the following rank 13 curves over $\mathbb{Q}(t)$:

A	x
$[0, 87, 164, 264, 375, 452]$	$7/31 \cdot t + 10848/31$
$[0, 55, 146, 255, 260, 346]$	$-7/27 \cdot t + 6920/27$
$[0, 355, 602, 910, 1580, 1827]$	$19/89 \cdot t + 127890/89$
$[0, 97, 104, 129, 500, 532]$	$1/23 \cdot t + 9804/23$
$[0, 42, 47, 82, 152, 175]$	$1/21 \cdot t + 410/3$
$[0, 37, 62, 110, 180, 205]$	$7/23 \cdot t + 1271/23$

The x column is the value of the x-coordinate of the additional point. Note that in each of these cases, we can parameterize the curve $s^2 = r_{4,A}(t)$ so that each of these curves contains two points at infinity. With one of these points taken to be the identity, we have found that the remaining 13 points are linearly independent. (In section 4.2.1 we describe how we check for linear independence.)

In most of the curves found to have rank 13 (including Nagao's curve), we found that $\omega(\beta)$ factored as the product of a linear factor, ω_1, and a cubic, ω_2. By looking for roots of $\omega_1 - a^2 \cdot \omega_2$ for some small set of integers a, we found at least one root which extended to a point on the curve $y^2 = r_A(x)$. For all but one of the curves found, such a point was linearly independent of the 12 constructed points. All of the x-coordinates above represent values of β found this way that were extended to points on the curve.

Kihara has shown that it is possible to find an elliptic curve over whose function field, Nagao's curve contains one more point, bringing the rank to 14. Kihara has similarly extended the rank of curves found by Fermigier and himself to produce infinite families of curves defined over $\mathbb{Q}$ of high rank with nontrivial torsion (see the table in section 1.1.2). Unfortunately, he does not describe his technique, but rather, just gives the curve.

3.4 Producing Curves over $\mathbb{Q}(t)$ with Nontrivial Torsion

3.4.1 Preliminaries

Nagao has shown that for any elliptic curve of the form

$$y^2 = a\,x^4 + b\,x^2 + c,$$

if the point (x, y) is taken to be the identity of the group, then $(-x, -y)$ is a point of order 2 ([20]). Fermigier has used this fact and theorem 3.1.1 to construct a curve of rank 8 over $\mathbb{Q}(t)$ with a point of order 2 ([3]). Kihara has since extended this result in the same manner as above to a curve of rank 9 ([6]).

We show how to use theorem 3.1.1 to construct curves over $\mathbb{Q}(t)$ with points of order 3 and 6. The construction follows the same general principal as in the preceding section. We let A be a set of values in $\mathbb{Q}(t)$ and form $p_A(x)$, the monic polynomial with exact roots equal to the elements of A. In this case we choose 8 elements to be in A. This gives a $g_A(x)$ of degree 4 and an $r_A(x)$ of degree no greater than 3 with

$$p_A(x) = g_A(x)^2 - r_A(x)$$

as before. If the degree of $r_A(x)$ is in fact 3 (and not strictly less than 3) and if $r_A(x)$ has no double roots, then we have that the curve $y^2 = r_A(x)$ is an elliptic curve. This curve will contain the eight points $(\alpha_i, g_A(\alpha_i))$ for each $\alpha_i \;\epsilon\; A$. Although this construction defines a curve with fewer points, the advantage is that we get an elliptic curve for almost every choice of A.

3.4.2 Curves Containing Points of Order 3

Similar to the general case, we let $\mathcal{A} = [a_1 + t, a_1 - t, a_2 + t, a_2 - t, ..., a_4 + t, a_4 - t]$ and let $A = [a_1, a_2, a_3, a_4]$, with each $a_i \;\epsilon\; \mathbb{Q}$. Let the polynomial $p_{\mathcal{A}}(x) = p_A(x)$ be the monic polynomial whose exact roots are the elements of $\mathcal{A}$. Note that we can define an equivalence relation and a set analagous to those in definitions 3.2.3 and 3.2.4. We would then get results similar to those of proposition 3.2.5 and 3.2.6. We do not prove these facts in such generality here. Let us simply observe that without loss of generality, we may assume that $a_1 = 0$ and that $a_2 = 1$. We let $a_3 = c$ and $a_4 = d$ for simplicity. If we now let $r_A(x)$ be as given by theorem 3.2.1, then we have

$$\begin{aligned}
\tfrac{4}{t^2} \cdot r_A(x) = \quad & (4\,c^3 + (-4\,d - 4)\,c^2 + \\
& (-4\,d^2 + 8\,d - 4)\,c + (4\,d^3 - 4\,d^2 - 4\,d + 4))\; x^3 + \\
& \quad ((-4\,d - 4)\,c^3 + (8\,d^2 + 4\,d + 8)\,c^2 + \\
& \quad (-4\,d^3 + 4\,d^2 + 4\,d - 4)\,c + \\
& \quad (-4\,d^3 + 8\,d^2 - 4\,d))\; x^2 + \\
& \qquad ((-4\,t^2 + 4\,d)\,c^3 + ((4\,d + 4)\,t^2 + \\
& \qquad (-8\,d^2 - 8\,d))\,c^2 + ((4\,d^2 - 8\,d + 4)\,t^2 + \\
& \qquad (4\,d^3 - 8\,d^2 + 4\,d))\,c + \\
& \qquad (-4\,d^3 + 4\,d^2 + 4\,d - 4)\,t^2)\,x + \\
& \qquad\quad (t^2\,c^4 + ((-2\,d^2 - 2)\,t^2 + 4\,d^2)\,c^2 + \\
& \qquad\quad (d^4 - 2\,d^2 + 1)\,t^2).
\end{aligned}$$

We set $s(x) = \frac{4}{t^2} r_A(x)$ and examine the conditions placed on the coefficients if we demand that $x = 0$ give a point of order 3. There are two conditions that must be satisfied:

1. $s(0)$ must be a square, and
2. $s'(x)^2 - 2 \cdot s''(x) \cdot s(x)$ evaluated at $x = 0$, must equal 0.

The first simply guarantees that 0 is the x-coordinate of point on the curve and the second gives that $x = 0$ is a point of inflection of $y^2 = s(x)$.

Observe that $s(0)$ is the polynomial in t given by

$$s(0) = (c^4 + (-2\,d^2 - 2)\,c^2 + (d^4 - 2\,d^2 + 1))\,t^2 + 4\,d^2\,c^2.$$

The discriminant of this polynomial is

$$\Delta = 16 \cdot c^2 \cdot d^2 \cdot (-c^4 + (2\,d^2 + 2)\,c^2 + (-d^4 + 2\,d^2 - 1)),$$

which equals

$$16 \cdot c^2 \cdot d^2 \cdot (c + d + 1) \cdot (c - d - 1) \cdot (c + d - 1) \cdot (c - d + 1).$$

Therefore, we have that $s(0)$ is a square if one of the linear factors is 0. Since, by replacing c with $-c$ or d with $-d$, we see that in fact these conditions are equivalent, we let $d = -c - 1$.

If we let $A = [0, 1, c, -c - 1]$, then the resulting $r_A(x)$ has a lead coefficient of $-8 \cdot c \cdot (c + 1)$. So then, if we let $\gamma = (-2) \cdot c \cdot (c + 1)$ and let $A = [0, 1, c, -c - 1] \cdot \gamma$, we have

$$\begin{aligned} \frac{r_A(x)}{\alpha^2} \quad = \quad & x^3 \; + \; (c^2 + c + 1)^2 \; x^2 - \\ & (t^2 \; - \; 2\,c^6 + 6\,c^5 + 8\,c^4 + 6\,c^3 + 2\,c^2) \; x \; + \; (c^2 + c)^4 \; . \end{aligned}$$

where $\alpha = 2\gamma^2$. We let $r(x) = \frac{r_A(x)}{\alpha^2}$.

In addition to the eighteen points whose x-coordinates are $0, \pm t, \gamma \pm t, \gamma c \pm t, -\gamma(c + 1) \pm t$, we find that the curve $y^2 = r_A(x)$ contains the six points whose x-coordinates are $-c^2, -(c+1)^2$ and $-c^2 \cdot (c+1)^2$. (We remark that these points generate a subgroup of rank 4 over $\mathbb{Q}(c, t)$.)

Now consider the second condition– that there be a point of inflection on the curve $y^2 = r(x)$ at the point $P = (0, c^2 \cdot (c + 1)^2)$. We define $\delta_3(x)$ to be

$$\delta_3(x) = r'(x)^2 - 2 \cdot r''(x) \cdot r(x).$$

The condition that P be a point of inflection on $y^2 = r(x)$ is equivalent to the condition that $\delta_3(0) = 0$. We have that

$$\delta_3(0) = (t^2 - 4 \cdot c^2 \cdot (c + 1)^2 \cdot (c^2 + c + 1)) \cdot t^2.$$

Observe that if we can parameterize the solutions to $(c^2 + c + 1) = u^2$, then we get that for $t = 2 \cdot c \cdot (c + 1) \cdot u$, $\delta_3(0) = 0$. Since $(0, 1)$ is a point on the curve $c^2 + c + 1 = u^2$, we can parameterize the solutions. Letting m be any rational number, we get that all solutions to $c^2 + c + 1 = u^2$ are described by

$$c = -\frac{2m - 1}{m^2 - 1} \quad \text{and} \quad u = -\frac{m^2 - m + 1}{m^2 - 1}.$$

With this substitution, the curve is defined over $\mathbb{Q}(m)$ with twenty four known $\mathbb{Q}(m)$-rational points. Two of these points, P and $-P$, are points of order three. By specializing at $m = 10$, we determine that the subgroup generated by the remaining twenty two points has rank 3– one less than the rank of the curve before the substitution. This, then gives an infinte family of elliptic curves defined over the rationals of rank at least 3 containing a point of order 3.

