ABSTRACT

Title of Dissertation: RATIONAL POINTS ON SOME FAMILIES OF ELLIPTIC CURVES

Edward Vincent Eikenberg, Doctor of Philosophy, 2004

Dissertation directed by: Professor Lawrence C. Washington
Department of Mathematics

Let E_m be the family of elliptic curves given by y^2=x^3-x+m^2, which has rank 2 when regarded as an elliptic curve over Q(m). (Here Q represents the field of rational numbers.) Brown and Myers show that a certain quadratic polynomial m(t) has the property that E_m(t) contains an additional rational point that is independent from the two original generators. This implies that there are infinitely many rational numbers n such that E_n(Q) has rank at least 3. We generalize this result, showing that every nonzero rational number n has the property that E_n sits inside such a subfamily of rank 3. Moreover, given any rational point P in E_n, there exists a quadratic polynomial m(t) and a Q(t)-point R(t) in E_m(t) that is independent from the original generators, such that the specialization to t=0 gives m(0)=n and R(0)=P. Such subfamilies can be intersected to increase the rank, demonstrating the existence of a rational

subfamily of rank 4 over Q(t), and infinitely many rational numbers n such that E_n(Q) has rank at least 5. Shioda's theory of Mordell-Weil lattices is used to find the generators of such E_m(t) over both Qbar(t) and Q(t) in these cases. (Here Qbar represents the algebraic closure of Q.) All quadratic polynomials m(t) are classified by whether or not E_m(t) contains an additional rational point of low degree. Results similar to these are also obtained for other families of elliptic curves.

# RATIONAL POINTS ON SOME FAMILIES OF ELLIPTIC CURVES

by

Edward Vincent Eikenberg

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2004

Advisory Committee:

Professor Lawrence C. Washington, Chairman/Advisor
Professor William Adams
Professor William Gasarch
Professor Niranjan Ramachandran
Professor James Schafer

# DEDICATION

To my parents: Thank you for all the love and support that you have given me. You made this possible.

# ACKNOWLEDGEMENTS

A project of this magnitude could not have been completed without help from many different people. Of course the most significant contribution came from my advisor Larry Washington in the form of advice and guidance on this project. Bud Brown is responsible for giving me a fresh outlook and planting the seed for this project. Invaluable guidance and support also came from Jim Schatz, Moss Sweedler, Charlie Toll and Jacquie Holmgren. Thank you all so much for your help. Also, this would not have been possible without the constant support of my parents, family, and friends.

TABLE OF CONTENTS

# LIST OF TABLES

# Chapter 1: Introduction

## 1.1 History

Elliptic curves are among the most fascinating and widely studied objects in modern mathematics. The first recorded appearance of an elliptic curve traces back to Diophantus in his book "Arithmetica," where he was looking for points on the elliptic curve (in a slightly different form):

$$y^2 = x^3 - x + 9.$$

Using the modern theory of elliptic curves, it is straightforward to show that the group of rational points on this curve has rank 2 and trivial torsion subgroup, generated by the points $(0, 3)$ and $(1, 3)$. This curve sits inside the family $E_m$ of elliptic curves given by

$$E_m : y^2 = x^3 - x + m^2. \tag{1.1}$$

This relatively simple equation has some obvious solutions for every value of $m$, including $P = (0, m)$ and $Q = (1, m)$. Viewing $E_m$ as an elliptic curve defined over the function field $\overline{\mathbb{Q}}(m)$, these become points in the group $E_m\big(\overline{\mathbb{Q}}(m)\big)$. Since $E_m$ is a rational elliptic surface, [Shi3] implies that the points $P$ and $Q$ generate $E_m\big(\overline{\mathbb{Q}}(m)\big)$ (see Theorem 2.4.1). In fact, since the generators are both contained in $\mathbb{Q}(m)$, it follows that $P$ and $Q$ generate $E_m(\mathbb{Q}(m))$.

Table 1.1: Classification of $E_m$ by Rank for $m = 1, \ldots, 500$

| Rank | First few $m$ where $E_m$ has this rank | $\#m \leq 500$ |
|---|---|---|
| 1 | 1 | 1 |
| 2 | 2, 3, 4, 6, 9, 10, 18, 21, 26, 30, ... | 125 |
| 3 | 5, 7, 8, 11, 12, 13, 14, 15, 16, 17, ... | 240 |
| 4 | 24, 25, 27, 31, 36, 41, 46, 58, 61, 63, ... | 112 |
| 5 | 113, 127, 163, 176, 181, 209, 215, 245, 283, 317, ... | 21 |
| 6 | 337, ... | 1 |

Brown and Myers [BM] also study this family of elliptic curves, noting that for many integer values of $m$, the rank of $E_m(\mathbb{Q})$ is often much higher than 2. For example, $m = 765617$ gives an elliptic curve of rank at least 10. Table 1.1 lists some small positive integer values of $m$ by the corresponding rank of $E_m(\mathbb{Q})$, as well as a count of how many integers $m$ from 1 to 500 have $E_m(\mathbb{Q})$ of a given rank. See Appendix A for more details. Since the rank of $E_m\big(\mathbb{Q}(m)\big)$ is 2, one would expect that the rank of $E_{m_0}(\mathbb{Q})$ would be 2 or 3 for most values of $m_0 \in \mathbb{Q}$. Note the surprisingly large number of rank 4 curves here.

In addition, Brown and Myers prove that there are infinitely many values of $m$ such that $E_m(\mathbb{Q})$ has rank at least 3. More specifically, if $m(t) = 54t^2 - 165t - 90$, then the subfamily $E_{m(t)}(\mathbb{Q}(t))$ contains the additional point $R = (36t + 17, 54t^2 + 267t + 114)$, which is independent from $P$ and $Q$ for all but finitely many values of $t \in \mathbb{Q}$. This can be viewed as a "lift" of the point $(17, 114) \in E_{90}(\mathbb{Q})$, as this is the point obtained when specializing to $t = 0$. (Note that the curves $E_{-90}$ and $E_{90}$ are the same.)

## 1.2 Summary of Primary Results

Chapter 3 of this paper generalizes the above result of Brown and Myers. A general criterion for lifting points on $E_m$ is presented (see Theorem 3.4.1). In particular,

THEOREM **1.2.1.** *For any $m_0 \in \mathbb{Q}$ with $m_0 \neq 0$ and any point $(p, q) \in E_{m_0}(\mathbb{Q})$, there exists a quadratic polynomial $m(t)$ with $m(0) = m_0$ and a point $R(t)$ with $R(0) = (p, q)$ such that $P = (0, m(t))$, $Q = (1, m(t))$ and $R(t)$ are independent points in $E_{m(t)}(\mathbb{Q}(t))$.*

This implies that for every rational $m_0 \neq 0$, the curve $E_{m_0}$ is a member of a quadratic subfamily which has rank 3, even if $E_{m_0}(\mathbb{Q})$ has rank less than 3. For example, the curve $E_1$, which only has rank 1, is contained in such a family. If $m_1(t) = t^2 - 3t + 1$, then the points

$$P = (0, m_1(t))$$

$$Q = (1, m_1(t))$$

$$R(t) = (2t - 1, t^2 + t - 1)$$

are independent in the group $E_{m_1(t)}(\mathbb{Q}(t))$, despite the fact that specializing to $t = 0$ gives the curve $E_1$ of rank 1. Here, $R(t)$ is a lift of the point $R(0) = (-1, -1)$ on the curve $E_1$.

The ideal use of Theorem 1.2.1 would be to apply this simultaneously to several different points on $E_m(\mathbb{Q})$ which are known to be independent. If the resulting lifts $m_i(t)$ are all the same, then $E_{m_i(t)}(\mathbb{Q}(t))$ would have high rank. However, this does not seem to be the case in practice. The next best thing is to set these $m_i(t)$ equal to each other and find the intersection. The intersection of

two quadratic functions is a conic section, and all rational solutions can be parameterized by a rational function. The intersection of three quadratic functions is actually an elliptic curve [W, pp. 39-41]. If this curve has positive rank, then there are infinitely many points in the intersection. Using this process we get the following results:

THEOREM **1.2.2.** *There exists a rational function $m(t) \in \mathbb{Q}(t)$ such that the group $E_{m(t)}(\mathbb{Q}(t))$ has rank at least 4.*

THEOREM **1.2.3.** *There exist infinitely many values of $m \in \mathbb{Q}$ such that $E_m(\mathbb{Q})$ has rank at least 5. These $m$ can be parameterized by points on an elliptic curve with positive rank.*

For the most part, the results in this paper deal with rational elliptic surfaces (see Chapter 2). Oguiso and Shioda [OS] have classified rational elliptic surfaces over an algebraically closed field by the type of lattice associated to the Mordell–Weil group. For example, the following is a corollary of their work.

THEOREM **1.2.4.** *If $m(t) \in \mathbb{Q}[t]$ is a quadratic polynomial, then $E_{m(t)}\big(\overline{\mathbb{Q}}(t)\big)$ has rank 6.*

This only gives an upper bound on the rank over $\mathbb{Q}(t)$. In Chapter 4, quadratic subfamilies of $E_m$ that contain additional rational generators are found, thus giving higher rank over $\mathbb{Q}(t)$.

THEOREM **1.2.5.** *Let $m(t) \in \mathbb{Q}[t]$ be a quadratic polynomial, and suppose that a linear shift of $t$ can change $m(t)$ into one of the following for some $c \in \mathbb{Q}$:*

$$m_1(t) = ct^2 - \frac{64c^4 + 1}{64c^3}$$

$$m_2(t) = ct^2 - \frac{16c^4 - 24c^2 + 1}{64c^3}$$

$$m_3(t) = ct^2 - \frac{16c^4 + 24c^2 + 1}{64c^3}$$

*Then $E_{m(t)}(\mathbb{Q}(t))$ has rank 3.*

Explicit generators over $\overline{\mathbb{Q}}(t)$ are given for this group, where three of the independent generators are defined over $\mathbb{Q}(t)$ and the other three lie over a finite extension $K(t)$. We use this to deduce that the rank of $E_{m(t)}\mathbb{Q}(t)$ is exactly 3 in these cases. On the other hand, if $m(t)$ does not fit the criteria of Theorem 1.2.5, then we conjecture that there should be only 2 independent rational generators.

CONJECTURE **1.2.6.** *Let $m(t) \in \mathbb{Q}[t]$ be a quadratic polynomial. Then the rank of $E_{m(t)}(\mathbb{Q}(t))$ is either 2 or 3. The rank is 3 if and only if $m(t)$ meets the criteria of Theorem 1.2.5.*

In addition, cubic subfamilies of $E_m$ are examined, as these are still rational elliptic surfaces. Criteria for generating cubic subfamilies of rank at least 3 are given in Section 4.4.

## 1.3 Additional Results

The process of lifting points is not restricted to the family $E_m$. Let $C_m$ be the family of elliptic curves given by

$$C_m : y^2 = x^3 - m^2x + 1$$

Then $C_m(\mathbb{Q}(m))$ has rank 3 generated by the points $(0, 1)$, $(m, 1)$ and $(-1, m)$. The lifting process for a specific point like $(12, 31) \in C_8(\mathbb{Q})$ works in exactly the same manner as it did for $E_m$. However, the computations to perform this lift in general (like Theorem 1.2.1 for $E_m$) are too large for `Pari` to handle.

CONJECTURE **1.3.1.** *Let $m_0 \in \mathbb{Q}$ with $m_0 \neq 0$ and let $(p,q) \in C_m(\mathbb{Q})$. Then there exists a quadratic polynomial $M(t)$ such that $M(0) = m_0$, and a point $R(t) \in C_{M(t)}(\mathbb{Q}(t))$ such that $R(0) = (p,q)$, where the points $P_1 = (0,1)$, $P_2 = (M(t),1)$, $P_3 = (-1,M(t))$ and $R(t)$ are independent in the group $C_{M(t)}(\mathbb{Q}(t))$.*

Even though the above conjecture could not be resolved, we are able to lift specific points. Thus lifts of several points on the same curve can be intersected to generate a subfamily of higher rank.

THEOREM **1.3.2.** *There exists a rational function $m(t) \in \mathbb{Q}(t)$ such that the group $C_{m(t)}(\mathbb{Q}(t))$ has rank at least 5.*

THEOREM **1.3.3.** *There exist infinitely many values of $m \in \mathbb{Q}$ such that $C_m(\mathbb{Q})$ has rank at least 6. These $m$ can be parameterized by points on an elliptic curve with positive rank.*

In Chapter 6, a lift on the curve $D_m : y^2 = x^3 - m^2x + m^2$ is examined. This family of curves provides a unique result, as one specific lift actually increases the rank by 2. We have the following:

THEOREM **1.3.4.** *The Mordell–Weil group $D_m\big(\overline{\mathbb{Q}}(m)\big)$ has rank 2 with trivial torsion subgroup, generated by the points $P = (m,m)$ and $Q = (0,m)$.*

THEOREM **1.3.5.** *There exists a quadratic polynomial $m(t)$ such that $D_{m(t)}(\mathbb{Q}(t))$ contains four independent points. Two of these points can be chosen as lifts of the point $(-7,35) \in D_{14}(\mathbb{Q})$. In particular, these points generate a subgroup of finite index in $D_{m(t)}(\mathbb{Q}(t))$.*

This result gives a *double lift* of the point $(-7,35)$. The results for $E_m$ and $C_m$ above only increase the rank by 1, whereas this increases the rank by 2.