3.4.3 Curves with Torsion Subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$

If we in the above, we let $t = 0$, then we see that in this case, we have $\delta_3(0) = 0$ as well. Therefore, the curve $y^2 = r_A(x)$ contains a point of order three when $t = 0$. Furthermore, we find that $r_A(x)$ is 0 when x is any one of $-c^2, -(c+1)^2, -c^2 \cdot (c+1)^2)$. This gives

$$s_A(x) = (x + (c+1)^2) \cdot (x + c^2) \cdot (x + (c(c+1))^2),$$

where $s_A(x)$ is the function $r_A(x)$ evaluated at $t = 0$. Since, there are three $\mathbb{Q}(c)$-rational points of order two and one $\mathbb{Q}(c)$-rational point of order three on the curve $y^2 = s_A(x)$, by Mazur's result, it must be that the torsion subgroup of this elliptic curve is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. In fact, we find that each of the remaining six constructed points is a point of order six.

Consider a point with x-coordinate, $a \cdot c^2$ on the curve $y^2 = s_A(x)$. We find that $s_A(a \cdot c^2) = (a+1)c^4 \cdot ((a+1)\ c^4 + ... + (a+1))$. We would therefore like $(a+1)$ to be a square. We let $a = b^2 - 1$. If we let $b = 2$, then $a = 3$ and we have that

$$s_A(3c^2) = 4 \cdot c^4 \cdot (4\,c^2 + 2\,c + 1) \cdot (c^2 + 2\,c + 4).$$

If $\alpha\ \epsilon\ \mathbb{Q}$, then we have that $s_A(3c^2)$ is a square whenever c is a root of

$$(4\,c^2 + 2\,c + 1) - \alpha^2 \cdot (c^2 + 2\,c + 4).$$

The discriminant of this quadratic polynomial in c is $-12(\alpha^4 - 5\alpha^2 + 1)$. Therefore, if we let C be the elliptic curve defined by

$$C : y^2 = -12(\alpha^4 - 5\alpha^2 + 1),$$

then we can consider the curve $y^2 = s_A(x)$ as defined over the function field $\mathbb{Q}(C)$. The curve then contains a point with x-coordinate equal to $3c^2$. One point on C gives rise to the value $c = 11$. With $c = 11$, the point whose x-coordinate on the curve $y^2 = s_A(x)$

is $3 \cdot 11^2$, is of infinite order. Finally, we found that the curve C contains more than 16 points. By Mazur's result on possible torsion subgroups, there must be a point of infinite order on C. For all but finitely many values of c corresponding to points on C, the specialization map is injective (see [24, section C.20]). Therefore, we have that there are infinitely many curves defined over $\mathbb{Q}$ of rank at least 1 with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

Alternatively, consider a point, Q, with x-coordinate $c^2 + c$. We have that

$$s_A(c^2 + c) = (c^2 + c + 1) \cdot c^2 \cdot (c + 1)^2 \cdot (2c + 1)^2.$$

Therefore, if we again let $c = (1 - 2m)/(m^2 - 1)$, then the point Q is $\mathbb{Q}(m)$-rational. With this value of c, the point Q is of infinite order and we have another infinite family of curves over $\mathbb{Q}$ of rank at least 1 whose torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

3.4.4 Curves with Torsion Subgroup Containing $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

Nagao has proved ([20]) that curves whose affine quartic model is of the form

$$y^2 = a^2\,x^4 \; + \; c\,x^2 \; + \; e$$

contain a point of order two. If we choose O to be the identity, then O' is such a point. Kihara has proven ([6]) that if e is a square, then the curve in fact contains three points of order 2. Kihara shows this by giving a birational map that takes the quartic model to Weierstrass form $y^2 = f(x)$, with $f(x)$ a cubic. He observes that $f(x)$ can be factored completely when e is a square. We prove the same result by examining the group law on the quartic model. This allows us to prove that e being a square is not only sufficient but also necessary for the curve to contain three points of order 2. Examining the group law on the quartic model also allows us to go further and give conditions for the curve to contain points of order four (see section 3.4.5).

Theorem 3.4.1 *An elliptic curve of the form $y^2 = a^2\,x^4 \; + \; c\,x^2 \; + \; e$ defined over K, with O the identity, has a K-rational point of order 2 in addition to O' if and only if e is a square in K. If this is the case, then there are three points of order two: O', $(0, \sqrt{e})$ and $(0, -\sqrt{e})$.*

Proof: An affine point $P = (x_0, y_0)$ is a point of order 2 if and only if $P = -P$. Recall from section 3.1.3, that the negative of P is the fourth point of intersection of $L(x, y) = 0$ with the elliptic curve, where $L(x, y) = 0$ is the parabola tangent at O' and containing the point P. This parabola is defined by

$$y = a\,x^2 \, + \, (-a\,x_0^2 \, + \, y_0).$$

Plugging this value of y into the equation for the elliptic curve yields

$$(-2\,a^2\,x_0^2 \, + \, (2\,a\,y_0 \, - \, c))\,x^2 \, + \, (a^2\,x_0^4 \, - \, 2\,a\,y_0\,x_0^2 \, + \, (y_0^2 \, - \, e)).$$

If P is a point of order 2, then x_0 should be a double root of this polynomial. This implies that

$$\frac{(a^2\,x_0^4 \, - \, 2\,a\,y_0\,x_0^2 \, + \, (y_0^2 \, - \, e))}{(-2\,a^2\,x_0^2 \, + \, (2\,a\,y_0 \, - \, c))} \, - \, x_0^2 \, = \, 0.$$

Since $y_0^2 = a^2\,x_0^4 \, + \, c\,x_0^2 \, + \, e$, the numerator of this fraction is

$$x_0^2 \cdot (4\,a^2\,x_0^2 \, + \, (-4\,a\,y_0 \, + \, 2\,c))).$$

Therefore, we have that either $x_0 = 0$ or

$$y_0 = a\,x_0^2 + \frac{c}{2\,a}.$$

If the latter occurs, we may plug this value of y_0 back into the equation of the curve and obtain

$$\frac{c^2 \, - \, 4\,a^2\,e}{4\,a^2} \, = \, 0.$$

The numerator of this fraction is the discriminant of the polynomial $a^2\,x^4 \, + \, c\,x^2 \, + \, e$. Since this polynomial cannot have a double root, the discriminant must be nonzero. Therefore y_0 cannot be $a\,x_0^2 + \frac{c}{2\,a}$.

If $x_0 = 0$, then we clearly get the statement of the theorem.

We now construct an example of a curve containing three points of order two. Let $A_b = [0, b, 1+t, 1-t, b+t, b-t]$. Let

$$\begin{aligned} q_{A_b}(x) \quad &= \quad \prod_{\alpha \;\epsilon\; A_b} (x - \alpha), \text{ and let} \\ p_{A_b}(x) \quad &= \quad q_{A_b}(x) \cdot q_{A_b}(-x). \end{aligned}$$

The roots of $p_{A_b}(x)$ are α and $-\alpha$ for each $\alpha \in A_b$ and so $p_{A_b}(x)$ is even in x. If we let $r_{A_b}(x)$ be as given by theorem 3.2.1, then $r_{A_b}(x)$ is even and so has degree less than or equal to 4. The degree 4 coefficient of $2^8 \cdot r_{A_b}(x)$ is equal to a degree 4 polynomial in t. The degree 4 coefficient of this polynomial in t is

$$2112\, b^4 - 4096\, b^2 + 2048.$$

We found that for $b = 7/4$, this is a square. If we let $r_t(x) = 2^{32} \cdot r_{A_{7/4}}$, then we have

$$\begin{aligned}
r_t(x) &= a(t)\, x^4 \,+\, c(t)\, x^2 \,+\, e(t), \text{ where} \\
a(t) &= 156233629696\, t^4 + 113235197952\, t^2 - 2288978944 \\
c(t) &= -93222600704\, t^6 + 175675015168\, t^4 - 308486664192\, t^2 + 3395820736 \text{ and} \\
e(t) &= 10070523904\, t^8 - 757858304\, t^6 + 22663102464\, t^4 - \\
&\quad\; 852220544\, t^2 + 12734445409.
\end{aligned}$$

We find that the point with t-coordinate equal to $-307527185/1807165536$ is a point of infinite order on the curve $s^2 = a(t)$. We let K be the function field of the curve $s^2 = a(t)$ and let $t_0 = -307527185/1807165536$. If we let A be $A_{7/4}$ evaluated at t_0, then we find that the subgroup generated by the points on the elliptic curve $y^2 = r_{t_0}(x)$ whose x-coordinates are the nonzero elements of A has rank 5. By theorem 3.4.1, the points with x-coordinate 0 are points of order 2. Since the specialization map is injective almost everywhere, the curve $y^2 = r_t(x)$ defined over $\mathbb{Q}(K)$ has rank at least 5 and contains three points of order 2.

We note that one may find other values of b for which this contruction works.

3.4.5 Curves with Torsion Subgroup Containing $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$

Observe that we can further examine the group law on the quartic model to compute what must be true for the torsion subgroup to contain $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. If a curve is to have a point of order four, then it must have a point of order two and so without loss of generality we can assume the curve is of the form $y^2 = x^4 + c\,x^2 + e$ with O the identity. If we demand that P be a point such that $2P = O'$, then P is a point of order four. The group law on the quartic implies that P must be a root of the polynomial $f(x) = x^4 + c\,x^2 + e$. If $f(x)$ has one root in some field K, then either $f(x)$ has two roots in K or four roots in K depending on whether or not e is a square in K. This then imposes conditions on the torsion subgroup. We summarize the situation in the following theorem.

Theorem 3.4.2 *Let $f(x) = x^4 + cx^2 + e^2$ and let E be the elliptic curve defined by $y^2 = f(x)$. Let c and e^2 be in K, let α be a root of $f(x)$ and let $\mathbb{T}$ be the torsion subgroup of $E(K)$.*

1. *If $\alpha \in K$, then $\mathbb{Z}/4\mathbb{Z} \subset \mathbb{T}$ with $(\pm\alpha, 0)$ points of order four. If e is not in K, then $\mathbb{T} = \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/12\mathbb{Z}$.*

2. *If $\alpha \in K$ and $e \in K$, then $\mathbb{T} = \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$, with $(\pm\alpha, 0), (\pm\frac{e}{\alpha}, 0)$ points of order 4.*

If we have that $f(x') = (x'-\alpha)(x'+\alpha)((x')^2-\epsilon^2)$ and the elliptic curve E' is defined by $(y')^2 = f(x')$, then by making the change of variables $y' = \alpha^2 y$ and $x' = \alpha x$, we see that E' is isomorphic to the curve E_{e^2} defined by:

$$y^2 = (x-1)(x+1)(x^2-e^2), \quad \text{where } e = \frac{\epsilon}{\alpha}.$$

We can now easily construct examples of elliptic curves with torsion subgroup containing $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ by choosing an appropriate value of e^2. We have the following:

1. If we let $t = (-m^2+2)/(2m)$, then the elliptic curve defined by $y^2 = (x^2 - 1)(x^2 - 4t^2)$ has torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. A point with x-coordinate t^2+1 is $\mathbb{Q}(m)$-rational and of infinite order.

2. If we let $t = (m^2+1)/(2m)$, then the elliptic curve defined by $y^2 = (x^2-1)(x^2+3t^2)$ has torsion subgroup $\mathbb{Z}/4\mathbb{Z}$. A point with x-coordinate t is $\mathbb{Q}(m)$-rational and of infinite order.

3.4.6 On Curves Containing a Point of Order 3

We conclude our discussion of constructing infinite families of elliptic curves defined over the rationals with a remark regarding curves that contain a point of order three.

Top has proven ([26]) that the Mordell-Weil group of the elliptic curve defined over $\mathbb{Q}(t)$ defined by

$$y^2 = x^3 + (t^2 - (\beta^2 + \beta + 1)^3)(x - (\beta^2 + \beta)^2)^2$$

is isomorphic to $\mathbb{Z}^3$. We note that this curve has a point of order three over the function field of the curve defined by $t^2 - (\beta^2 + \beta + 1)^3 = s^2$. We have found that the curve defined over this function field has rank 3. This gives another infinite family of curves containing a point of order 3. In this case the rank is known to be exactly 3. The curve given in section 3.4.2 has rank at least 4 over $\mathbb{Q}(c, t)$ and only upon specialization of c and t to make the point of order three rational, do we get the curve defined over $\mathbb{Q}(m)$ of rank at least 3. Without further analysis, it is possible that the elliptic curve constructed in section 3.4.2, E, has rank strictly greater than 3, while it is known that the curve constructed from the results of Top does not. However, the sum $H_E(N)$ appears to approach 3 as $N \to \infty$. This gives some indication that the rank of this curve E is in fact equal to 3.

3.5 Applying to Finding Curves over $\mathbb{Q}$ with Nontrivial Torsion

3.5.1 Curves Containing Points of Order 3

From section 3.4.2 we have that the curve

$$E_m : y^2 = x^3 + a_2(m)\, x^2 + a_4(m)\, x + a_6(m),$$

where

$$\begin{aligned}
a_2(m) &= (m^8 - 4\,m^7 + 10\,m^6 - 16\,m^5 + 19\,m^4 - 16\,m^3 + 10\,m^2 - 4\,m + 1),\\
\\
a_4(m) &= (-8\,m^{14} + 56\,m^{13} - 154\,m^{12} + 196\,m^{11} - 42\,m^{10} - 252\,m^9 +\\
&\quad 408\,m^8 - 252\,m^7 - 42\,m^6 + 196\,m^5 - 154\,m^4 + 56\,m^3 - 8\,m^2) \text{ and}\\
\\
a_6(m) &= (16\,m^{20} - 160\,m^{19} + 600\,m^{18} - 840\,m^{17} - 639\,m^{16} + 3480\,m^{15} -\\
&\quad 3100\,m^{14} - 2480\,m^{13} + 6246\,m^{12} - 2480\,m^{11} - 3100\,m^{10} + 3480\,m^9 -\\
&\quad 639\,m^8 - 840\,m^7 + 600\,m^6 - 160\,m^5 + 16\,m^4)
\end{aligned}$$

contains the point of order three given by

$$(0, 4\,m^{10} - 20\,m^9 + 25\,m^8 + 20\,m^7 - 58\,m^6 + 20\,m^5 + 25\,m^4 - 20\,m^3 + 4\,m^2).$$

Furthermore, the three points whose x-coordinates are

$$4\,m^7 - 22\,m^6 + 38\,m^5 - 10\,m^4 - 34\,m^3 + 32\,m^2 - 8\,m,$$
$$4\,m^7 - 14\,m^6 + 14\,m^5 - 14\,m^3 + 14\,m^2 - 4\,m \text{ and}$$
$$8\,m^7 - 24\,m^6 + 10\,m^5 + 20\,m^4 - 18\,m^3 + 4\,m^2$$

are linearly independent points for almost all $m \in \mathbb{Q}$. We will denote a specialization of this curve at a particular rational value m as E_m.

We let $S = \{\frac{a}{b} \in \mathbb{Q} \mid 1 \le b \le 10 \text{ and } 1 \le |\frac{a}{b}| \le 10\}$. For each m in S, we computed Mazur's bound and $G_{E_m}(p_{500})$ for the curve. If both bounds were greater than 3, we searched the curve for additional points. In this way, we were able to find only one curve with rank strictly greater than 3. The curve is listed below together with a set of linearly independent points on the minimal Weierstrass form of the curve.

m	rank	m_E	$G_E(p_{500})$	Independent points
9/2	≥ 4	7	5	[5393740, 9871250290], [9662620, 27873061810], [3619660, 3903245170], [-4525988, 467348146].

Note that the value listed above for $G_E(p_{500})$ is actually a rounded off value and this is in fact what was used in the sieving process. This is true in the folowing sections as well.

3.5.2 Curves with Torsion Subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$

From section 3.4.3 we have that the curve

$$E_m : y^2 = (x - \alpha(m))(x - \beta(m))(x - \gamma(m)),$$

where

$$\begin{aligned}\alpha(m) &= -4\,m^6+4\,m^5+7\,m^4-8\,m^3-2\,m^2+4\,m-1,\\ \beta(m) &= -m^8+4\,m^7-2\,m^6-8\,m^5+7\,m^4+4\,m^3-4\,m^2,\ \text{and}\\ \gamma(m) &= -4\,m^6+20\,m^5-33\,m^4+20\,m^3-4\,m^2,\end{aligned}$$

contains the points of order six whose x-coordinates are

$$4\,m^7-10\,m^6-4\,m^5+20\,m^4-4\,m^3-10\,m^2+4\,m,$$

$$-8\,m^6+24\,m^5-10\,m^4-20\,m^3+18\,m^2-4\,m \text{ and}$$

$$4\,m^{11}-38\,m^{10}+128\,m^9-167\,m^8-4\,m^7+202\,m^6-148\,m^5+7\,m^4+20\,m^3-4\,m^2.$$

E_m contains a point of infinite order whose x-coordinate is

$$-2\,m^7+5\,m^6+2\,m^5-10\,m^4+2\,m^3+5\,m^2-2\,m.$$

We have found by sieving using Kretschmer's bound, the following curves defined over $\mathbb{Q}$. In some cases we were able to count the number of homogeneous spaces containing a rational solution and show that the Shafarevich-Tate group was trivial from this count alone. In other cases, we were not able to compute the Shafarevich-Tate group. For these curves, by finding the points on the elliptic curve corresponding to the points on each homogeneous space, we achieved a better lower bound on the rank than given by counting alone. For each curve we list a set of linearly independent points on the minimal Weierstrass form of the curve found. See section 4.3.4 (and section 4.2.3) for more details on how this sieving was performed.