# Chapter 2: Background Material

## 2.1 The Canonical Height Pairing

Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Then the canonical height of a point $P \in E(\mathbb{Q})$ is defined as

$$\hat{h}(P) = \frac{1}{2} \lim_{n \to \infty} \frac{1}{4^n} h_x([2^n]P)$$

where $h_x$ is the logarithmic height of the $x$-coordinate. Among the properties of this height function are

- $\hat{h}(P) \geq 0$ for any $P \in E(\mathbb{Q})$, and $\hat{h}(P) = 0$ if and only if $P \in E(\mathbb{Q})_{tors}$.
- $\hat{h}(kP) = k^2 \hat{h}(P)$ for any $k \in \mathbb{Z}$ and any $P \in E(\mathbb{Q})$.
- $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$ for any $P, Q \in E(\mathbb{Q})$.
- For any constant $c$, the number of points $P \in E(\mathbb{Q})$ such that $\hat{h}(P) < c$ is finite.

In addition, the canonical height gives a bilinear pairing on $E(\mathbb{Q})$ called the *canonical height pairing* (or Néron–Tate height pairing):

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

This height pairing can be used to determine whether or not a set of points in $E(\mathbb{Q})$ are independent.

THEOREM **2.1.1.** *Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and $P_1, \ldots, P_n \in E(\mathbb{Q})$. Then these points are independent if the $n \times n$ determinant*

$$det\big(\langle P_i, P_j \rangle\big) \neq 0.$$

PROOF: Suppose that the points are dependent, so there exists a relation of the form $a_1P_1 + \cdots + a_nP_n = \infty$ where the $a_i \in \mathbb{Z}$ are not all 0. Without loss of generality, suppose that $a_1 \neq 0$. Since the height pairing is bilinear, $a_1$ times the first row can be written as a linear combination of the other rows, making the determinant be 0. ■

The matrix $\big(\langle P_i, P_j \rangle\big)$ is referred to as the height matrix. This result is used freely throughout the paper.

## 2.2 Elliptic Surfaces

Let $k$ be an algebraically closed field, let $C$ be a smooth projective curve defined over $k$, and let $K = k(C)$ be the function field of $C$. An elliptic surface $S$ over the curve $C$ is a smooth projective surface along with a morphism $f : S \to C$ which has the following properties:

1. almost all fibers $F_v = f^{-1}(v)$ are elliptic curves,
2. no fiber contains an exceptional curve with self intersection number $-1$,
3. $f$ has a global section $O : C \to S$ called the zero section, and
4. at least one fiber of $f$ is singular.

Property 2 is a minimality condition, and property 4 implies that the discriminant is non-constant. The section $O$ corresponds to the point at infinity on each fiber.

Given irreducible curves $\Gamma_1$ and $\Gamma_2$ on $S$ which intersect transversally, we define $\Gamma_1 \cdot \Gamma_2$ to be the number of points where $\Gamma_1$ and $\Gamma_2$ intersect. This definition can be extended to the entire group $\mathrm{Div}(S)$ of divisors on $S$ by the following:

THEOREM **2.2.1.** [Sil2, p. 233], [H, p. 367] *There is a unique symmetric bilinear pairing*

$$\mathrm{Div}(S) \times \mathrm{Div}(S) \longrightarrow \mathbb{Z}, \qquad (D_1, D_2) \longmapsto D_1 \cdot D_2,$$

*with the following two properties:*

*(i) If $\Gamma_1$ and $\Gamma_2$ are irreducible curves on $S$ that meet everywhere transversally, then $\Gamma_1 \cdot \Gamma_2 = \#(\Gamma_1 \cap \Gamma_2)$.*

*(ii) If $D$, $D_1$, $D_2 \in \mathrm{Div}(S)$ are divisors with $D_1 \sim D_2$, then $D \cdot D_1 = D \cdot D_2$. (Here $\sim$ represents algebraic equivalence of divisors).*

The Néron-Severi group $NS(S)$ is defined as the group of divisors on $S$ modulo algebraic equivalence. This is a finitely generated group. By property $(ii)$ above, the intersection pairing on $\mathrm{Div}(S)$ is well-defined on $NS(S)$. Thus $NS(S)$ has the structure of a finite dimensional lattice.

The elliptic surface $S$ can be viewed as an elliptic curve $E$ over $K = k(C)$ with identity element $O$. A point $P \in E(K)$ corresponds to a section $\sigma_P : C \to S$. We use the notation $(P)$ to refer to the divisor class of the section $\sigma_P$. To simplify the notation for the pairing defined in Theorem 2.2.1, we use $(PQ)$ to mean $\big((P) \cdot (Q)\big)$ for any points $P, Q \in E(K)$ and similar notation for any fibers $F_v$.

LEMMA **2.2.2.** *Let $P \in E(K)$ and let $F_v$ be any fiber of $f : S \to C$. Then we have*

*(a)* $(PF_v) = (OF_v) = 1$

*(b)* $(F_vF_{v'}) = ({F_v}^2) = 0.$

PROOF: It is fairly obvious that any fiber $F_v$ intersects a section in a unique point by evaluating the section at $v$. This proves $(a)$. If $v \neq v'$ in $C$, then clearly $F_v$ and $F_{v'}$ are disjoint. Also, since all fibers are algebraically equivalent, $(F_vF_{v'}) = ({F_v}^2)$, which completes the proof. ■

Part $(a)$ of this Lemma implies that for any $P \in E(K)$, the divisor $(P) - (O)$ is orthogonal to any fiber $F_v$. However, some fibers may be reducible, and there may be fibral divisors which are not orthogonal to $(P) - (O)$. Let $R = \{v \in C \mid F_v \text{ is reducible}\}$, and for each $v \in R$ let

$$F_v = f^{-1}(v) = \Theta_{v,0} + \sum_{i=1}^{m_v - 1} \mu_{v,i}\Theta_{v,i} \tag{2.1}$$

where $m_v$ is the number of irreducible components of $F_v$, $\Theta_{v,0}$ is the unique irreducible component which intersects the zero section $O$, and $\Theta_{v,i}$ are the remaining irreducible components for $1 \leq i \leq m_v - 1$.

Given a point $P \in E(K)$, there exists a fibral divisor $\Phi_P \in \mathrm{Div}(S) \otimes \mathbb{Q}$ such that the divisor

$$D_P = (P) - (O) + \Phi_P \tag{2.2}$$

satisfies $D_P \cdot F = 0$ for all fibral divisors $F \in \mathrm{Div}(S)$ [Sil2, p. 240]. This allows for the definition of a pairing on $E(K)$, which gives $E(K)/E(K)_{tor}$ the structure of a positive-definite lattice.

THEOREM **2.2.3 (Manin).** *The pairing*

$$\langle \cdot\,, \cdot \rangle : E(K) \times E(K) \longrightarrow \mathbb{Q} \qquad \langle P, Q \rangle = -D_P \cdot D_Q.$$

*has the following two properties:*

*(a)* $\langle \cdot\,, \cdot \rangle$ *is bilinear.*

*(b)* $\langle P, P\rangle = h(P) + O(1)$ *for all* $P \in E(K)$*, where* $h(P) = h(x_P)$ *is the degree of the map* $x_P : C \to \mathbb{P}^1$*.*

*In addition, this pairing agrees with the canonical height pairing, so for all* $P \in E(K)$ *we have* $\hat{h}(P) = \frac{1}{2}\langle P, P\rangle \in \mathbb{Q}$*.*

Let $T$ be the sublattice of $NS(S)$ generated by $(O)$, any fiber $(F)$, and $\Theta_{v,i}$ for all $v \in R$ and $1 \leq i \leq m_v - 1$. The rank of $T$ is given by

$$rk(T) = 2 + \sum_{v \in R}(m_v - 1). \tag{2.3}$$

The map

$$\phi : E(K) \longrightarrow NS(S)/T \qquad P \longmapsto (P) \bmod T \tag{2.4}$$

is an isomorphism. Thus if the rank of $NS(S)$ is known, the structure of reducible fibers $F_v$ determines the rank of $E(K)$.

## 2.3 Rational Elliptic Surfaces

For the purposes of this paper, we are mostly concerned with the case where $S$ is a rational elliptic surface, so we take $k = \overline{\mathbb{Q}}$ and $C = \mathbb{P}^1$, which makes $K = \overline{\mathbb{Q}}(t)$. Equivalently, the associated elliptic curve $E(K)$ can be put in short Weierstrass normal form:

$$y^2 = x^3 + a(t)x + b(t),$$

where $deg(a) \leq 4$ and $deg(b) \leq 6$, and the discriminant $\Delta \notin \overline{\mathbb{Q}}$. In this form, the section $O$ corresponds to the point $\infty \in E(K)$. Now the Néron-Severi group

$NS(S)$ is unimodular and has rank 10. Together with (2.3) and (2.4) above, this implies that

$$\begin{aligned} rk(E(K)) &= rk(NS(S)) - rk(T) \\ &= 8 - \sum_{v \in R} (m_v - 1). \end{aligned} \tag{2.5}$$

All rational elliptic surfaces can now be classified according to the lattice structure of $E(K)$, which depends on the structure of the singular fibers. This classification is carried out in [OS]. Shioda [Shi2] shows that $NS(S)/\langle (O), (F) \rangle \simeq E_8$ and that all possible lattices that occur are sublattices of $E_8$. In particular, the largest possible rank for $E(K)$ is 8, and this only occurs when all singular fibers of $S$ have Kodaira type $I_1$, indicating that they have only one irreducible component. We state what happens in the $E_8$ case explicitly.

THEOREM **2.3.1.** *If $S$ is a rational elliptic surface where all singular fibers have only one irreducible component, then the Mordell–Weil lattice of the associated elliptic curve $E(K)$ is of type $E_8$. This lattice has rank 8, and there are 240 vectors of minimal norm 2 which generate the lattice. These correspond to 240 points $(x(t), y(t)) \in E(K)$ where $deg(x) \leq 2$ and $deg(y) \leq 3$, and these points generate the group $E(K)$.*

SKETCH OF PROOF: From (2.5), if all singular fibers of $S$ have only one irreducible component, then $rk(E(K)) = 8$. In this case, $T = \langle (O), (F) \rangle$ and $E(K) \simeq NS(S)/T \simeq E_8$.

Since all fibers of $S$ have only one irreducible component, we can take

$$D_P = (P) - (O) \qquad \text{and} \qquad \Phi_P = 0.$$

by Lemma 2.2.2. This gives

$$\begin{aligned}\langle P, P\rangle &= -(D_P \cdot D_P) \\ &= -\big((P) - (O)\big) \cdot \big((P) - (O)\big) \\ &= -(PP) - (OO) + 2(PO) \\ &= 2 + 2(PO).\end{aligned}$$

Here we have used the fact that $(PP) = -\chi$, where $\chi$ is the arithmetic genus of $S$. In the case where $S$ is a rational elliptic surface, we have $\chi = 1$. Thus $\langle P, P\rangle$ is a positive even integer for all $P \in E(K)$, which corresponds to the fact that $E_8$ is a positive-definite even unimodular lattice.

It is well known [CS, pp. 120-121] that $E_8$ has 240 minimal vectors of length 2. These minimal vectors are the points in $E(K)$ with minimal norm. Suppose that $P = (x(t), y(t)) \in E(K)$ has minimal norm 2. Then $(PO) = 0$, so $P = (x(t), y(t))$ cannot intersect the $O$ section for any $t \in \mathbb{P}^1$. Using the fact that the $O$ section is "at infinity," $x(t)$ and $y(t)$ must be polynomials (otherwise a root of the denominator would make $P$ intersect $O$). In addition, at $t = \infty$ there can be no intersection. To evaluate at $t = \infty$, substitute $t = \frac{1}{s}$, multiply through by the appropriate power of $s$ to clear denominators, and then evaluate at $s = 0$. If we have $a(t) = \sum_{i=0}^{4} a_i t^i$ and $b(t) = \sum_{i=0}^{6} b_i t^i$, then we get

$$\begin{aligned} y\Big(\frac{1}{s}\Big)^2 &= x\Big(\frac{1}{s}\Big)^3 + a\Big(\frac{1}{s}\Big)x\Big(\frac{1}{s}\Big) + b\Big(\frac{1}{s}\Big) \\ &= x\Big(\frac{1}{s}\Big)^3 + \Big(a_0 + \frac{a_1}{s} + \cdots + \frac{a_4}{s^4}\Big)x\Big(\frac{1}{s}\Big) + \Big(b_0 + \frac{b_1}{s} + \cdots + \frac{b_6}{s^6}\Big)\end{aligned}$$

Multiply through by $s^6$ to clear denominators. This gives

$$\begin{aligned}\Big(s^3y\Big(\frac{1}{s}\Big)\Big)^2 &= \Big(s^2x\Big(\frac{1}{s}\Big)\Big)^3 + (a_0s^4 + a_1s^3 + \cdots + a_4)\Big(s^2x\Big(\frac{1}{s}\Big)\Big) \\ &\quad +(b_0s^6 + b_1s^5 + \cdots + b_6) \\ y_1(s)^2 &= x_1(s)^3 + (a_0s^4 + a_1s^3 + \cdots + a_4)x_1(s) + (b_0s^6 + b_1s^5 + \cdots + b_6)\end{aligned}$$

where $y_1(s) = s^3y\big(\frac{1}{s}\big)$ and $x_1(s) = s^2x\big(\frac{1}{s}\big)$. Now evaluating at $s = 0$ does not give $\infty$ since $(PO) = 0$, so it follows that $deg(x) \leq 2$ and $deg(y) \leq 3$. ■

In general when $S$ is a rational elliptic surface, we have that $E(K)$ is isomorphic to a sublattice of $E_8$ determined by the structure of the reducible fibers [OS]. Results similar to Theorem 2.3.1 exist in each possible case. The structure of the reducible fibers can be determined from Table 2.1 by looking up the behavior of the discriminant $\Delta$ and the $j$-invariant in the first two columns.