m	rank	k_E	$G_E(p_{500})$	Independent points
$\frac{15}{2}$	3	3	3	[17863890, 1223609769360], [111724800, 120095583300], [443454915/4, 749348661795/8]
$\frac{46}{5}$	≥ 3	6	4	[109909065880/9, 1585766951606270/27], [9578699246, -364178333488588], [111508906300/9, 2934207966602830/27]

3.5.3 Curves with Torsion Subgroup Containing $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

In section 3.4.4, we found an elliptic curve $y^2 = r_t(x)$ with the lead term of $r_t(x)$ being $a(t)$. If we let C be the curve defined by $s^2 = a(t)$, then we found that $y^2 = r_t(x)$ defined over $\mathbb{Q}(C)$ has three points of order 2. The curve can be written in Weierstrass form as

$$E_t : y^2 = (x - \alpha(t)) \cdot (x - \beta(t)) \cdot (x + \beta(t)),$$

where

$$\alpha(t) = -93222600704\, t^6 + 175675015168\, t^4 - 308486664192\, t^2 + 3395820736$$

and

$$\beta(t) = 200704\, s\, t^4 - 7552\, s\, t^2 + 225694\, s.$$

We let

$$\begin{aligned} x_1(t, s) = \quad & -540672\, s\, t^4 - 1622016\, s\, t^3 + (2\, s^2 - 1755584\, s)\, t^2 + \\ & (4\, s^2 - 20096\, s)\, t + (2\, s^2 + 235298\, s), \\ x_2(t, s) = \quad & -540672\, s\, t^4 - 2838528\, s\, t^3 + (2\, s^2 - 3178048\, s)\, t^2 + \\ & (7\, s^2 - 911008\, s)\, t + (49/8\, s^2 + 81634\, s), \text{ and} \\ x_3(t, s) = \quad & -200704\, s\, t^4 + 2852480\, s\, t^2 + (49/8\, s^2 + 81634\, s). \end{aligned}$$

The curve C is itself an *elliptic* curve and contains the point $P = [49/176, 10427592/121]$ of infinite order on C. Specializing at the point P does not yield a smooth curve, but $2P = [-307527185/1807165536, 553304883862791998/16524891082953]$ does. Upon specialization at $2P$, we find that the five points $x_1(t, s), x_1(-t, s), x_2(t, s), x_2(-t, s)$, and $x_3(t, s)$ are linearly independent. Unfortunately, the points on C in the subgroup generated by P were the only points we could find on C. The values of t and s corresponding to nP for $n > 2$ are quite large and make searching for additional points very difficult. We had similar failure when trying to perform a descent. We point out however, that Mazur's bound for this curve is 38.

3.5.4 Curves with Torsion Subgroup $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$

We have found the following curves by sieving in the same manner as above, beginning with the curves given in section 3.4.2, 3.4.5 and in section 3.4.3.

m	rank	k_E	$G_E(p_{500})$	Independent points
$(\mathbb{Z}/4\mathbb{Z} \subset \mathbb{T})$ $y^2 = x^3 + (-6\,m^4 - 4\,m^2 - 6)\,x^2 + (9\,m^8 + 60\,m^6 + 118\,m^4 + 60\,m^2 + 9)\,x$				
$\frac{43}{5}$	3	3	4	[-199919, 216785257], [83533, 157017965], [-429467, 28455035]
$\frac{25}{7}$	$3 \leq r \leq 4$	4	5	[-14431, 12552913], [-40747, 8774675], [30053, 14651075]
$(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \subset \mathbb{T})$ $y^2 = x^3 + (-m^4 - 6\,m^3 + 3\,m^2 + 12\,m - 4)\,x^2 + (4\,m^7 + 8\,m^6 - 20\,m^5 - 32\,m^4 + 40\,m^3 + 32\,m^2 - 32\,m)\,x$				
$\frac{41}{5}$	$3 \leq r \leq 4$	3	4	[-354245,95315220], [-178502, 127300446], [825620284/1681, 9695052447120/68921]
$\frac{43}{7}$	3	3	3	[-416110, 208228410], [-452650, 181068750], [1131518900/1849, 19439056350000/79507]
$\frac{23}{9}$	$3 \leq r \leq 5$	4	5	[-12693, 438281], [-9413, 988091], [7977269/529, 17186141403/12167]

Chapter 4

Algorithms and Code

Unless otherwise stated, all the code represented here is written in the language *GP*. The program uses the C library of functions *PARI*. We used GP version 1.39 on an ultrasparc processor running the solaris 2.0 operating system. Some minor changes have been made to make the code more readable, but otherwise it is the exact code used to perform all calculations presented. As mentioned later, since GP is an interpreted language, the speed of the algorithms would be greatly improved by implementing the code in a compiled language.

4.1 Weierstrass Form

4.1.1 The Quartic Model to Weierstrass Form

This set of functions transforms a quartic of the form: $a^2x^4 + bx^3 + cx^2 + dx + e = y^2$ to Weierstrass form. The functions also move the points originally on the quartic to the newcurve. In the code below, q is the vector $[a, b, c, d, e]$. Note that the first component is a and not a^2. *ecurve* gives the 5-tuple representing the elliptic curve: $[a_1, a_2, a_3, a_4, a_6]$.

```
ecurve(q)=
       [ 0,  q[3],  0,  q[2]*q[4]-4*q[1]^2*q[5]
         q[2]^2*q[5]+q[1]^2*q[4]^2-4*q[1]^2*q[3]*q[5] ]
```

The function *newxy* takes a point, *xy=[xy[1],xy[2]]*, on the quartic model and returns a point on the elliptic curve in Weierstrass form given by *ecurve*. *eptz* performs *newxy* on a list of points.

```
newxy(q,xy) =
      x1=xy[1];
      y1=xy[2];
      [ -2*q[1]*y1+2*q[1]^2*x1^2+q[2]*x1,
          4*q[1]^2*x1*y1+q[2]*y1-4*q[1]^3*x1^3-
          3*q[1]*q[2]*x1^2-2*q[1]*q[3]*x1-q[1]*q[4] ];


eptz(q,manyxy) = vector(length(manyxy),j,newxy(q,manyxy[j]));
```

We give a geometric interpretation of the transformation given by *ecurve*. The parabola which is tangent at the point O' is described by

$$y = a\,x^2 + \frac{b}{2a}\,x + \gamma.$$

The intersection of this parabola with the elliptic curve defined by the quartic model consists of the points O' with multiplicity two and two other points. Therefore, the polynomial in x, $f(x) - y^2$, is a quadratic. The two other points are rational only when the discriminant is a square. (Note that when the two points are rational that they are inverses of each other.) The discriminant, written as a polynomial in γ is the following:

$$-8\,a\,\gamma^3 + 4\,c\,\gamma^2 + \frac{8\,e\,a^2 - 2\,d\,b}{a}\,\gamma + \frac{(-4\,e\,c + d^2)\,a^2 + e\,b^2}{a^2}.$$

If we multiply through by a^2 and make the change of variables $\gamma = -x/(2a)$, then we get the polynomial:

$$g(x) = x^3 + c\,x^2 \;+\; (-4\,e\,a^2 + d\,b)\,x \;+\; ((-4\,e\,c + d^2)\,a^2 + e\,b^2).$$

The curve $y^2 = g(x)$ is precisely the curve given by *ecurve*. (Note that the two points that correspond to a given x are inverses as expected.)

4.1.2 Minimal Weierstrass Form and Laska's Algorithm

The algorithms used to compute Mazur's bound, the rank of a subgroup generated by a set of points and a_p (and hence the sums for sieving) all require an elliptic curve to be in minimal Weierstrass form. We use an algorithm due to Laska to perform this task. Laska's algorithm requires the curve to have integral coefficients and so our first function, *makeintegral* does just that. The two functions that follow, *laska* and *aiprimes*, perform Laska's algorithm precisely as given in [12].

Recall that if $u = 1/n$ and $r = s = t = 0$, then the transformation defined in theorem 1.2.1 takes the curve

$$[a_1, a_2, a_3, a_4, a_6] \quad \text{to} \quad [n\, a_1, n^2\, a_2, n^3\, a_3, n^4\, a_4, n^6\, a_6].$$

makeintegral computes the minimal u necessary to make each coefficient in the latter curve an integer.

```
makeintegral(eevec,u,den1,den2,den3,den4,den5,dens,primez,maxexp) =
        u=1;
        den1=vec(factor(denom(eevec[1])));
        den1=[den1[1]~,den1[2]~];
        den2=vec(factor(denom(eevec[2])));
        den2=[den2[1]~,vector(length(den2[2]),j,ceil(den2[2][j]/2))];
        den3=vec(factor(denom(eevec[3])));
        den3=[den3[1]~,vector(length(den3[2]),j,ceil(den3[2][j]/3))];
        den4=vec(factor(denom(eevec[4])));
        den4=[den4[1]~,vector(length(den4[2]),j,ceil(den4[2][j]/4))];
        den5=vec(factor(denom(eevec[5])));
        den5=[den5[1]~,vector(length(den5[2]),j,ceil(den5[2][j]/6))];
        dens=[den1,den2,den3,den4,den5];
        primez=den1[1];
        for(j=2,5,primez=setunion(primez,dens[j][1]));
        primez=vector(length(primez),j,
                    [primez[j],vector(5,jj,setsearch(dens[jj][1],primez[j]))]);
        for(j=1,length(primez),
            maxexp=0;
            pj2=primez[j][2];
            for(jj=1,5,
```

```
                if(pj2[jj]!=0,maxexp=max(maxexp,dens[jj][2][pj2[jj]]),));
            u=u*primez[j][1]^(-maxexp));
[chell(smallinitell(eevec),[u,0,0,0]),[u,0,0,0]];


laska(eevec,u,evec,c4,c6,gev,pjev,ejev,tmpai,uev) =
      mi=makeintegral(e);
      e=mi[1];
      u=mi[2];
      uev=1;
      c4=e[10];
      c6=e[11];
      gev=vec(factor(gcd(c4,c6)));
      tmpai=[1];
      for(jev=1,length(gev[1]),
            pjev=gev[1][jev];
            ejev=floor(gev[2][jev]/4);
            while(ejev,if(c4%(pjev^(4*ejev))+c6%(pjev^(6*ejev)),
                  ejev=ejev-1,
                  if(pjev==2,tmpai=aiprimes(2,ejev,c4,c6,evec);
                        uev=tmpai[1]*uev;
                        ejev=0,
                        if(pjev==3,if(tmpai[1]==1,
                              tmpai=aiprimes(3,ejev,c4,c6,evec);
                              uev=uev*tmpai[1];
                              ejev=0,
                                 tmpai3=aiprimes(3,ejev,c4,c6,evec);
                                 if(tmpai3[1]==1,,uev=uev*tmpai3[1];
                                                  tmpai=[1];
                                                  ejev=0)),
                        uev=uev*pjev^ejev;
```

```
                  tmpai=[1];
                  ejev=0)))));
      if(tmpai[1]==1,preai=aiprimes(uev,1,c4,c6,evec),preai=tmpai);
      p2=preai[2];
      [ preai[3],
        p2[1]*u, p2[2]*u^2, p2[3]*u, p2[4]*u^3] ];

aiprimes(p23,expont,c4ev,c6ev,e,ansa1,xu,yu,u23,
         r23,s23,t23,a1p,a2,a2p,a3,a3p,a4,a4p,a6,a6p) =
      if(expont,a1=e[1];a2=e[2];a3=e[3];a4=e[4];a6=e[5];
      u23=p23^expont;
      xu=c4/u23^4;
      yu=c6/u23^6;
      a1p=xu%8;
      a2p=(-a1p-yu)%3;
      a2p=a2p/2*(5-3*a2p);
      if(a1p==0,if(yu%8==0,a3p=(yu/8)%4,
                  ans=aiprimes(p23,expont-1,c4,c6,e)),
            if(a1p==1,a3p=(a2p+(xu-1)/8)%2,
                  ans=aiprimes(p23,expont-1,c4,c6,e)));
      if(ans,ans,
      a4p=(xu-(a1p+4*a2p)^2+24*a1p*a3p)/(-48);
      a6p=(yu+(a1p+4*a2p)^3-36*(a1p+4*a2p)*(a1p*a3p+2*a4p)+216*a3p)/(-864);
      s23=(u23*a1p-a1)/2;
      r23=(u23^2*a2p-a2+s23*a1+s23^2)/3;
      t23=(u23^3*a3p-a3-r23*a1)/2;
      if(denom(a5p)!=1 || denom(a4p)!=1 || denom(a3p)!=1 ||
         denom(a2p)!=1 || denom(a1p)!=1,  aiprimes(p23,expont-1,c4,c6,e),
            if(u23^4*a4p-(a4-s23*a3+2*r23*a2-
               (t23+r23*s23)*a1+3*r23^2-2*s23*t23)==0 &&
```

```
            u23^6*a6p-(a6+r23*a4+r23^2*a2+r23^3-
            t23*a3-t23^2-r23*t23*a1)==0,
             [p23^expont,[u23,r23,s23,t23],[a1p,a2p,a3p,a4p,a6p]],
        aiprimes(p23,expont-1,c4,c6,e)))),
    [1,[1,0,0,0],e]);
```

4.2 Computing Rank and Searching for Points

4.2.1 Code for Computing Rank of a Subgroup

We employ two methods for estimating rank. The method we discuss here is used to give only a lower bound on the rank. We compute the rank of the subgroup generated by a set of points. In order to get upper bounds on the rank we use the bounds given by Mazur and Kretschmer. In the case of computing Kretschmer's bound, we may also use the results of that computation to produce a lower bound on the rank. (See section 4.2.3 below.)

Recall that there is a function, $\hat{h}$, called the *canonical height*, which defines a positive definite quadratic form on the real vector space $\mathbb{R} \otimes E(\mathbb{Q})$. This canonical height then defines a symmetric bilinear form, called the *canonical height pairing*, in the usual way:

$$< P, Q >= \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q).$$

We then have that, given a set of points, $\{P_1, P_2, ..., P_n\}$, if we let M be the matrix $(< P_i, P_j >)$, the determinant of M is 0 if and only if the points are linearly dependent in the Mordell-Weil group. We call the matrix M, the height matrix for the points $\{P_1, P_2, ..., P_n\}$. We have further that $< P, P >= 0$ if and only if P is a point of finite order. We may use these facts to compute the rank of the subgroup generated by a given set of points.

Given an $n \times n$ matrix M and a vector $v = [i_1, i_2, ..., i_k]$, $k \leq n$, let M' be the matrix (a_{ij}), with i and j both in v. The function *matdet* below, computes the determinant of the matrix M' for a given M and v. Given an elliptic curve e and a set of points, *pts*, *computepts* computes the rank r of the subgroup generated by *pts* and a set of r linearly independent points in this subgroup. Note that while theoreticaly, the determinant is exactly 0 when the points are linearly dependent, the existence of precision error requires us to test for approximate zeroes.

```
matdet(M,v) = det(matextract(M,v,v));


computepts(e,pts) =
      alist=[];
      v=[];
      M=mathell(e,pts);
      olddetvalue=.1;
      for(j=1,length(pts),
            detvar=abs(matdet(M,concat(v,j)));
            if(detvalue>olddetvalue,v=concat(v,j);
                                    olddetvalue=detvalue*1.5,));
      [length(v), extract(pts,v)];
```

4.2.2 Code for Computing Mazur's Bound

The code below follows the formula outlined in section 1.3.2. We let *fe* be the elliptic curve and *plist* be the list of primes, p, for which the curve has a point of order p. *mbound* takes these two values as input. *plist* is first ordered and *fe* is replaced by its minimal Weierstrass form. We then factor the minimal discriminant and for each p in *plist*, we compute Mazur's bound relative to p. This is done by *bound2* for the prime 2 and by *bound* for all other primes. *mbound* returns the minimum of all the bounds computed. In the functions *bound* and *bound2* we use the fact that a prime p of bad reduction is additive if and only if $p \mid c_4$.

```
mbound(fe,plist,bnd) =
      plist=set(plist);
      fd=vec(factor(abs(fe[12])));
```

```
    if(plist[1]==2,
        bnd=bound2(fe,2,fd);
        plist=extract(plist,vector(length(plist)-1,j,j+1)),
         bnd=10^10);
    for(j=1,length(plist),bnd=min(bnd,bound(fe,plist[j],fd)));
    bnd;



bound(fe,p,fd,b,a,m) =
    b=length(fd[1]);
    for(j=1,b,
        if(fe[10]%fd[1][j],
            if(fd[2][j]%p,
                if(fd[1][j]%p!=1,m=m+1,),),
                 a=a+1));
    a+b-1-m;

bound2(fe,p,fd,b,a,m,e) =
    b=length(fd[1]);
    for(j=1,b,
        if(fe[10]%fd[1][j],
            if(fd[2][j]%p,
                if(fd[1][j]%p!=1,m=m+1,);
                if(fd[2][j]%4!=1,e=1,),),
             a=a+1));
    a+b-1-m-e;
```

4.2.3 Code for Computing Kretschmer's Bound

In many cases we were not able to find enough linearly independent points on an elliptic curve to come close to the bounds or estimates given by Mazur's bound or the sum $G_E(N)$. In these cases, if the elliptic curve contained a point of order two, we used the descent procedure and Kretschmer's theorem 1.3.1 to compute the Selmer group.