## 2.4 Results For Specific Rational Elliptic Surfaces

Here we specialize the results of the previous section and those in [OS] to the specific rational elliptic surfaces that are studied in this paper.

THEOREM **2.4.1.** *The elliptic curve $E_m : y^2 = x^3 - x + m^2$ defined over $\overline{\mathbb{Q}}(m)$ has Mordell–Weil group $E_m\big(\overline{\mathbb{Q}}(m)\big) \cong \mathbb{Z}^2$, which is generated by the points $P = (0, m)$ and $Q = (1, m)$.*

PROOF: We have $\Delta = -16(-4 + 27m^4)$, which has four distinct roots in $\overline{\mathbb{Q}}$. For each root $m_0$, we have $v_{m_0}(\Delta) = 1$ and $v_{m_0}(j) = -1$. From Table 2.1, this gives a

Table 2.1: Classification of singular fibers

| $v(\Delta)$ | $j$-invariant | Kodaira Type | Contribution to $T$ |
|---|---|---|---|
| 0 | $v(j) \geq 0$ | $I_0$ | 0 |
| $n$ | $v(j) = -n$ | $I_n$ | $A_{n-1}$ |
| 2 | $j = 0$ | $II$ | 0 |
| 3 | $j = 1728$ | $III$ | $A_1$ |
| 4 | $j = 0$ | $IV$ | $A_2$ |
| 6 | $v(j) \geq 0$ | $I_0^*$ | $D_4$ |
| $6 + n$ | $v(j) = -n$ | $I_n^*$ | $D_{n+4}$ |
| 8 | $j = 0$ | $IV^*$ | $E_6$ |
| 9 | $j = 1728$ | $III^*$ | $E_7$ |
| 10 | $j = 0$ | $II^*$ | $E_8$ |

reducible fiber of Kodaira type $I_1$, which gives trivial contribution ($A_0$) to $T$. At $m = \infty$, we make the substitution $m = \frac{1}{s}$, and the curve becomes $y^2 = x^3 - s^4x + s^4$ which has discriminant $\Delta = -16(-4s^4 + 27)s^8$. At $s = 0$ ($m = \infty$), we have $v_\infty(\Delta) = 8$ and $j = 0$, so from Table 2.1, this reducible fiber has Kodaira type $IV^*$, which contributes a lattice of type $E_6$ to $T$. From [OS], if the image of $T$ in $NS(S)/\langle (O), (F) \rangle$ is a lattice of type $E_6$, then $E_m\big(\overline{\mathbb{Q}}(m)\big) \cong A_2^*$, which has rank 2 and trivial torsion. There are 6 minimal vectors of norm $\frac{2}{3}$ in the $A_2^*$ lattice [CS, p. 115]. These correspond to points on $E_m$ which have $deg(x) = 0$ and $deg(y) \leq 1$ [Shi3], giving $\pm(0, m)$, $\pm(1, m)$, and $\pm(-1, m)$. Since $(-1, m) = (0, m) + (1, m)$, we can take $P = (0, m)$ and $Q = (1, m)$ as generators. ■

THEOREM **2.4.2.** *Let $m_2(t) \in \mathbb{Q}[t]$ be a quadratic polynomial, and let $E_{m_2(t)}$ be*

*the elliptic curve* $y^2 = x^3 - x + m_2(t)^2$ *defined over* $\overline{\mathbb{Q}}(t)$. *Then the Mordell–Weil group* $E_{m_2(t)}\big(\overline{\mathbb{Q}}(t)\big) \cong \mathbb{Z}^6$, *which is generated by 54 points* $(x(t), y(t))$, *where* $deg(x) \leq 1$ *and* $deg(y) \leq 2$.

PROOF: We have $\Delta = -16(-4 + 27m_2(t)^4)$, which we claim has eight distinct roots in $\overline{\mathbb{Q}}$. Any multiple root of $\Delta$ must be a root of both $\Delta$ and $\Delta' = -16 \cdot 27 \cdot 4m_2(t)^3 m_2'(t)$. Clearly a root of $m_2(t)$ cannot be a root of $\Delta$. Since $m_2(t)$ is quadratic, $m_2'(t)$ is linear and so has a rational root $t_0$. Then $m_2(t_0)$ is rational, which will make $\Delta \neq 0$.

Each of these roots of $\Delta$ gives a reducible fiber of Kodaira type $I_1$, which gives trivial contribution $(A_0)$ to $T$. At $t = \infty$, we make the substitution $t = \frac{1}{s}$, and the curve becomes $y^2 = x^3 - s^4 x + s^2 n(s)^2$ where $n(s) = s^2 m_2\big(\frac{1}{s}\big)$. This has discriminant $\Delta = -16(-4s^8 + 27n(s)^4)s^4$. Note that since $m_2(t)$ has degree 2, $n(s)$ is a polynomial with a nontrivial constant term, which implies $n(0) \neq 0$. At $s = 0$, this reducible fiber has Kodaira type $IV$, which contributes a lattice of type $A_2$ to $T$. From [OS], if the image of $T$ in $NS(S)/\langle (O), (F) \rangle$ is a lattice of type $A_2$, then $E_{m_2(t)}\big(\overline{\mathbb{Q}}(t)\big) \cong E_6^*$, which has rank 6 and trivial torsion. There are 54 minimal vectors of norm $\frac{4}{3}$ in the $E_6^*$ lattice [CS, pp. 125-126]. These correspond to points on $E_{m_2(t)}$ which have $deg(x) \leq 1$ and $deg(y) \leq 2$ [Shi3]. ■

THEOREM **2.4.3.** *Let* $m_3(t) \in \mathbb{Q}[t]$ *be a cubic polynomial, and let* $E_{m_3(t)}$ *be the elliptic curve* $y^2 = x^3 - x + m_3(t)^2$ *defined over* $\overline{\mathbb{Q}}(t)$. *Then the Mordell–Weil group* $E_{m_3(t)}\big(\overline{\mathbb{Q}}(t)\big) \cong \mathbb{Z}^8$, *which is generated by 240 points* $(x(t), y(t))$, *where* $deg(x) \leq 2$ *and* $deg(y) \leq 3$.

PROOF: We have $\Delta = -16(-4 + 27m_3(t)^4)$, which we claim has twelve distinct roots in $\overline{\mathbb{Q}}$. If $t_0$ is a multiple root of $\Delta$ then it is a root of both $\Delta$ and $\Delta' =$

$-16 \cdot 27 \cdot 4m_3(t)^3 m_3'(t)$. Any root of $m_3(t)$ cannot be a root of $\Delta$, so $t_0$ must be a root of $m_3'(t)$ which is a quadratic polynomial. Thus $m_3(t_0)$ generates at most a degree 2 extension of $\mathbb{Q}$. However, $m_3(t_0) = \sqrt[4]{4/27}$ generates a degree four extension of $\mathbb{Q}$, so we have a contradiction.

Each of these roots of $\Delta$ gives a reducible fiber of Kodaira type $I_1$, which gives trivial contribution $(A_0)$ to $T$. At $t = \infty$, we make the substitution $t = \frac{1}{s}$, and the curve becomes $y^2 = x^3 - s^4 x + n(s)^2$ where $n(s) = s^3 m_3\big(\frac{1}{s}\big)$. This has discriminant $\Delta = -16(-4s^{12} + 27n(s)^4)$. Note that since $m_3(t)$ has degree 3, $n(s)$ is a polynomial with a nontrivial constant term, which implies $n(0) \neq 0$. At $s = 0$, we have $\Delta \neq 0$, so $t = \infty$ makes no contribution to $T$. Thus all singular fibers have only one irreducible component, so Theorem 2.3.1 implies the result. ■

The following results are not proved here since the proofs are very similar to the ones above.

THEOREM **2.4.4.** *The elliptic curve $C_m : y^2 = x^3 - m^2 x + 1$ defined over $\mathbb{Q}(m)$ has Mordell–Weil group $C_m\big(\overline{\mathbb{Q}}(m)\big) \cong \mathbb{Z}^4$, which is generated by 24 points $(x(t), y(t))$, where $deg(x) \leq 1$ and $deg(y) \leq 1$.*

THEOREM **2.4.5.** *Let $m(t) \in \mathbb{Q}[t]$ be a quadratic polynomial, and let $C_{m(t)}$ be the elliptic curve $y^2 = x^3 - m(t)^2 x + 1$ defined over $\mathbb{Q}(t)$. Then the Mordell–Weil group $C_{m(t)}\big(\overline{\mathbb{Q}}(t)\big) \cong \mathbb{Z}^8$, which is generated by 240 points $(x(t), y(t))$, where $deg(x) \leq 2$ and $deg(y) \leq 3$.*

The Mordell–Weil groups of $C_m\big(\overline{\mathbb{Q}}(m)\big)$ and $C_{m(t)}\big(\overline{\mathbb{Q}}(t)\big)$ are of types $D_4^*$ and $E_8$ respectively.

## 2.5 Independence of Points

The results of this section deal with the effects of specialization on the independence of points. Let $C$ be a curve defined over a field $k$, let $S$ be an elliptic surface over $C$, and let $K = k(C)$. Then $S$ can be viewed as an elliptic curve $E$ over the field $K$. For any $t \in C(\overline{k})$, let $E_{(t)}$ denote the specialization of $E$ at $t$.

THEOREM **2.5.1 (Silverman).** [Sil2, p. 271] *The specialization map*

$$\sigma_t : E(K) \to E_{(t)}(\overline{k})$$

*is injective for all but finitely* $t \in C(\overline{k})$.

Given a set of independent points on an elliptic surface, this implies that the points remain independent when specializing to some $t \in C(\overline{k})$ with only a finite number of exceptions.

In addition, a set of points on an elliptic surface $E(K)$ which specialize to independent points for some $t \in C(k)$ must be independent in $E(K)$.

PROPOSITION **2.5.2.** *Let* $P_1, \ldots, P_n$ *be a collection of points in* $E(K)$*, and suppose that the fiber* $E_{t_0}$ *is nonsingular, where* $t_0 \in C(k)$*. If the images of the points* $P_i$ *under the specialization* $\sigma_{t_0}$ *are independent in* $E_{(t_0)}(k)$*, then the points* $P_i$ *must be independent in the group* $E(K)$*.*

PROOF: Suppose that the points $P_i$ for $i = 1 \ldots n$ are dependent in the group $E(K)$. Then there exists a relation of the form

$$\sum_i a_i P_i = O$$

where $a_i \in \mathbb{Z}$, and not all $a_i$ are 0. This relation holds under all specializations, including $t_0$, so the specialized points must be dependent. Thus if the specialized

points are independent, then the original points in $E(k(C))$ must be independent as well. ■

This proposition provides a simple technique for proving the independence of generic sections on an elliptic surface. Simply specialize to any value $t_0 \in C(k)$, and check whether or not the resulting points are independent. If they are, then the generic sections must be independent in $E(K)$. If they are in fact dependent, no conclusion can be drawn. However, any relation among the generic sections in $E(K)$ must also hold among the specialized points. This suggests that when a relation is discovered among the specialized points, it is a good idea to check whether the corresponding relation holds among the generic sections in $E(K)$.

# Chapter 3: Lifting $\mathbb{Q}$-points to $\mathbb{Q}(t)$-points

## 3.1 Basic Facts

A parameterized family of elliptic curves can also be viewed as an elliptic curve over a function field. This often provides insight into the basic properties that all curves in the family share. For example, [BM] studies the family

$$E_m : y^2 = x^3 - x + m^2.$$

With very little effort, several "generic" solutions to this equation can be found, including $P = (0, m)$, $Q = (1, m)$, $R = (-1, m)$ and $S = (m^2, m^3)$. Solutions of this type are referred to as generic points on $E_m$, and they exist for every value of $m$. Equivalently, treating $m$ as an indeterminate makes $E_m$ an elliptic curve defined over the function field $\mathbb{Q}(m)$, and these are points in the group $E_m(\mathbb{Q}(m))$. As such, the addition law on this group can be used to generate more generic points from these.