Given an elliptic curve, E, defined by $y^2 = x^3 + a\,x^2 + b\,x$, let E' be the curve defined by $y^2 = x^3 - 2a\,x^2 + (a^2 - 4b)\,x$. Then for points P written as $[x, y, z]$ in $E(\mathbb{Q})$, we have the degree 2 isogeny φ,

$$\varphi : E(\mathbb{Q}) \longrightarrow E'(\mathbb{Q}) \quad \text{by} \quad \varphi(P) = \begin{cases} [y^2, y(x^2 - b), x^2] & \text{if } P \neq [0,1,0], [0,0,1] \\ [0,1,0] & \text{otherwise.} \end{cases}$$

Recall that there is a dual isogeny which we denote φ' which maps E' to E and that the composition of these two maps is multiplication by 2 on the appropriate curve. Furthermore, we have the homomorphism $\alpha : E(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$ defined by

$$\begin{aligned} \alpha([0,1,0]) &= 1, \\ \alpha([0,0,1]) &= b, \quad \text{and} \\ \alpha([x,y,1]) &= x. \end{aligned}$$

A similar map α' from $E'(\mathbb{Q})$ to $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ exists as well. For each divisor, d of b, we have the homogeneous space

$$H_d : z^2 = d\,x^4 + a\,x^2 + \frac{b}{d}.$$

The image of α in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ is precisely the set consisting of 1, b and those d for which H_d has a rational solution (x_0, z_0), $x_0 \neq 0$. (Note that given a point (x_0, z_0) on H_d, we get the point $(d\,x_0^2,\, d\,x_0\,z_0)$ on E.) Kretschmer's theorem 1.3.1 gives us a way to decide if H_d is everywhere locally soluble for a given d and hence a way to compute the Selmer group $S = S^{\varphi}(E/\mathbb{Q})$. The image of α sits inside this Selmer group and similarly, the image of α' sits inside the Selmer group $S' = S^{\varphi'}(E'/\mathbb{Q})$. Since we have the relation:

$$2^{r_E} = \frac{|\alpha(E(\mathbb{Q}))| \cdot |\alpha'(E'(\mathbb{Q}))|}{4},$$

we get an upper bound on the rank of E by computing the two Selmer groups S and S'.

The function *totalpadics* below computes for a curve E, the isogenous curve E' and hands these two curves off to the function *padics*. The function *padics* then computes the homogeneous spaces H_d which are elements of the Selmer group by first checking to see if H_d has a real point, then by checking the conditions given in Kretschmer's theorem. We then use the relation above to give an upper bound on the rank. By searching for points on each the homogeneous spaces returned, we can also provide a lower bound. Note that $|\alpha(E(\mathbb{Q}))|$ and $|\alpha'(E'(\mathbb{Q}))|$ are powers of 2. This allows us to deduce that some of the homogeneous spaces for which we could not find rational points, must have rational points.

```
padics(aa,bb,vfa,vfb,pcheck1,pcheck2,v1j,p1l,p2l,ctr,hss,cb1,cb2,
       gcdb1b2,ctr,fb1,fb2,openps,divb,b1s,kb,sfb1,sfb2)=
      vfb=vec(factor(abs(bb)));
      vfa=vec(factor(abs(aa^2-4*bb)));
      pcheck1=setminus(setminus(vfb[1]~,vfa[1]~),[2,3]);
      pcheck2=[];
      for(j=1,length(vfa[1]),v1j=vfa[1][j];
            if(v1j==2||v1j==3||setsearch(vfb[1]~,v1j),,
                  pcheck2=concat(pcheck2,[[v1j,vfa[2][j]%2]])));
      p1l=length(pcheck1);
      p2l=length(pcheck2);
      openps=[];
      for(j=1,p2l,if(pcheck2[j][2]==1,
          openps=concat(openps,pcheck2[j][1]),
            if(round(((kro(aa,pcheck2[j][1])*pcheck2[j][1])%8)/8),,
                openps=concat(openps,pcheck2[j][1]))));
      divb=divisors(bb);
      b1s=[];
      for(j=1,length(divb),if(issqfree(divb[j]),
            tmpb=[divb[j],bb/divb[j]];
```

```
      if(aa>0,b1s=concat(b1s,[tmpb,-tmpb]),
         if(bb<0,b1s=concat(b1s,[tmpb,-tmpb]),
      b1s=concat(b1s,[tmpb]))),));
hss=[];
for(j=1,length(b1s),
      cb1=b1s[j][1];cb2=b1s[j][2];
      fb1=0;fb2=0;
      ctr=min(length(openps),1);
      while(ctr>0 && ctr<=length(openps),
            kb=kro(cb1,openps[ctr]);
            ctr=ctr*kb+kb);
      if(ctr<0,,
            gcdb1b2=gcd(cb1,cb2);
            ctr=min(p1l,1);
            while(ctr>0 && ctr<=p1l,
              if(gcdb1b2%pcheck1[ctr],ctr=ctr+1,
                 if(kro(aa,pcheck1[ctr])+1,ctr=ctr+1,
                    if(fb1,,fb1=vec(factor(cb1)));
                     sfb1=setsearch(fb1[1]~,pcheck1[ctr]);
                     if(sfb1,sfb1=fb1[2][sfb1]%2,);
                     if(sfb1-1,ctr=ctr+1,
                        if(fb2,,fb2=vec(factor(cb2)));
                           sfb2=setsearch(fb2[1]~,pcheck1[ctr]);
                           if(sfb2,sfb2=fb2[2][sfb2]%2,);
                           if(sfb2-1,ctr=ctr+1,ctr=-1))))));
      if(ctr<0,,
         if(cb2%3==2,if(set([cb1,aa]%3)==[0,2],,
                  hss=concat(hss,cb1*x^4+aa*x^2+cb2)),
                        hss=concat(hss,cb1*x^4+aa*x^2+cb2))));
hss;
```

```
totalpadics(fe,vfe,aa,bb,daa,dbb,ans,rub) =
        aa=vfe[2];
        bb=vfe[3];
        daa=-2*aa;
        dbb=aa^2-4*bb;
        ans1=padics(aa,bb);ans2=padics(daa,dbb);
        ans=[ans1,ans2];
        rub=floor(log(length(ans1)*length(ans2))/log(2)-2);
        [ans,rub];
```

4.2.4 Rank and the Sign of the Functional Equation

We make one final comment regarding the computation of rank. Recall that the Birch, Swinnerton-Dyer conjecture also includes the statement that the L function for an elliptic curve satisfies a functional equation. There is also the conjecture that the sign of this functional equation can be used to predict the parity of the rank. In particular, it is conjectured that

$$(-1)^r = -\prod_{p|\Delta} \varepsilon_p,$$

where the ε_p are the local factors. If p is a prime of multiplicative reduction, then we have that $\varepsilon_p = -(\frac{-c_6}{p})$, where $(\frac{a}{b})$ is the Jacobi symbol. If we compute this product, we may in some cases be able to reduce the possibilities for the rank of a given curve. We carried out this calculation for all curves with no additive reduction and found that if we assume the parity conjecture, we have the following.

1. The curve in section 2.3.2 with torsion subgroup $\mathbb{Z}/4\mathbb{Z}$ has rank 2.

2. The curve in section 3.5.1 with torsion subgroup $\mathbb{Z}/3\mathbb{Z}$ has rank 5 or 7.

4.2.5 Code for Searching for Points

Searching for points on an elliptic curve is perhaps the most speed critical algorithm of those presented here. We implemented this search in the language *gp*, but since this is not a compiled language, our implementation suffers from the deficiencies inherent in an interpreted language. For this reason, we present the algorithm as pseudo-code (which should be implemented in some compiled language such as C).

The pseudo-code below assumes that we are given a curve in the form $y^2 = f(x)$. The algorithm searches for values of x near some base value x_0 which gives $f(x)$ a square. In particular, the x-coordinates are chosen from the set

$$\{\frac{a}{b} \ \epsilon\ \mathbb{Q} \ | \ b_1 \leq b \leq b_2,\ |x_0 - \frac{a}{b}| \leq n\}.$$

In practice, we have n much greater than $b_2 - b_1$ and so we do the following:

```
search(f,b1,b2,x0,n,pts) =
      for b=b1 to b2,
            compute S(b)=the set of least reduced residues for b;
            for each k in S(b),
                  for j=(x0-n-1)  to  (x0+n-1),
                        let a=j*b + k;
                        if f(a/b) is a square, then add the point to pts.
```

4.3 The Polynomial Method and the Quartic Model

4.3.1 Choosing a Polynomial Construction

Throughout Chapter 3, we use theorem 3.2.1 to construct elliptic curves of large rank. We choose to use theorem 3.2.1 as opposed to theorem 3.2.2 for two simple reasons. First, it is easier to search and test for squares than it is to search and test for roots of a cubic. Theorem 3.2.2 would have produced curves of the form $f(x, y) = 0$, where in general $f(x, y)$ is a cubic with both y^3 and x^3 terms appearing. Searching for points on this curve is more difficult than curves of the form $y^2 = f(x)$. Furthermore, the quartic model has the advantage of giving the possibility of two additional points– the points at infinity. This advantage, and hence the extra points, would be lost by using theorem 3.2.2

4.3.2 Code for the Polynomial Construction

The function *mestrep* below, computes the polynomial whose roots are the elements of the vector v passed as argument of the function. This corresponds to what we called $p_A(x)$ in chapter 3. *mestreg* first computes *tay* = the complete Taylor expansion of $\sqrt{p_A(1/x)}$ and then *extracts* the Laurent expansion from this. The resulting polynomial corresponds to $g_A(x)$. Similarly, *mestrer* corresponds to $r_A(x)$. The final function below, *mestrert* is simply the function *mestrer* for the special choice of roots given in section 3.2.2.

```
mestrep(v) = prod(1,j=1,length(v),x-v[j])


mestreg(v,tay) =
      tay=taylor((x^length(v)*subst(mestrep(v),x,1/x)))^(1/2),x);
      poly(extract(vec(tay),vector(length(v)/2+1,j,j)),x)


mestrer(v) = vec(mestreg(v)^2-mestrep(v))


mestrert(v,pts) =
      pts=concat(v+vector(length(v),j,t),v-vector(length(v),j,t));
      [mestrer(pts)/t^2,pts]
```

4.3.3 Code for the Group Law

Throughout this section we let the elliptic curve E be defined by $y^2 = f(x)$, where $f(x)$ is a quartic with lead coefficient a^2. In the code below, *fun* corresponds to this f and *lda* corresponds to this a.