For any specific value of $m_0 \in \mathbb{Q}$, let $P|_{m_0}$ denote the point $P$ evaluated at $m_0$, and similarly for $Q$, $R$, and $S$. For example, setting $m = 2$ gives $P|_2 = (0, 2) \in E_2(\mathbb{Q})$. It is fairly simple to find the relations $P|_2 + Q|_2 + R|_2 = \infty$ and $P|_2 + 2Q|_2 + S|_2 = \infty$. Also, the determinant of the height matrix from $P|_2$ and $Q|_2$ is 0.3729918, so $P|_2$ and $Q|_2$ are independent. Thus $P|_2$ and $Q|_2$ generate a rank 2 subgroup of $E_2(\mathbb{Q})$, and $R|_2$ and $S|_2$ are in this subgroup.

By Proposition 2.5.2, $P$ and $Q$ must be independent in $E_m(\mathbb{Q}(m))$ since they are independent under the specialization to $m = 2$. The two relations found above when $m = 2$ suggest the possibility that these relations may hold for the generic points in $E_m(\mathbb{Q}(m))$ as well, and in fact they do:

$$P + Q + R = \infty$$

$$P + 2Q + S = \infty$$

Thus $P$ and $Q$ generate a subgroup of rank 2 in $E_m(\mathbb{Q}(m))$. In fact, using the methods of Shioda [OS, Shi1, Shi2, Shi3], we have already proven an even stronger result (see Theorem 2.4.1) about the group $E_m\big(\overline{\mathbb{Q}}(m)\big)$.

THEOREM **3.1.1.** *$E_m\big(\overline{\mathbb{Q}}(m)\big)$ has rank 2 generated by $P = (0, m)$ and $Q = (1, m)$.*

Since both $P$ and $Q$ are in the field $\mathbb{Q}(m)$, we have

COROLLARY **3.1.2.** *$E_m(\mathbb{Q}(m))$ has rank 2 generated by $P = (0, m)$ and $Q = (1, m)$.*

## 3.2 An Example of a Lift

A rather interesting result about the family $E_m$ is proved in [BM]:

THEOREM **3.2.1 (Brown–Myers).** *There are infinitely many values of $m$ such that the rank of $E_m(\mathbb{Q})$ is at least 3.*

This is not a surprising result given the number of small positive integers $m \leq 500$ for which this is true (see Table 1.1 or Appendix A). What makes it interesting is the way in which it is proved in [BM]. Suppose we set $m(t) = 54t^2 - 165t - 90$. Then direct computation verifies that the point $R(t) = (36t+17, 54t^2+267t+114)$

lies on the curve $E_{m(t)}$. Elementary techniques are used to prove that this point is independent from the original generators $P = (0, m(t))$ and $Q = (1, m(t))$ for every $t \in \mathbb{Z}$. Here we prove a related result:

THEOREM **3.2.2.** *Let* $m(t) = 54t^2 - 165t - 90$. *Then the points* $P = (0, m(t))$, $Q = (1, m(t))$ *and* $R(t) = (36t + 17, 54t^2 + 267t + 114)$ *are independent in the group* $E_{m(t)}(\mathbb{Q}(t))$.

PROOF: Specializing to $t = 0$ gives $m(0) = -90$ and the points $P|_{-90} = (0, -90)$, $Q|_{-90} = (1, -90)$ and $R(0) = (17, 114) \in E_{90}(\mathbb{Q})$. The determinant of the height matrix for these points is 22.684449, so these points are independent in $E_{90}(\mathbb{Q})$. By Proposition 2.5.2, the $\mathbb{Q}(t)$ points $P$, $Q$ and $R(t)$ are independent in $E_{m(t)}(\mathbb{Q}(t))$. ■

One can view this subfamily as a "lift" of the point $(17, 114)$ on the curve $E_{90}$. In general, we define a lift to be an elliptic surface $E_{m(t)}$ that contains an additional point $R(t) = (x(t), y(t))$, where this point was derived from a given point $(x_0, y_0) \in E_{m_0}(\mathbb{Q})$. Specializing to $t = 0$ gives $m(0) = m_0$ and $R(0) = (x_0, y_0)$. This is our first concrete example of a lift, which leads to several questions:

- Given $m_0 \in \mathbb{Q}$ and a point $(x_0, y_0) \in E_{m_0}(\mathbb{Q})$, does there exist a lift? In other words, can we find a nonconstant polynomial $m(t)$ and a point $R(t) \in E_{m(t)}(\mathbb{Q}(t))$ such that $m(0) = m_0$ and $R(0) = (x_0, y_0)$?
- Does there exist a lift which has four independent points over $\mathbb{Q}(t)$?
- Are there lifts like this in other families?

## 3.3 Finding Another Lift

There are many values of $m$ for which $E_m$ has rank 3 or more (see Table 1.1). Some of these actually fall into the subfamily $m(t) = 54t^2 - 165t - 90$ given in Theorem 3.2.2. For example, $m\left(\frac{11}{3}\right) = 31$ is in this subfamily with the extra point $R\left(\frac{11}{3}\right) = (149, 1819)$. This point turns out to be independent from the original generators $P$ and $Q$. Actually, $E_{31}(\mathbb{Q})$ has rank 4 generated by these three points and the point $(-7, 25)$. Also, $m\left(-\frac{1}{2}\right) = 6$ is in this subfamily. In this case, the additional point $R\left(-\frac{1}{2}\right) = (-1, -6)$ is not independent from the original generators, as $(-1, -6) = (0, 6) + (1, 6) = P|_6 + Q|_6$.

On the other hand, many values of $m$ do not fall into this subfamily, like $m = 5$ for example. An attempt to solve $m(t) = 5$ gives $54t^2 - 165t - 95 = 0$, which has discriminant $3^2 \cdot 5 \cdot 1061$. This is not a perfect square, so there are no rational roots. Also, setting $m(t) = -5$ gives a quadratic polynomial with no rational roots, since its discriminant is $3^2 \cdot 5 \cdot 1013$. This implies that there is no $t \in \mathbb{Q}$ such that $m(t) = \pm 5$, so 5 does not fall in the subfamily given in Theorem 3.2.2. We now find such a lift for $m = 5$.

Example **3.3.1.** A quick search for points on $E_5$ gives $(-3, -1)$ as a point which turns out to be independent from $P|_5 = (0, 5)$ and $Q|_5 = (1, 5)$. In fact, $E_5(\mathbb{Q})$ has rank 3 generated by these three points. Thus we attempt to find a quadratic function $M_5(t)$ with $M_5(0) = 5$ such that $E_{M_5(t)}(\mathbb{Q}(t))$ has an extra point $R_5(t) = (x(t), y(t)) \in E_{M_5(t)}(\mathbb{Q}(t))$ with $R_5(0) = (-3, -1)$. Theorem 2.4.2 implies that generators of this group have $deg(x) \leq 1$ and $deg(y) \leq 2$, so set

$$M_5(t) = At^2 + Bt + 5 \qquad R_5(t) = (x_1 t - 3,\ y_2 t^2 + y_1 t - 1)$$

Substituting into the equation for $E_{M_5(t)}$ gives

$$(y_2t^2 + y_1t - 1)^2 = (x_1t - 3)^3 - (x_1t - 3) + (At^2 + Bt + 5)^2 \tag{3.1}$$

The constant terms cancel out here, leaving five unknowns $(x_1, A, B, y_2, y_1)$ with four relations given by equating the coefficients of $t^1$ through $t^4$. These relations are

$$-2y_1 = 10B + 26x_1 \qquad (t^1)$$

$$-2y_2 + {y_1}^2 = 10A + B^2 - 9{x_1}^2 \qquad (t^2)$$

$$2y_2y_1 = 2AB + {x_1}^3 \qquad (t^3)$$

$${y_2}^2 = A^2 \qquad (t^4)$$

If $x_1 = 0$, then the only solution to these equations is $A = B = y_2 = y_1 = 0$, which just gives the point $(-3, -1)$ on $E_5$. Thus $x_1 \neq 0$. Now $t$ can be scaled by a constant multiple to get $x_1 = 1$. This leaves four unknowns and four relations.

The coefficient $(t^1)$ is linear in $y_1$ and the coefficient $(t^2)$ is linear in $y_2$. Solving (with $x_1 = 1$) gives

$$\begin{aligned} y_1 &= -5B - 13 \\ y_2 &= -5A + \frac{1}{2}\big({y_1}^2 - B^2 + 9\big) \\ &= -5A + 12B^2 + 65B + 89 \end{aligned}$$

Substituting these into the coefficient $(t^3)$ leaves a linear function of $A$, which can be solved to give

$$A = \frac{120B^3 + 962B^2 + 2580B + 2315}{48B + 130}$$

Putting all of these into the $(t^4)$ term gives

$$\frac{(B+3)(2B+5)(3B+8)(4B+11)(12B+29)(12B+35)}{(24B+65)^2} = 0$$

Table 3.1: Lifts of the point $(-3,-1)$ on $E_5$

| $B$ | $M_5(t) = At^2 + Bt + 5$ | $R_5(t) = (t-3, y_2t^2 + y_1t - 1)$ |
|---|---|---|
| $-3$ | $\frac{1}{2}t^2 - 3t + 5$ | $(t-3, -\frac{1}{2}t^2 + 2t - 1)$ |
| $-5/2$ | $\frac{1}{4}t^2 - \frac{5}{2}t + 5$ | $(t-3, \frac{1}{4}t^2 - \frac{1}{2}t - 1)$ |
| $-8/3$ | $\frac{1}{6}t^2 - \frac{8}{3}t + 5$ | $(t-3, \frac{1}{6}t^2 + \frac{1}{3}t - 1)$ |
| $-11/4$ | $\frac{1}{4}t^2 - \frac{11}{4}t + 5$ | $(t-3, -\frac{1}{4}t^2 + \frac{3}{4}t - 1)$ |
| $-29/12$ | $\frac{1}{3}t^2 - \frac{29}{12}t + 5$ | $(t-3, \frac{1}{3}t^2 - \frac{11}{12}t - 1)$ |
| $-35/12$ | $\frac{3}{8}t^2 - \frac{35}{12}t + 5$ | $(t-3, -\frac{3}{8}t^2 + \frac{19}{12}t - 1)$ |

The roots of this equation give 6 values for $B$. The results are given in Table 3.1. Specializing any of these to $t = 0$ reduces to the point $(-3,-1)$, which is independent from $P|_5$ and $Q|_5$. So by Proposition 2.5.2, $P = (0, M_5(t))$, $Q = (1, M_5(t))$ and $R_5(t)$ must be independent on $E_{M_5(t)}(\mathbb{Q}(t))$. This gives six different subfamilies of rank at least 3, each of which is a lift of the point $(-3,-1)$ on $E_5$. $\square$

## 3.4 Generalizing the Lift

The lifting process described in the previous section can be generalized to work starting with almost any point on any curve $E_m$.

THEOREM **3.4.1.** *Let $m_0 \in \mathbb{Q}$, with $m_0 \neq 0$ and suppose that $(p,q)$ is a rational point on $E_{m_0}$ with $q \neq m_0$ and $p \neq 0$. Let $c = \frac{q-m_0}{p}$ and set*

$$M(t) = \frac{1}{2c}t^2 + \frac{2p - c^2}{2c}t + m_0$$

$$(X(t), Y(t)) = \left(t + p,\ \frac{1}{2c}t^2 + \frac{2p + c^2}{2c}t + q\right)$$

*Then* $(X(t), Y(t)) \in E_{M(t)}(\mathbb{Q}(t))$ *is a lift of the point* $(p, q)$.

PROOF: Notice that the equation for $E_m$ can be rearranged into the form

$$(y - m)(y + m) = x(x - 1)(x + 1). \tag{3.2}$$

Evaluating each factor on the left hand side separately, we get:

$$\begin{aligned} Y(t) - M(t) &= \left(\frac{1}{2c}t^2 + \frac{2p + c^2}{2c}t + q\right) - \left(\frac{1}{2c}t^2 + \frac{2p - c^2}{2c}t + m_0\right) \\ &= ct + (q - m_0) \\ &= c(t + p) \\ &= cX(t) \end{aligned}$$

and

$$\begin{aligned} Y(t) + M(t) &= \left(\frac{1}{2c}t^2 + \frac{2p + c^2}{2c}t + q\right) + \left(\frac{1}{2c}t^2 + \frac{2p - c^2}{2c}t + m_0\right) \\ &= \frac{1}{c}t^2 + \frac{2p}{c}t + (q + m_0) \\ &= c^{-1}(t^2 + 2pt + c(q + m_0)) \\ &= c^{-1}(t^2 + 2pt + p^2 - 1) \\ &= c^{-1}(t + p + 1)(t + p - 1) \\ &= c^{-1}(X(t) + 1)(X(t) - 1). \end{aligned}$$

Note that $c(q + m_0) = (q^2 - {m_0}^2)/p = (p^3 - p)/p = p^2 - 1$ since $(p, q) \in E_{m_0}(\mathbb{Q})$. Multiplying these two equations together completes the proof. ■

REMARK **3.4.2.** Theorem 3.4.1 was originally developed by the rather tedious process of substituting $M(t) = At^2 + Bt + m_0$ and $(X(t), Y(t)) = (t + p, y_2t^2 + y_1t + q)$ into the equation for $E_{M(t)}$ and equating coefficients. (Theorem 2.4.2 implies

that the generators should have this form.) The form (3.2) of the equation for $E_m$ made this process much easier.