We begin with the code for doubling a point. A parabola that contains the point O' is of the form $y = a\,x^2+\beta\,x+\alpha$. The functions *beta* and *alpha* compute the β and α such that the parabola is also tangent at the point $P = (x_1, y_1)$. This point is represented by *pt=(pt[1],pt[2])* in the code. *yydouble* gives the parabola described above. *qdouble* finds the fourth point of intersection by computing the root of $(f(x) - y^2)/(x - x_1)^2$.

The returned point, $2P$, is then the reflection of this fourth point of intersection across the x-axis.

```
alpha(pt,fun,lda) = lda*pt[1]^2-beta(pt,fun,lda)*pt[1]-pt[2]


beta(pt,fun,lda) = 2*lda*pt[1]-(subst(deriv(fun,x),x,pt[1])/(2*pt[2]))


yydouble(pt,fun,lda)= lda * x^2  -  beta(pt,fun,lda) * x  -  alpha(pt,fun,lda)


qdouble(pt,fun,lda,fyy,yyt,x3) =
      yyt=yydouble(pt,fun,lda);
      fyy=(fun-yyt^2)/(x-pt[1])^2;
      x3=-compo(fyy,1)/compo(fyy,2);
      [x3,-subst(yyt,x,x3)]
```

Similarly, the functions below do the same but with different parabolas. *yyneg* gives the parabola containing P and tangent at O'. The negative of the point P is then given by *qneg*. *yysum* gives the parabola that passes through P_1 and P_2. Note that P_1 and P_2 are such that the x-coordinate of P_1 not equal to the x-coordinate of P_2.

```
yyneg(pt,fun,lda) =
      lda * x^2 +
        compo(fun,4)/(2*lda) * x -
          lda*pt[1]^2 + pt[2] - compo(fun,4)/(2*lda)*pt[1]


qneg(pt,fun,lda,fyy,yyt,x3) =
      yyt=yyneg(pt,fun,lda);
      fyy=(fun-yyt^2)/(x-pt[1]);
      x3=compo(fyy,1)/compo(fyy,2);
      [x3,subst(yyt,x,x3)]
```

```
yysum(pt1,pt2,fun,lda) =
      lda * x^2 +
        ((x1+x2)*(-lda)+(1/(x1-x2)*y1-y2/(x1-x2))) * x +
           (-x2*x1*(-lda)+(-x2/(x1-x2)*y1+y2*x1/(x1-x2)))


qsum(pt1,pt2,fun,lda,fyy,yyt,x3) =
      yyt=yysum(pt1,pt2,fun,lda);
      fyy=(fun-yyt^2)/((x-pt[1])(x-pt[2]));
      x3=compo(fyy,1)/compo(fyy,2);
      [x3,-subst(yyt,x,x3)]
```

4.3.4 Code for Sieving

The functions *sieve* and *sieve2* below search for curves with nontrivial torsion for which the sum $G_E(500)$ is high. The function G computes $G_E(N)$. In the case of the function *sieve* we also look for curves with high Mazur bound. In the case of *sieve2* we look for curves with high Kretschmer bound.

The elliptic curve, *ec*, is assumed to be defined over $\mathbb{Q}(m)$ and *sieve* specializes the curve to values of m with numerator between $n1$ and $n2$ and denominator between $d1$ and $d2$. Known points are passed to the function as *pts* and once a curve is found with high sum ($\geq$ *mingbound*) and high Mazur bound ($\geq$ *minmbound*), the function searches for additional points on the curve. The search for points is done on two different models of the curve and if the rank of the subgroup generated by all found and known points is larger than *rnk* the curve is accepted. We note that the function *rprimevec* simply returns the least reduced residues for a given n.

Similarly, *sieve2* specializes the curve *ec* defined over $\mathbb{Q}(m)$ at many values m and finds curves with large sum and Kretschmer bound. In addition, *sieve2* also does a rudimentary search over the homogeneous spaces found to be everywhere locally soluble. From these points, we find the corresponding points on the elliptic curve and compute a lower bound on the rank as well.

```
sieve(ec,n1,n2,d1,d2,pts,plist,mingbound,minmbound,rnk,
      ptsm,ecm,rdl,rd,mm,ans) =
     for(dz=d1,d2,
          rd=rprimevec(dz);
          for(numctr=n1-1,n2-1,
               for(rr=1,length(rd),
                    mm=(rd[rr]+numctr*dz)/dz;
                    ecm=subst(ec,m,mm);
                    ptsm=subst(pts,m,mm);
                    ecm=[ecm,makeintegral(ecm)];
                    ecm=[ecm[1],ecm[2],laska(ecm[2][1])];
                    ecms=smallinitell(ecm[3][1]);
                    bnds=round(G(ecms,gn));
                    if(bnds>=mingbound,
                          bnds=[bnds,mbound(ecms,plist)];
                          if(bnds[2]>=minmbound,
 ptsm=concat(ptsm,
   search(x^3+ecm[1][2]*x^2+ecm[1][4]*x+ecm[1][5],0,1,100));
 ptsm=chptell(ptsm,ecm[2][2]);
 ptsm=concat(ptsm,
   search(x^3+ecm[2][1][2]*x^2+ecm[2][1][4]*x+ecm[2][1][5],0,1,100));
 ptsm=chptell(ptsm,ecm[3][2]);
 ecms=initell(ecms);
 cps=computepts(ecms,ptsm);
 ptsm=cps[3];
 if(cps[1]>rnk,
       ans=concat(ans,[[ecm[1],ecm[3][1],ptsm,ecm[3][2],bnds,
                    cps[1]]]),),),),))));
     ans;
```

```
sieve2(ec,n1,n2,d1,d2,p1,mingbound,mindbound,rnk,gn,tmp,cps,
       ecm,funecm,rdl,rd,mm,ans,b1,b2,tatesh1,tatesh2,ptsm) =
     ans=[];
     for(dz=d1,d2,
          rd=rprimevec(dz);
          rdl=length(rd);
          for(numctr=n1-1,n2,
               for(rr=1,rdl,
                    mm=(rd[rr]+numctr*dz)/dz;
                    ecm=subst(ec,m,mm);
                    ptsm=[subst(p1,m,mm)];
                    ecm=[ecm,prelaska(ecm)];
                    ecm=concat(ecm,[laska(ecm[2][1])]);
                    ecm=[ecm[1],ecm[2],[initell(ecm[3][1]),ecm[3][2]]];
                    ptsm=chptell(ptsm,ecm[2][2]);
                    funecm=x^3+ecm[2][1][2]*x^2+ecm[2][1][4]*x;
                    bnds=round(G(ecm[3][1],gn));
                    if(bnds>=mingbound,
                          bnds=[bnds,totalpadics(funecm)];
                          if(bnds[2][2]>=mindbound,
 if(min(bnds[1],bnds[2][2])>=rnk,
b1=0;tatesh1=[];
 for(j=1,length(bnds[2][1][1]),
  tmp=hssearch(bnds[2][1][1][j],5001,4999,1,1);
  if(length(tmp),b1=b1+1;
                  b2=compo(bnds[2][1][1][j],5);
                  ptsm=concat(ptsm,[[b2*tmp[1][1]^2,b2*tmp[1][2]*tmp[1][1]]]),
       tatesh1=concat(tatesh1,bnds[2][1][1][j])));
b2=0;tatesh2=[];
 for(j=1,length(bnds[2][1][2]),
```

```
  tmp=hssearch(bnds[2][1][2][j],5001,4999,1,1);
  if(length(tmp),b2=b2+1,tatesh2=concat(tatesh2,bnds[2][1][2][j])));
b1=(ceil(log(max(b1,1))/log(2))+ceil(log(max(b2,1))/log(2))-2;
cps=computepts2(ecm[3][1],chptell(ptsm,ecm[3][2]));
b1=max(b1,cps[1]);
   ans=concat(ans,[[b1,mm,cps[3],cps[2],
                   [tatesh1,tatesh2],
                   [length(bnds[2][1][1]),length(bnds[2][1][2])],
                   vector(5,j,ecm[2][1][j]),
                   bnds[1],bnds[2][2]]]),),),))));
     ans;


G(ecms,N) =
     1/(log(prime(N))-2)*sum(0.,j=1,N,
        log(prime(j))*(1-(prime(j)-1)/(prime(j)+1-apell(ecms,prime(j)))));


rprimevec(n,ans) =
     ans=[1];
     if(n<101,ans=primevec[n],
     for(j=2,n-1,if(gcd(j,n)==1,ans=concat(ans,j),)));
     ans;
```

4.4 The Finite Field Method

4.4.1 Two Types of Tate Normal Forms

There are essentially two categories of Tate normal forms we consider– ones parameterized by one variable and ones parameterized by two variables. Elliptic curves that contain a point of order three are parameterized by two variables and elliptic curves that contain a point of order 4 are parameterized by two variables. The algorithm for searching for these curves follows the outline given in section 2.1.1.