If $X(t) = t+p$ then $deg(X^3-X) = 3$. Since both $Y(t)$ and $M(t)$ are quadratic, then either $Y(t)-M(t)$ or $Y(t)+M(t)$ must have its leading term vanish so that both sides of (3.2) have degree 3. Thus one of the factors $Y(t) \pm M(t)$ must be linear in $t$ and must divide $X(t)^3 - X(t) = (t+p)(t+p-1)(t+p+1)$. Theorem 3.4.1 corresponds to the case $Y(t) - M(t) = cX(t)$. Here $c$ can be computed by comparing the constant terms ($q - m_0 = cp$), and $Y(t) + M(t) = \frac{1}{c}(X(t)-1)(X(t)+1)$. In all there are 6 cases: two choices of whether $Y(t)-M(t)$ or $Y(t) + M(t)$ is linear; and three choices of the corresponding linear factor, namely $X(t)$, $X(t)+1$ or $X(t)-1$. Here are the results in each case:

$$
\begin{array}{llll}
Y_1 - M_1 = c_1 X & c_1 = \dfrac{q-m_0}{p} & M_1 = \dfrac{1}{2c_1}t^2 + \dfrac{2p - {c_1}^2}{2c_1}t + m_0 \\
Y_2 - M_2 = c_2(X-1) & c_2 = \dfrac{q-m_0}{p-1} & M_2 = \dfrac{1}{2c_2}t^2 + \dfrac{2p - {c_2}^2 + 1}{2c_2}t + m_0 \\
Y_3 - M_3 = c_3(X+1) & c_3 = \dfrac{q-m_0}{p+1} & M_3 = \dfrac{1}{2c_3}t^2 + \dfrac{2p - {c_3}^2 - 1}{2c_3}t + m_0 \\
Y_4 + M_4 = c_4(X+1) & c_4 = \dfrac{q+m_0}{p+1} & M_4 = \dfrac{-1}{2c_4}t^2 + \dfrac{-2p + {c_4}^2 + 1}{2c_4}t + m_0 \\
Y_5 + M_5 = c_5(X-1) & c_5 = \dfrac{q+m_0}{p-1} & M_5 = \dfrac{-1}{2c_5}t^2 + \dfrac{-2p + {c_5}^2 - 1}{2c_5}t + m_0 \\
Y_6 + M_6 = c_6 X & c_6 = \dfrac{q+m_0}{p} & M_6 = \dfrac{-1}{2c_6}t^2 + \dfrac{-2p + {c_6}^2}{2c_6}t + m_0
\end{array}
$$

For each of these cases, $X(t) = t + p$, and $Y(t)$ can be computed from the information given. Note that each case only works if both the numerator and denominator of the given $c_i$ are nonzero. This is why Theorem 3.4.1 contains the assumptions $q \neq m_0$ and $p \neq 0$. $\square$

REMARK **3.4.3.** In Example 3.3.1, six lifts of the point $(-3,-1) \in E_5(\mathbb{Q})$ were produced (see Table 3.1). Applying Theorem 3.4.1 produces $M(t) = \frac{1}{4}t^2 - \frac{5}{2}t + 5$,

which is the second one listed in the table. The six $M(t)$ polynomials in the remark above correspond to the six lifts in Table 3.1. $\square$

As a consequence of Theorem 3.4.1 and Remark 3.4.2, we have the following general result that any point on $E_m$ can be lifted.

THEOREM **3.4.4.** *For any $m_0 \in \mathbb{Q}$ with $m_0 \neq 0$ and any point $(p, q) \in E_{m_0}(\mathbb{Q})$, there exists a quadratic polynomial $M(t)$ with $M(0) = m_0$ and a point $R(t)$ with $R(0) = (p, q)$ such that $P = (0, m(t))$, $Q = (1, m(t))$ and $R(t)$ are independent points in $E_{m(t)}(\mathbb{Q}(t))$.*

PROOF: First we show that every point in $(p, q) \in E_{m_0}(\mathbb{Q})$ has a lift. Note that Theorem 3.4.1 contains the conditions $q \neq m_0$ and $p \neq 0$. These are included so that $c = \frac{q-m_0}{p}$ and $c^{-1}$ do not have 0 in the denominator. Other cases listed in Remark 3.4.2 have different values of $c$, and so have different conditions. Overall, at least two of the six lifts in Remark 3.4.2 are defined for any point $(p, q) \in E_{m_0}(\mathbb{Q})$. For example, the point $(0, m_0)$ has the lifts given by $M_4(t)$ and $M_5(t)$.

The fact that these points are independent in $E_{m(t)}(\mathbb{Q}(t))$ requires more work. In Section 4.2, we show that if $m(t) \in \mathbb{Q}[t]$ is a quadratic polynomial and $E_{m(t)}(\mathbb{Q}(t))$ contains an additional point $(x(t), y(t))$ with $deg(x) = 1$ and $deg(y) = 2$, then this point and the points $P = (0, m(t))$ and $Q = (1, m(t))$ are independent in $E_{m(t)}(\mathbb{Q}(t))$. This covers the present situation. $\blacksquare$

REMARK **3.4.5.** The lift given by Brown and Myers [BM] started with the point $(17, 114) \in E_{90}(\mathbb{Q})$. It turns out that $E_{90}(\mathbb{Q})$ has rank 3, and is generated by this point and the points $P = (0, 90)$ and $Q = (1, 90)$. The above Theorem shows that they could have started with *any rational point* on any $E_{m_0}(\mathbb{Q})$ with $m_0 \neq 0$ and obtained a similar result. $\square$

## 3.5 Subfamilies of Higher Rank

A rather interesting result comes from using Theorem 3.4.1 repeatedly on the same curve. The smallest positive integer $m$ such that $E_m$ has rank 5 is $m = 113$. The points $P|_{113} = (0, 113)$, $Q|_{113} = (1, 113)$, $R_1 = (-23, -25)$, $R_2 = (-19, -77)$, and $R_3 = (-11, 107)$ are on the curve $E_{113}$, and are independent since the determinant of the height matrix for these points is 104.60041. Applying Theorem 3.4.1 to each $R_i$ gives a subfamily $m_i(t_i)$ and a point $D_i(t_i) = (X(t_i), Y(t_i)) \in E_{m_i(t_i)}$ as follows:

$$\begin{aligned} m_1(t_1) &= \frac{1}{12}t_1^2 - \frac{41}{6}t_1 + 113 \qquad & D_1(t_1) &= (t_1 - 23, \frac{1}{12}t_1^2 - \frac{5}{6}t_1 - 25) \\ m_2(t_2) &= \frac{1}{20}t_2^2 - \frac{69}{10}t_2 + 113 \qquad & D_2(t_2) &= (t_2 - 19, \frac{1}{20}t_2^2 + \frac{31}{10}t_2 - 77) \\ m_3(t_3) &= \frac{1}{40}t_3^2 - \frac{211}{20}t_3 + 113 \qquad & D_3(t_3) &= (t_3 - 11, \frac{1}{40}t_3^2 + \frac{189}{20}t_3 - 107) \end{aligned} \tag{3.3}$$

Ideally, all of these subfamilies would have the same $m(t)$, which would give 5 points on a curve over $\mathbb{Q}(t)$. These points would then be independent since they specialize to independent points on $E_{113}$. Instead, we need to find the intersection of these subfamilies.

Setting $m_1(t_1) = m_2(t_2)$ gives a conic section which has the obvious solution $t_1 = t_2 = 0$. This can be used to parameterize all solutions. Set $t_2 = wt_1$ and substitute to get:

$$t_1(w) = \frac{414w - 410}{3w^2 - 5} \tag{3.4}$$

$$t_2(w) = \frac{414w^2 - 410w}{3w^2 - 5} \tag{3.5}$$

and $m_1(t_1(w)) = m_2(t_2(w))$ is given by:

$$M_{1,2}(w) = \frac{1017w^4 - 8487w^3 + 19298w^2 - 14145w + 2825}{(3w^2 - 5)^2} \tag{3.6}$$

Note that specializing these to $w = \frac{410}{414} = \frac{205}{207}$ gives $t_1\left(\frac{205}{207}\right) = 0 = t_2\left(\frac{205}{207}\right)$ and $M_{1,2}\left(\frac{205}{207}\right) = 113$.

THEOREM **3.5.1.** *Let $M_{1,2}(w)$ be as above in (3.6). Then the elliptic surface $E_{M_{1,2}(w)}$ contains the four $\mathbb{Q}(w)$ points $P = (0, M_{1,2}(w))$, $Q = (1, M_{1,2}(w))$, $D_1(t_1(w))$ and $D_2(t_2(w))$, where the $D_i(t)$ and $t_i(w)$ are given above. Moreover, these points are independent in the group $E_{M_{1,2}(w)}(\mathbb{Q}(w))$.*

PROOF: From Theorem 3.4.1, $D_i(t) \in E_{m_i(t)}(\mathbb{Q})$ for any $t$. Setting $t = t_i(w)$ implies that $D_1(t_1(w))$, $D_2(t_2(w)) \in E_{M_{1,2}(w)}(\mathbb{Q}(w))$. To show that these points are independent, specialize to $w = \frac{205}{207}$. This gives $t_1\left(\frac{205}{207}\right) = 0 = t_2\left(\frac{205}{207}\right)$ and $M_{1,2}\left(\frac{205}{207}\right) = 113$, which gives:

$$P|_{w=\frac{205}{207}} = P|_{m=113} = (0, 113)$$

$$Q|_{w=\frac{205}{207}} = Q|_{m=113} = (1, 113)$$

$$D_1\Big(t_1\Big(\frac{205}{207}\Big)\Big) = D_1(0) = (-23, -25)$$

$$D_2\Big(t_2\Big(\frac{205}{207}\Big)\Big) = D_2(0) = (-19, -77)$$

These are independent points on $E_{113}(\mathbb{Q})$. It follows from Proposition 2.5.2 that the points must be independent on $E_{M_{1,2}(w)}(\mathbb{Q}(w))$. ■

The next step is to set all three $m_i(t_i)$ equal to each other. A solution to this gives a curve of rank 5. This actually is the intersection of two quadratic surfaces, which gives an elliptic curve [W, pp. 39-41]. We already have the solutions to $m_1(t_1) = m_2(t_2)$ given by $M_{1,2}(w)$ from (3.6) above. Now we need solutions to $M_{1,2}(w) = m_3(t_3)$. Making the substitution

$$t_3 = v/(3w^2 - 5) + 211 \tag{3.7}$$

and clearing the denominators gives the curve

$$C' : v^2 = 400689w^4 - 339480w^3 - 428110w^2 - 565800w + 1113025 \qquad (3.8)$$

This quartic equation has a solution that comes from $t_1 = t_2 = t_3 = 0$, which is $w = \frac{205}{207}$ and $v = -211(3w^2 - 5) = -\frac{6201290}{14283}$. This makes $C'$ into an elliptic curve with minimal Weierstrass model

$$E' : y^2 = x^3 - x^2 - 103307652308x + 12301315572924612 \qquad (3.9)$$

The program `mwrank` yields that $E'(\mathbb{Q}) \cong \mathbb{Z}^2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ and is generated by the points $A = (223142, 18967200)$, $B = (298232, 89537850)$, $T_1 = (214182, 0)$ and $T_2 = (155402, 0)$.

THEOREM **3.5.2.** *Let $(w, v)$ run through the points on $C'$ as given by (3.8). Let $M_{1,2}$ be given by (3.6) and let $S$ be the elliptic surface over $C'$ given by $E_{M_{1,2}}$. Let $P, Q, D_1, D_2$ be as in Theorem 5.5.1, and let $D_3 = D_3(t_3)$ where $t_3$ is given by (3.7) and $D_3$ is given by (3.3). Then $P, Q, D_1, D_2, D_3$ are independent points in the Mordell–Weil group of $S$.*

PROOF: Let $P' = \left(\frac{410}{414}, -\frac{6201290}{14283}\right) \in C'$. Then specializing the five points to $(v, w) = P'$ gives the original five independent points $P|_{113} = (0, 113)$, $Q|_{113} = (1, 113)$, $D_1 = (-23, -25)$, $D_2 = (-19, -77)$, and $D_3 = (-11, 107)$ in the group $E_{113}(\mathbb{Q})$. Proposition 2.5.2 implies the desired result. ■

THEOREM **3.5.3.** *There are infinitely many values of $m$ such that $E_m(\mathbb{Q})$ has rank at least 5.*

PROOF: Since $C'(\mathbb{Q})$ has rank 2, it has infinitely many rational points. Specializing the five points in Theorem 3.5.2 to any point $P_0 = (v_0, w_0) \in C'(\mathbb{Q})$ gives

five rational points in the group $E_{M_{1,2}(w_0)}(\mathbb{Q})$. By Theorem 2.5.1 (Silverman's Specialization Theorem), these points remain independent under all but finitely many specializations. ■

REMARK **3.5.4.** Instead of using Silverman's Specialization Theorem, a weaker result due to Néron could be used. Néron's result states that the specialization map is injective for an infinite number of points, whereas Silverman's result states that it is injective for all but finitely many points. □

EXAMPLE **3.5.5.** The generators of the curve $E'(\mathbb{Q})$ in (3.9) are

$$A = (223142, 18967200) \qquad B = (298232, 89537850)$$

These correspond to the following points on the quartic $C'(\mathbb{Q})$ in (3.8):

$$(w_A, v_A) = \Big(\frac{139}{40}, \frac{6950}{17}\Big) \qquad (w_B, v_B) = \Big(\frac{69}{41}, -\frac{1240258}{1681}\Big)$$

Substituting these values of $w$ into (3.6) to compute $M_{1,2}$ gives

$$M_{1,2}^{(A)} = -\frac{6263}{289} \qquad M_{1,2}^{(B)} = 113$$

Substituting $w$ into (3.4) and (3.5), and $(w, v)$ into (3.7) gives

$$\begin{aligned} t_1^{(A)} &= -\frac{560}{17} & t_1^{(B)} &= 82 \\ t_2^{(A)} &= -\frac{1946}{17} & t_2^{(B)} &= 138 \\ t_3^{(A)} &= -\frac{6950}{17} & t_3^{(B)} &= 422 \end{aligned}$$

This gives the following 5 points on the curve $E_{M_{1,2}}$:

$$P^{(A)} = \Big(0, -\frac{6263}{289}\Big) \qquad P^{(B)} = (0, 113)$$
$$Q^{(A)} = \Big(1, -\frac{6263}{289}\Big) \qquad Q^{(B)} = (1, 113)$$
$$D_1(t_1^{(A)}) = \Big(\frac{169}{17}, \frac{10975}{289}\Big) \qquad D_1(t_1^{(B)}) = (59, 467)$$
$$D_2(t_2^{(A)}) = \Big(\frac{1623}{17}, \frac{269647}{289}\Big) \qquad D_2(t_2^{(B)}) = (119, 1303)$$
$$D_3(t_3^{(A)}) = \Big(\frac{6763}{17}, \frac{2293157}{289}\Big) \qquad D_3(t_3^{(B)}) = (411, 8333)$$

The determinants of the height matrices for these points (on the corresponding minimal models of $E_{M_{1,2}^{(A)}}$ or $E_{M_{1,2}^{(B)}}$) are:

$$det_A = 2680.24718 \qquad det_B = 104.60041$$

Since these determinants are nonzero, the points listed above are independent on the curves $E_{M_{1,2}^{(A)}}(\mathbb{Q})$ and $E_{M_{1,2}^{(B)}}(\mathbb{Q})$. Thus each of these curves has rank at least 5. In fact, $E_{M_{1,2}^{(A)}}(\mathbb{Q})$ actually has rank 6 with additional generator $\big(-\frac{63}{68}, \frac{50111}{2312}\big)$. □

# Chapter 4: Classifying Subfamilies of $E_m$ by Rank

## 4.1 Parameterizing Points on $E_m$

As we have seen above, the elliptic curve $E_m$ can be put in the form

$$(y-m)(y+m) = x(x-1)(x+1). \tag{4.1}$$

View $y$ and $m$ as the variables here and $x$ as a parameter, and set $y-m=u$. It follows that $y+m=(x^3-x)/u$, giving two equations which are linear in $y$ and $m$. Solving simultaneously gives:

$$m(x,u) = \frac{x^3-x}{2u} - \frac{u}{2} \tag{4.2}$$

$$y(x,u) = \frac{x^3-x}{2u} + \frac{u}{2} \tag{4.3}$$

For any field $K$ and any $x, u \in K$, this parameterization gives values of $m$ and $y$ such that $E_m(K)$ contains the point $(x,y)$.

EXAMPLE **4.1.1.** Let $x=3$ and $u=2$. This gives $m=5$ and the point $(3,7) \in E_5(\mathbb{Q})$. This point is actually independent from the two known generators $(0,5)$ and $(1,5)$. Thus $E_5$ has rank at least 3 (in fact, exactly 3). $\square$

EXAMPLE **4.1.2.** Let $x=36t+17$ and $u=12(36t+17)$. This gives $m(t) = 54t^2-165t-90$ and the point $R(t)=(36t+17, 54t^2+267t+114) \in E_{m(t)}(\mathbb{Q}(t))$.

This is the subfamily used in [BM] to prove that there are infinitely many values of $m$ such that $E_m$ has rank at least 3 (see Theorem 3.2.2). $\square$

There are several symmetries built into the parameterization given by (4.2) and (4.3). For example,

$$u \longmapsto -u \tag{4.4}$$

$$m(x,-u) = -m(x,u)$$

$$y(x,-u) = -y(x,u)$$

Note that $E_m$ and $E_{-m}$ are the same curve, so this just gives the point $(x,-y)$ which is the negative of the point $(x,y)$.

Another symmetry is:

$$x \longmapsto -x, \qquad u \longmapsto -u \tag{4.5}$$

$$m(-x,-u) = y(x,u)$$

$$y(-x,-u) = m(x,u)$$

In other words, if the point $(x,y)$ is on $E_m$, then the point $(-x,m)$ is on $E_y$. For example, given the point $(m^2,m^3) \in E_m(\mathbb{Q}(m))$, this symmetry gives the point $(-m^2,m) \in E_{m^3}(\mathbb{Q}(m))$. This leads to the following result:

PROPOSITION **4.1.3.** *$E_{m^3}(\mathbb{Q}(m))$ has rank at least 3, containing the independent points $(-m^2,m)$, $P=(0,m^3)$ and $Q=(1,m^3)$.*

PROOF: Clearly $E_{m^3}(\mathbb{Q}(m))$ contains the points $(-m^2,m)$, $P=(0,m^3)$ and $Q=(1,m^3)$. Evaluating at $m=2$ gives the points $(-m^2,m)=(-4,2)$, $P=(0,8)$ and $Q=(1,8)$ in $E_8(\mathbb{Q})$. The determinant of the height matrix

for these points is 2.8436, so the points are independent in $E_8(\mathbb{Q})$. By Proposition 2.5.2, $(-m^2, m)$, $(0, m^3)$ and $(1, m^3)$ are independent in $E_{m^3}(\mathbb{Q}(m))$. ■

A more interesting symmetry is given by:

$$u \longmapsto \frac{x^3 - x}{u} \tag{4.6}$$
$$m\Big(x, \frac{x^3 - x}{u}\Big) = -m(x, u)$$
$$y\Big(x, \frac{x^3 - x}{u}\Big) = y(x, u)$$

As we demonstrate in the next section and in Section 4.4, this symmetry is of particular use when searching for $m(t) \in \mathbb{Q}[t]$ which yield an additional point, as in Example 4.1.2.

## 4.2 Quadratic Subfamilies of Rank 3

Suppose we wish to find $m(t) \in \mathbb{Q}[t]$ of degree 2 such that $E_m(t)(\mathbb{Q}(t))$ has rank at least 3. By Theorem 2.4.2, the points that generate $E_{m(t)}\big(\overline{\mathbb{Q}}(t)\big)$ have $deg(x) \leq 1$ and $deg(y) \leq 2$, so it makes sense to look for $m(t)$ which yield an extra point of this form where $x(t)$ and $y(t)$ have rational coefficients. Much like in Example 4.1.2, the parameterization given by (4.2) and (4.3) can be used to search for such $m(t)$.

Given that $m(t)$ is a polynomial of degree 2, this places restrictions on the choices of $x(t)$ and $u$. Since $m(t)$ and $y(t)$ are both polynomials, $u = y(t) - m(t)$ must also be a polynomial. Moreover, $u$ must divide $x^3 - x$ to force $m(t)$ and $y(t)$ to be polynomials in $t$.

First let $deg(x) = 0$, so $x^3 - x$ is a constant. If $x^3 - x = 0$, we get the points $(0, \pm m(t))$ and $(\pm 1, \pm m(t))$, which are already known. If $x^3 - x \neq 0$, then $u$

must be a constant since $u|x^3 - x$. This makes $m(t)$ be a constant, which is not the desired case.

This leaves the case $deg(x) = 1$, so $deg(x^3-x) = 3$. Since $u|(x^3-x)$, the degree of $u$ can be no more than 3. Let $u' = (x^3 - x)/u$. Then $deg(u') = 3 - deg(u)$, and from the symmetry (4.6), $u$ and $u'$ generate the same solution (up to the sign of $m(t)$). This implies a symmetry in the degrees of $u$. In particular, the $u$'s of degree 1 and the $u$'s of degree 2 produce the same solutions, as do the $u$'s of degree 0 and the $u$'s of degree 3. Therefore we only need to consider $deg(u) = 0, 1$. In fact, if $deg(u) = 0$, this gives $deg(m) = 3$ (see Section 4.4). Thus we only need to consider $deg(u) = 1$.

Since $deg(x) = 1$, $deg(u) = 1$ and $u|(x^3-x)$, we see that $u$ must be a constant multiple of either $x$, $x - 1$, or $x + 1$. In each case, a linear shift of $t$ is made to put $m(t)$ in the form $ct^2 + d$. Here are the cases:

1. $u = kx$ where $k \in \mathbb{Q}$. Equation (4.2) yields $m(t) = \frac{1}{2k}(x^2 - k^2x - 1)$. Since $x$ is linear in $t$, an affine shift of $t$ can make $x = t + \frac{k^2}{2}$. Setting $c = \frac{1}{2k}$ gives:

$$m_1(t) = ct^2 - \frac{64c^4 + 1}{64c^3} \tag{4.7}$$

$$P_1(t) = \left(t + \frac{1}{8c^2},\ ct^2 + \frac{1}{2c}t - \frac{64c^4 - 3}{64c^3}\right)$$

   where $P_1(t) \in E_{m_1(t)}(\mathbb{Q}(t))$.

2. $u = k(x - 1)$ where $k \in \mathbb{Q}$. Equation (4.2) yields $m(t) = \frac{1}{2k}(x^2 - (k^2 - 1)x + k^2)$. Since $x$ is linear in $t$, an affine shift of $t$ can make $x = t + \frac{k^2-1}{2}$. Setting $c = \frac{1}{2k}$ gives:

$$m_2(t) = ct^2 - \frac{16c^4 - 24c^2 + 1}{64c^3} \tag{4.8}$$

$$P_2(t) = \left(t - \frac{1}{2} + \frac{1}{8c^2},\ ct^2 + \frac{1}{2c}t - \frac{16c^4 + 24c^2 - 3}{64c^3}\right)$$

where $P_2(t) \in E_{m_2(t)}(\mathbb{Q}(t))$.

3. $u = k(x+1)$ where $k \in \mathbb{Q}$. Equation (4.2) yields $m(t) = \frac{1}{2k}(x^2 - (k^2+1)x - k^2)$. Since $x$ is linear in $t$, an affine shift of $t$ can make $x = t + \frac{k^2+1}{2}$. Setting $c = \frac{1}{2k}$ gives:

$$m_3(t) = ct^2 - \frac{16c^4 + 24c^2 + 1}{64c^3} \tag{4.9}$$

$$P_3(t) = \left(t + \frac{1}{2} + \frac{1}{8c^2},\ ct^2 + \frac{1}{2c}t - \frac{16c^4 - 24c^2 - 3}{64c^3}\right)$$

where $P_3(t) \in E_{m_3(t)}(\mathbb{Q}(t))$.

This gives three different families with $m(t)$ quadratic, each of which has an extra point over $\mathbb{Q}(t)$.

THEOREM **4.2.1.** *Let $m(t) \in \mathbb{Q}[t]$ be a quadratic polynomial, and suppose that a linear shift of $t$ can change $m(t)$ into one of the following for some $c \in \mathbb{Q}$:*

$$m_1(t) = ct^2 - \frac{64c^4 + 1}{64c^3}$$

$$m_2(t) = ct^2 - \frac{16c^4 - 24c^2 + 1}{64c^3}$$

$$m_3(t) = ct^2 - \frac{16c^4 + 24c^2 + 1}{64c^3}$$

*Then $E_{m(t)}(\mathbb{Q}(t))$ has rank at least 3.*

PROOF: It has already been shown above that $P_i(t) \in E_{m_i(t)}(\mathbb{Q}(t))$ for $i = 1, 2, 3$, where the $P_i(t)$ are defined in (4.7), (4.8) and (4.9). Also, we have the points $P = (0, m_i(t))$ and $Q = (1, m_i(t))$. In Theorem 4.3.1 we shall show that $E_{m_1(t)}\big(\overline{\mathbb{Q}}(t)\big)$ is a lattice of rank 6, and the points $P(t)$, $Q(t)$ and $P_1(t)$ are three of the generators. Thus these points must be independent. Since these three points are rational, $E_{m(t)}(\mathbb{Q}(t))$ must have rank at least 3. The results for $m_2(t)$ and $m_3(t)$

are similar. ■

In fact, it is the case that each of these subfamilies can have no more than rank 3 over $\mathbb{Q}(t)$. This is proved in Theorem 4.3.5 in the next section by giving the explicit generators for $E_{m_1(t)}\big(\overline{\mathbb{Q}}(t)\big)$ and showing that no combination of the non-rational generators can be rational.