In each case, the algorithm computes a list of curves defined over $\mathbb{F}_p$ in Tate normal form which maximize the number of points on the curve in $\mathbb{F}_p$. The routine *mchinese* then computes a list of curves in Tate normal form modulo the product of every prime used in the previous step. This list of curves has the property that each curve reduced modulo p gives a curve with maximal $\#E_p$. This list of curves is then passed on to the sieving routines. The sieving routines used are analagous to those described in section 4.3.4. The only distinction is that here we are sieving over lifts of the curves in the list given by *mchinese* rather than sieving over curves parameterized by some subset of the rationals.

4.4.2 Finding Curves with Points of Order 3

```
prepv(v) = [0,v[1]^2,0,v[1]*8*v[3],16*v[3]^2];


funell(v) = x^3+v[2]*x^2+v[4]*x+v[5];


gform(a1,a3)=[a1,0,a3,0,0];


gform2(a1,a3,ec) =
      ec=gform(a1,a3);
      if(smallinitell(ec)[12]==0,[a1,a3,0],
            [a1,a3,smallinitell(laska(ec)[1])]);


mx(n,p)=if(n==0,,p=prime(n));
      matrix(p,p-1,a1index,a3index,gform2(a1index-1,a3index));


precurves(n,mxn,apj,pj,mxn133,maxpj,goodcurves,allgoodcurves) =
      allgoodcurves=[[2,1,[[mod(1,2),mod(1,2)]]]];
      for(j=2,n,
            pj=prime(j);
            maxpj=-ceil(2*sqrt(pj));
```

```
            goodcurves=[];
            for(a1i=1,pj,for(a3i=1,floor(pj/2),
                  mxn133=mxn[a1i,a3i][3];
                  if(mxn133==0,,
                  apj=-apell(mxn[a1i,a3i][3],pj);
                  if(apj>=maxpj,if(apj>maxpj,
   goodcurves=[mod([a1i-1,-a3i],pj),mod([a1i-1,a3i],pj)];
   maxpj=apj,
      goodcurves=concat(goodcurves,
          [mod([a1i-1,-a3i],pj),mod([a1i-1,a3i],pj)])),))));
                  allgoodcurves=concat(allgoodcurves,
                        [[pj,floor(2*sqrt(pj))-maxpj,goodcurves]]));
      allgoodcurves;

curves(n) = precurves(n,mx(n));



subchinese(clist,n,k,cval,ckl,ck) =
      k=k+1;
      ckl=clist[k][3];
      ck=length(ckl);
if(k<n,for(j=1,ck,subchinese(clist,n,k,
           [chinese(cval[1],ckl[j][1]),chinese(cval[2],ckl[j][2])])),
   for(j=1,ck,anslist=concat(anslist,[[chinese(cval[1],ckl[j][1]),
                              chinese(cval[2],ckl[j][2])]])));

mchinese(clist,anslist,n) =
      if(anslist,,anslist=[]);
      n=length(clist);
      for(j=1,length(clist[1][3]),
```

```
        subchinese(clist,n,1,[clist[1][3][j][1],clist[1][3][j][2]]));
    anslist;
```

4.4.3 Finding Curves with Points of Order 4

```
prepv(v) = [0,-8*v[2]+1,0,16*v[2]^2,0];

funell(v) = x^3+v[2]*x^2+v[4]*x+v[5];

gform(c) = [1,c,c,0,0];

gform2(c,ec) =
    ec=gform(c);
    if(smallinitell(ec)[12]==0,[c,0],
        [c,smallinitell(laska(ec)[1])]);

t4(c,ec) =
    ec=smallinitell([1,c,c,0,0]);
    if(ec[12]==0,[c,0],[c,smallinitell(laska(ec)[1])]);

vctr(n,p) =
    if(n==0,,p=prime(n));
    vector(p,j,t4(j));

curves4(n,vctrn,apj,pj,vctrn2,maxpj,goodcurves,allgoodcurves) =
    if(vctrn,,vctrn=vctr(n));
    allgoodcurves=[];
    for(j=1,n,
        pj=prime(j);
        maxpj=-ceil(2*sqrt(pj));
```

```
            goodcurves=[];
            for(cj=1,pj-1,
                  vctrn2=vctrn[cj][2];
                  if(vctrn2==0,,
                  apj=-apell(vctrn2,pj);
                  if(apj>=maxpj,if(apj>maxpj,
                  goodcurves=[mod(cj,pj)];maxpj=apj,
                  goodcurves=concat(goodcurves,[mod(cj,pj)])),)));
            allgoodcurves=concat(allgoodcurves,
[[pj,floor(2*sqrt(pj))-maxpj,goodcurves]]));
      allgoodcurves;

subchinese4(clist,n,k,cval,ckl,ck) =
      k=k+1;
      ckl=clist[k][3];
      ck=length(ckl);
if(k<n,for(j=1,ck,subchinese4(clist,n,k,
            chinese(cval,ckl[j]))),
      for(j=1,ck,anslist=concat(anslist,chinese(cval,ckl[j]))));

mchinese(clist,anslist,n) =
      if(anslist,,anslist=[]);
      n=length(clist);
      for(j=1,length(clist[1][3]),
            subchinese4(clist,n,1,clist[1][3][j]));
      anslist;
```

References

[1] Henri Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, 1995.

[2] Stefane Férmigier. Un exemple de courbe elliptique définie sur Q de rang ≥ 19. *C. R. Acad. Sci. Paris*, 315, Série I(6):719 – 722, 1992.

[3] Stefane Férmigier. Exemples de courbe elliptiques de grand rang sur $Q(t)$ et sur Q possédant des points d'ordre 2. *C. R. Acad. Sci. Paris*, 322, Série I(10):949 – 952, 1996.

[4] Stefane Férmigier. Une courbe elliptique définie sur Q de rang ≥ 22. *Acta Arithmetica*, LXXXII(4):359 – 363, 1997.

[5] Dale Husemöller. *Elliptic Curves.* Springer-Verlag, 1987.

[6] Shoichi Kihara. Construction of high-rank elliptic curves with a non-trivial rational point of order 2. *Proc. Japan Acad.*, 73, Series A(9):165, 1997.

[7] Shoichi Kihara. On an infinite family of elliptic curves with rank ≥ 14 over Q. *Proc. Japan Acad.*, 73, Series A(2):32, 1997.

[8] Shoichi Kihara. On the rank of elliptic curves with three rational points of order 2. *Proc. Japan Acad.*, 73, Series A(5):77 – 78, 1997.

[9] Shoichi Kihara. On the rank of elliptic curves with three rational points of order 2. ii. *Proc. Japan Acad.*, 73, Series A(8):151, 1997.

[10] Anthony W. Knapp. *Elliptic Curves.* Princeton University Press, 1992.

[11] Thomas J. Kretschmer. Construction of elliptic curves with large rank. *Mathematics of Computation*, 46(174):627 – 635, 1986.

[12] Michael Laska. An algorithm for finding a minimal weierstrass equation for an elliptic curve. *Mathematics of Computation*, 38(157):257 – 260, 1982.

[13] Jean-François Mestre. Construction d'une courbe elliptique de rang ≥ 12. *C. R. Acad. Sci. Paris*, 295, Série I(12):643 – 644, 1982.

[14] Jean-François Mestre. Courbes elliptiques de rang ≥ 11 sur $Q(t)$. *C. R. Acad. Sci. Paris*, 313, Série I(3):139 – 142, 1991.

[15] Jean-François Mestre. Courbes elliptiques de rang ≥ 12 sur $Q(t)$. *C. R. Acad. Sci. Paris*, 313, Série I(4):171 – 174, 1991.

[16] Jean-François Mestre. Un exemple de courbe elliptique sur Q de rang ≥ 15. *C. R. Acad. Sci. Paris*, 314, Série I(6):453 – 455, 1992.

[17] L. J. Mordell. *Diophantine Equations.* Academic Press, 1969.

[18] Koh-Ichi Nagao. An example of ellipitic curve over Q with rank ≥ 20. *Proc. Japan Acad.*, 69, Series A(8):291 – 293, 1993.

[19] Koh-Ichi Nagao. An example of ellipitic curve over $Q(t)$ with rank ≥ 13. *Proc. Japan Acad.*, 70, Series A(5):152 – 153, 1994.

[20] Koh-Ichi Nagao. Construction of high-rank elliptic curves with a nontrivial torsion point. *Math. Comp.*, 66(217):411 – 415, 1997.

[21] Koh-Ichi Nagao. Examples of ellipitic curves over Q with rank ≥ 17. *Proc. Japan Acad.*, 68, Series A(9):287 – 289, 1997.

[22] Koh-Ichi Nagao. $Q(t)$-rank of elliptic curves and certain limit coming from the local points. *Manuscripta Math.*, 92(1):13 – 32, 1997.

[23] Koh-Ichi Nagao and Tomonori Kouya. An example of ellipitic curve over Q with rank ≥ 21. *Proc. Japan Acad.*, 70, Series A(4):104 – 105, 1994.

[24] Joseph Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1986.

[25] Joseph Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer-Verlag, 1994.

[26] Jaap Top. Descent by 3-isogeny and 3-rank of quadratic fields. In *Advances in Number Theory*, pages 303 – 317. Oxford Science Publications, Oxford Univ. Press, 1993.

[27] Jacobus H. van Lint and Gerard van der Geer. *Introduction to coding theory and algebraic geometry.* Birkhäuser, 1988.