## 4.3 Classifying Quadratic Subfamilies By Rank

Theorem 4.2.1 gives three families of quadratic polynomials $m_i(t)$ for $i = 1, 2, 3$ which each have at least three independent points in $E_{m_i(t)}(\mathbb{Q}(t))$. Could any of these possibly have additional points over $\mathbb{Q}(t)$? In this section, we examine the case $m_1(t)$ with the extra point $P_1$ as given in (4.7). We repeat it here for convenience:

$$m_1(t) = ct^2 - \frac{64c^4 + 1}{64c^3} \tag{4.10}$$

$$P_1(t) = \Big(t + \frac{1}{8c^2}, ct^2 + \frac{1}{2c}t - \frac{64c^4 - 3}{64c^3}\Big) \tag{4.11}$$

From the proof of Theorem 4.2.1, the group $E_{m_1(t)}(\mathbb{Q}(t))$ contains the three points $P = (0, m_1(t))$, $Q = (1, m_1(t))$ and $P_1(t)$ given above. We show that these points are independent by showing that they are three of the generators of $E_{m_1(t)}\big(\overline{\mathbb{Q}}(t)\big)$. According to Theorem 2.4.2, since $m_1(t) \in \mathbb{Q}[t]$ is quadratic, $E_{m_1(t)}\big(\overline{\mathbb{Q}}(t)\big)$ has rank 6 with 54 points of the form $(x(t), y(t))$, where $x(t), y(t) \in \overline{\mathbb{Q}}(t)$ with $deg(x) \leq 1$ and $deg(y) \leq 2$. The goal here is to find all 54 of these points (27 $+/-$ pairs), and to prove that $E_{m_1(t)}(\mathbb{Q}(t))$ has exactly rank 3. Thus we set $x(t) = At + B$ and $y(t) = y_2t^2 + y_1t + y_0$ and substitute into the equation for $E_{m_1(t)}$:

$$(y_2t^2 + y_1t + y_0)^2 = (At + B)^3 - (At + B) + \left(ct^2 - \frac{64c^4 + 1}{64c^3}\right)^2$$

Here we treat $c$ as a constant ($c \neq 0$) and solve for $A$ and $B$. The coefficient of $t^4$ gives ${y_2}^2 = c^2$, so by changing the sign of $y$ if necessary we can take $y_2 = c$. This leaves the following four relations from the coefficients of $t^0$ through $t^3$ in four unknowns:

$$ {y_0}^2 = B^3 - B + \left(\frac{64c^4 + 1}{64c^3}\right)^2 \qquad (t^0) $$

$$ 2y_1y_0 = 3AB^2 - A \qquad (t^1) $$

$$ 2cy_0 + {y_1}^2 = 3A^2B - \frac{64c^4 + 1}{32c^2} \qquad (t^2) $$

$$ 2cy_1 = A^3 \qquad (t^3) $$

The relations $(t^3)$ and $(t^1)$ are linear in $y_1$ and $y_0$ respectively. Solving gives

$$ y_1 = \frac{A^3}{2c} $$
$$ y_0 = \frac{3AB^2 - A}{2y_1} = \frac{c(3B^2 - 1)}{A^2} $$

This leaves the relations $(t^2)$ and $(t^0)$, both of which are nonlinear polynomials in $A$ and $B$. Computing the resultant of these two polynomials with respect to $B$ gives a degree 32 polynomial in $A$ which factors as

$$ A^8(A - 1)(A + 1) \cdot f_1(A) \cdot f_2(A) \cdot f_3(A) \cdot f_4(A) \cdot f_5(A) = 0 \qquad (4.12) $$

where the $f_i(A)$ are polynomials given by:

$$f_1(A) = A^4 - 2A^3 + 2A^2 - (8c^2+1)A + 4c^2$$
$$f_2(A) = A^4 - 2A^3 + 2A^2 + (8c^2-1)A - 4c^2$$
$$f_3(A) = A^4 + 2A^3 + 2A^2 - (8c^2-1)A - 4c^2$$
$$f_4(A) = A^4 + 2A^3 + 2A^2 + (8c^2+1)A + 4c^2$$
$$f_5(A) = A^6 + A^4 + A^2 - 64c^4$$

We shall prove that for any $0 \neq c \in \mathbb{Q}$, all of these $f_i$ are irreducible, and in fact generate the same $S_4$ extension of $\mathbb{Q}$ (see Proposition 4.3.2 and Proposition 4.3.4). For the present, these facts are assumed.

THEOREM **4.3.1.** *Let $c \in \mathbb{Q}$, $c \neq 0$, and let $f_1(x) = x^4 - 2x^3 + 2x^2 - (8c^2+1)x + 4c^2$. Let $K/\mathbb{Q}$ be the splitting field of $f_1$. Let $\alpha$ be a root of $f_1$, and set $\beta = \frac{\alpha^4}{8c^2} - \frac{1}{2}$ and*

$$R = \Big(\alpha t + \beta,\ ct^2 + \frac{\alpha^3}{2c}t - c + \frac{3\alpha^2\beta}{2c} - \frac{8\alpha^6+1}{64c^3}\Big).$$

*Then $R \in E_{m_1(t)}\big(\overline{\mathbb{Q}}(t)\big)$, where $m_1(t) = ct^2 - \frac{64c^4+1}{64c^3}$. Moreover, if $R_1$, $R_2$, $R_3$, $R_4$ correspond to the four possible choices of $\alpha \in K$, then $R_1 + R_2 + R_3 + R_4 \in E_{m_1(t)}(\mathbb{Q}(t))$. The group $E_{m_1(t)}\big(\overline{\mathbb{Q}}(t)\big)$ has rank 6 and is generated by $P = (0, m_1)$, $Q = (1, m_1)$, $P_1 = \big(t + \frac{1}{8c^2}, ct^2 + \frac{1}{2c}t - \frac{64c^4-3}{64c^3}\big)$, and any three of the $R_i$'s.*

PROOF: The fact that $R \in E_{m_1(t)}\big(\overline{\mathbb{Q}}(t)\big)$ can be verified by direct computation. By Theorem 2.4.2, $E_{m_1(t)}\big(\overline{\mathbb{Q}}(t)\big)$ has rank 6 generated by 54 points (27 pairs of points) of the form $(x(t), y(t))$, where $deg(x) \leq 1$ and $deg(y) \leq 2$. For each of these points, if $x(t) = At + B$, then $A$ must be a root of (4.12). These 27 pairs of points were computed using `Pari`, and one member of each pair is given in

Table 4.1: Points of Minimal Norm on $E_{m_1(t)}\big(\overline{\mathbb{Q}}(t)\big)$ (see Theorem 4.3.1)

| | | | | |
|---|---|---|---|---|
| $A=0$ | $P=(0,m)$ | $-P-Q=(-1,m)$ | | $Q=(1,m)$ |
| $A=1$ | $P_1=\big(t+\frac{1}{8c^2}, ct^2+\frac{1}{2c}t-\frac{64c^4-3}{64c^3}\big)$ | | | |
| $A=-1$ | $P_1+P=\big(-t+\frac{1}{8c^2}, ct^2-\frac{1}{2c}t-\frac{64c^4-3}{64c^3}\big)$ | | | |
| $f_1(A)=0$ | $R_1$ | $R_2$ | $R_3$ | $R_4$ |
| $f_2(A)=0$ | $R_1-P-P_1$ | $R_2-P-P_1$ | $R_3-P-P_1$ | $R_4-P-P_1$ |
| $f_3(A)=0$ | $R_1+Q-P_1$ | $R_2+Q-P_1$ | $R_3+Q-P_1$ | $R_4+Q-P_1$ |
| $f_4(A)=0$ | $R_1+Q$ | $R_2+Q$ | $R_3+Q$ | $R_4+Q$ |
| $f_5(A)=0$ | $R_1+R_2+Q-P_1$ | | $R_1+R_3+Q-P_1$ | |
| | $R_1+R_4+Q-P_1$ | | $R_2+R_3+Q-P_1$ | |
| | $R_2+R_4+Q-P_1$ | | $R_3+R_4+Q-P_1$ | |

Table 4.1. For each factor of (4.12), the corresponding points are listed next to the factor. For example, $f_1(A)$ is one factor, and the points which have a root of $f_1(A)$ as the lead coefficient of their $x$ coordinate are $R_1$, $R_2$, $R_3$ and $R_4$. Since all 27 of these minimal points and their negatives are written in terms of the points $P$, $Q$, $P_1$, and the four $R_i$'s, this implies that these points generate $E_{m_1(t)}\big(\overline{\mathbb{Q}}(t)\big)$.

Let $S=R_1+R_2+R_3+R_4$, and let $\tau\in Gal(K/\mathbb{Q})$. Then $\tau$ permutes the $R_i$, and so must fix $S$. Since this is true for any $\tau$ in the Galois group, it follows that $S$ must lie in the fixed field of the Galois action, so $S\in E_{m_1(t)}(\mathbb{Q}(t))$. In fact, direct computation shows that $S=P-2Q+2P_1$, which gives the dependency relation:

$$R_1+R_2+R_3+R_4-P+2Q-2P_1=\infty. \tag{4.13}$$

This implies that $P$, $Q$, $P_1$, and any three of the four $R_i$'s generate the group $E_{m_1(t)}\big(\overline{\mathbb{Q}}(t)\big)$. ■

We now prove that $f_1, \ldots, f_4$ are irreducible and generate the same $S_4$ extension of $\mathbb{Q}$. First, note that $f_1(A) = f_2(1-A) = f_3(A-1) = f_4(-A)$. This shows that $f_1, \ldots, f_4$ all generate the same extension of $\mathbb{Q}$. Also, if $\alpha$ is a root of $f_1$ and $\sigma$ is any Galois element with $\alpha^\sigma \neq \alpha$, then $f_5(\alpha + \alpha^\sigma - 1) = 0$. Thus the splitting field of $f_5$ is contained in the splitting field of $f_1$. Now we prove that $f_1$ is irreducible, and that its splitting field is an $S_4$ extension of $\mathbb{Q}$. For convenience, we work with the linear shift of $f_1$ given by

$$f(x) = 16 f_1\Big(\frac{x+1}{2}\Big) = x^4 + 2x^2 - 64c^2x - 3.$$

PROPOSITION **4.3.2.** *Let $c \in \mathbb{Q}$, $c \neq 0$, and let $f(x) = x^4 + 2x^2 - 64c^2x - 3$. Then $f$ is irreducible over $\mathbb{Q}$.*

PROOF: First, suppose $f$ factors as a product of two quadratics, so

$$f(x) = x^4 + 2x^2 - 64c^2x - 3 = (x^2 + a_1x + a_2)(x^2 + b_1x + b_2).$$

Equating coefficients of $x^3$ and of $x^2$, we get that $b_1 = -a_1$, and that $b_2 = a_1^2 - a_2 + 2$. Equating the constant terms gives $a_2^2 - (a_1^2 + 2)a_2 - 3 = 0$. This quadratic polynomial in $a_2$ has a rational root if and only if its discriminant is a square: $(a_1^2 + 2)^2 + 12 = a_1^4 + 4a_1^2 + 16 = v^2$. This quartic has the rational point $(a_1, v) = (0, 4)$. Making the birational transformation $x = 2(v+4)/a_1^2$, $y = (8(v+4) + 4a_1^2)/a_1^3$ (with inverse transformation $a_1 = 4(x+1)/y$, $v = -4 + a_1^2x/2$) gives the elliptic curve $E$: $y^2 = x^3 + x^2 - 4x - 4$. This curve has conductor 48, and has rank 0. The only rational points on E are $(\pm 2, 0)$, $(-1, 0)$, and $\infty$. These points correspond to $(a_1, v) = (0, \pm 4)$ and the two points at infinity on the quartic, so these are the only rational points on the quartic. Thus $a_1 = 0$ is the only possibility for this factorization of $f(x)$, which leads to

$c = 0$, a contradiction. This implies that $f(x)$ cannot factor as a product of two quadratics.

Note that $f(x)$ cannot have 2 rational roots, otherwise it would factor as a product of two quadratics. The only remaining factorization of $f$ is for it to have one rational root and an irreducible cubic factor. In this case, rewrite $f(x) = 0$ as $64c^2x = x^4 + 2x^2 - 3$. Multiply through by $x$ and set $y = 64cx$ to get the genus 2 hyperelliptic curve:

$$y^2 = x^5 + 2x^3 - 3x = x(x-1)(x+1)(x^2+3) \tag{4.14}$$

By Faltings' Theorem, this can only have finitely many rational points, but in this case we can find them explicitly. A few are obvious: $(0,0)$, $(1,0)$, and $(-1,0)$. These last two of these come from $c = 0$, which cannot happen, and $(0,0)$ is an extraneous solution which comes from multiplying through by $x$.

Mirroring the method of descent on an elliptic curve, we set

$$x(x-1)(x+1) = dv^2 \tag{4.15}$$

$$x^2 + 3 = dw^2, \tag{4.16}$$

where $v, w \in \mathbb{Q}$ and $d$ is a squarefree integer. Let $p$ be a prime dividing $d$. We claim that $p$ must be either 2 or 3. Suppose that $p$ divides the denominator of $x$. Then the valuation $v_p(x^2+3)$ must be a negative even integer, but the valuation $v_p(dw^2)$ must be odd since $p|d$ and $d$ is squarefree. This cannot happen, so $p$ cannot divide the denominator of $x$, and $x$ can be considered as a $p$-adic integer. This implies that the denominators of $v$ and $w$ cannot be divisible by $p$ either. Reducing (4.15) mod $p$ implies that $x \equiv 0, 1, -1 \bmod p$. Substituting these into (4.16) gives $3 \equiv 0 \bmod p$ or $4 \equiv 0 \bmod p$. This implies that $p$ must be either 2 or 3, so the only possible values for $d$ are $\{\pm 1, \pm 2, \pm 3, \pm 6\}$.

For $d = \pm 1, \pm 2, \pm 3$, (4.15) is an elliptic curve of rank 0, and the only rational points have $x = 0, \pm 1$. These points correspond to the points on (4.14) that were already known. For $d = \pm 6$, the elliptic curve (4.15) has rank 1, but equation (4.16) has no 2-adic solutions, and hence no rational solutions. Therefore, we have already listed all rational points on (4.14). So $f(x)$ has no rational roots, and therefore is irreducible for all rational $c \neq 0$. ■

PROPOSITION **4.3.3.** *Let $f(x)$ be an irreducible polynomial of degree $n$ over a field $F$, and let $K$ be the splitting field of $f$. Then $Gal(K/F) \subseteq A_n$ if and only if $disc(f) = D$ is the square of an element of $F$.*

For a proof of this, see [DF, pp. 587-598].

PROPOSITION **4.3.4.** *Let $c \in \mathbb{Q}$, $c \neq 0$, and let $f(x) = x^4 + 2x^2 - 64c^2x - 3$. Let $K/\mathbb{Q}$ be the splitting field of $f$. Then $Gal(K/\mathbb{Q}) = S_4$.*

PROOF: Since $deg(f) = 4$, we have that $G = Gal(K/\mathbb{Q}) \subset S_4$. From the previous proposition, $f$ is irreducible. This implies that only conjugates of the following subgroups are possible [DF, pp. 587-598]:

$S_4$

$A_4$

$D_4 = \{1, (1234), (12)(34), (1432), (13)(24), (14)(23), (12), (34)\}$

$V = \{1, (12)(34), (13)(24), (14)(23)\}$ (the Klein 4-subgroup)

$C = \{1, (1234), (12)(34), (1432)\}$ (the cyclic group of order 4)

Since $disc(f) = D = -4096(110592c^8 + 896c^4 + 3) < 0$ can never be a square in $\mathbb{Q}$, we have that $G \not\subset A_4$ for any $c \in \mathbb{Q}$. The resolvent cubic of $f$ is $r(x) = x^3 - 4x^2 + 16x + 4096c^4$. This generates a subfield of $K$, so if this is

irreducible then order of $G = Gal(K/\mathbb{Q})$ must be divisible by 3, leaving $G = S_4$ as the only possibility. Note that a cubic polynomial is irreducible if it has no rational root, so it suffices to show that $r(x) = 0$ has no rational solutions. Suppose there exists a $c \neq 0$ for which $r$ has a rational root $x$. After the substitutions $v = 8c^2$ and $u = -x/4$, we get $v^2 = u^3 + u^2 + u$. This is an elliptic curve of conductor 48, which has rank 0. (Note that this elliptic curve is not isogenous to the one of conductor 48 in the proof of Proposition 4.3.2.) The only finite rational point is $(u, v) = (0, 0)$, which comes from $c = 0$. Thus $r(x)$ is irreducible for all $c \in \mathbb{Q}$ except $c = 0$, and so $Gal(K/\mathbb{Q}) = S_4$. ■

Using these facts, we can prove the following:

THEOREM **4.3.5.** *Let $c \in \mathbb{Q}$, $c \neq 0$, and let $m_1 = ct^2 - \frac{64c^4+1}{64c^3}$. Then $E_{m_1}(\mathbb{Q}(t))$ has rank 3, generated by the points $P = (0, m_1)$, $Q = (1, m_1)$ and $P_1 = \big(t + \frac{1}{8c^2}, ct^2 + \frac{1}{2c}t - \frac{64c^4-3}{64c^3}\big)$.*

PROOF: From Theorem 4.3.1, we know that $P$, $Q$, $P_1$, $R_1$, $R_2$ and $R_3$ form a basis for $E_{m_1(t)}\big(\overline{\mathbb{Q}}(t)\big)$. Suppose that some linear combination of $R_1$, $R_2$ and $R_3$ is in $E_{m_1(t)}(\mathbb{Q}(t))$, so we have

$$S = a_1R_1 + a_2R_2 + a_3R_3 \in E_{m_1(t)}(\mathbb{Q}(t)) \tag{4.17}$$

By Proposition 4.3.4, the Galois group $Gal(K/\mathbb{Q})$ is transitive on the $R_i$'s, so there exists $\sigma \in Gal(K/\mathbb{Q})$ such that ${R_1}^\sigma = R_2$, ${R_2}^\sigma = R_1$, and $\sigma$ fixes $R_3$ and $R_4$. Then $\sigma$ fixes $S$, and subtracting gives

$$O = S - S^\sigma = (a_1 - a_2)R_1 + (a_2 - a_1)R_2 = (a_1 - a_2)(R_1 - R_2)$$

Notice that $R_1 \neq R_2$ since the leading coefficients of the $x$ coordinates are distinct. Since there is no torsion in $E_{m_1(t)}\big(\overline{\mathbb{Q}}(t)\big)$, it follows that $a_1 = a_2$ and similarly

that $a_1 = a_2 = a_3 = a$. From (4.13), we have

$$S = a(R_1 + R_2 + R_3) = a(P - 2Q + 2P_1 - R_4) \in E_{m_1(t)}(\mathbb{Q}(t)).$$

Since $S$, $P$, $Q$ and $P_1$ are rational, it follows that $aR_4$ must be rational.

Let $\tau \in Gal(K/\mathbb{Q})$ have nontrivial action on $R_4$, say ${R_4}^\tau = R_1$. Then since $aR_4$ is rational, we have

$$O = aR_4 - (aR_4)^\tau = aR_4 - a(R_4)^\tau = a(R_4 - R_1)$$

Since $R_4 \neq R_1$, it follows that $a = 0$. This gives $S = O$ is the only linear combination of $R_1$, $R_2$ and $R_3$ which is rational, so $E_{m_1(t)}(\mathbb{Q}(t))$ must be generated by $P$, $Q$ and $P_1$. ■

All of the results thus far have been restricted to the $m_1(t)$ case. Analogous results for the $m_2(t)$ and $m_3(t)$ case can be proved using the same techniques. These are not stated here.

In Section 4.2, we found quadratic $m(t)$ such that $E_{m(t)}$ contains an additional rational generator $(x(t), y(t))$ with $deg(x) \leq 1$ and $deg(y) \leq 2$. This process exhausted every possible case with a third rational generator satisfying these inequalities, which leads to the following:

CONJECTURE **4.3.6.** *Let $m(t) \in \mathbb{Q}[t]$ by a quadratic polynomial. Then the rank of $E_{m(t)}(\mathbb{Q}(t))$ is either 2 or 3. The rank is 3 if and only if $m(t)$ meets the criteria of Theorem 4.2.1.*

The only way that this conjecture is false is if there exists a quadratic polynomial $m(t)$ with the following properties:

- $m(t)$ cannot be changed into one of the $m_i(t)$ polynomials by a linear shift of $t$, and

- some nontrivial linear combination of the four non-rational generators of $E_{m(t)}\big(\overline{\mathbb{Q}}(t)\big)$ must add up to a rational point.

## 4.4 Cubic Subfamilies

Suppose we wish to find cubic subfamilies of $E_m$ which have higher rank. If $m(t)$ is cubic in $t$, then $E_{m(t)}$ is still a rational elliptic surface. By Theorem 2.4.3, the generators of $E_{m(t)}\big(\overline{\mathbb{Q}}(t)\big)$ are points of the form $(x(t), y(t))$ where $deg(x) \leq 2$ and $deg(y) \leq 3$. Much like in Section 4.2, the parameterization given by (4.2) and (4.3) can be used to search for cubic $m(t)$ where $E_{m(t)}$ has an extra point of the appropriate form with rational coefficients. The parameterization (4.2) of $m$ in terms of $x$ and $u$ is repeated here for convenience:

$$m(x,u) = \frac{x^3 - x}{2u} - \frac{u}{2} \tag{4.18}$$

Given that $m(t)$ is a polynomial of degree 3, this places restrictions on the choices of $x$ and $u$. Since $m(t)$ and $y(t)$ are both polynomials, $u = y(t) - m(t)$ must also be a polynomial. Moreover, $u$ must divide $x^3 - x$ to force $m(t)$ and $y(t)$ to be polynomial in $t$.

If $deg(x) = 0$ and $x \neq \pm 1$, then $u$ must also be a constant since $u|x^3 - x$. This forces $m(t)$ to be constant rather than cubic, which is not the desired case. We are left with the following cases:

A. $deg(x) = 1$.

B. $deg(x) = 2$ and one of $x$, $x-1$, $x+1$ divides $u$.

C. $deg(x) = 2$ and none of $x$, $x-1$, $x+1$ divides $u$.

**Case A:** Suppose $deg(x) = 1$. If $deg(u) = 1, 2$ and $u|x^3 - x$, then $m(t)$ is quadratic. This leaves $deg(u) = 0, 3$. Suppose $deg(u) = 0$ and let $u' = (x^3 - x)/u$. Then $deg(u') = 3$. Moreover, by the symmetry (4.6), $u$ and $u'$ generate the same solution (up to the sign of $m(t)$). Thus we only need to consider $deg(u) = 0$. Since $deg(x) = 1$, we can perform a linear shift so that $x = 2ut$. Substituting into (4.18) gives

$$m_A = 4u^2t^3 - t - \frac{u}{2}$$

which yields $E_{m_A}$ with the additional point $P_A = (2ut, 4u^2t^3 - t + u/2)$.

**Case B:** When $x(t)$ is quadratic in $t$, the situation is much more complicated. The degree of $x^3 - x$ is 6, so we must have $deg(u) = 3$ in order for $m(t)$ to have degree 3. Since $u$ must divide $x(x-1)(x+1)$ and each of $x$, $x-1$ and $x+1$ have degree 2, at least one of these quadratics must factor into two linear terms. With a linear shift of $t$, the term that factors can be written as either $a(t-1)(t+1)$ or $at^2$. Then $u$ must have a linear factor from this term and a quadratic factor from one of the other terms. (The case where $u$ has one linear factor from each of the three quadratic terms is Case C.) This gives three cases depending on which term factors, and each of these gives two cases depending on whether or not the quadratic that factors happens to be a perfect square.

Here are the cases. In each case, the $x$-coordinate of the additional point is specified, and the $y$-coordinate can be calculated from $x$ and $u$ using (4.3).

1a. $x = a(t-1)(t+1)$. Take $u = k(t-1)(x-1) = k(t-1)(a(t^2-1)-1)$.

$$\begin{aligned} m_{1a} &= \frac{a(a-k^2)}{2k}t^3 + \frac{a(a+k^2)}{2k}t^2 - \frac{a^2-(k^2+1)a-k^2}{2k}t \\ &\quad -\frac{a^2+(k^2-1)a+k^2}{2k} \end{aligned}$$

Similarly, choosing $u = k(t+1)(x-1)$, $u = k(t-1)(x+1)$ or $u = k(t+1)(x+1)$ produces the same results up to a change in the sign of $t$ or the sign of $m_{1a}$. This same phenomenon occurs in cases 2a and 3a below.

1b. $x = at^2$. Take $u = kt(x-1) = kt(at^2-1)$.

$$m_{1b} = \frac{a(a-k^2)}{2k}t^3 + \frac{a+k^2}{2k}t$$

Similarly, choosing $u = kt(x+1)$ produces the same results up to changing the sign of $m_{1b}$. This same phenomenon occurs in cases 2b and 3b below.

2a. $x - 1 = a(t-1)(t+1)$. Take $u = k(t-1)x = k(t-1)(a(t^2-1)+1)$.

$$\begin{aligned} m_{2a} &= \frac{a(a-k^2)}{2k}t^3 + \frac{a(a+k^2)}{2k}t^2 - \frac{a^2-(k^2+2)a+k^2}{2k}t \\ &\quad - \frac{a^2+(k^2-2)a-k^2}{2k} \end{aligned}$$

2b. $x - 1 = at^2$. Take $u = ktx = kt(at^2+1)$.

$$m_{2b} = \frac{a(a-k^2)}{2k}t^3 + \frac{2a-k^2}{2k}t$$

3a. $x + 1 = a(t-1)(t+1)$. Take $u = k(t-1)x = k(t-1)(a(t^2-1)-1)$.

$$\begin{aligned} m_{3a} &= \frac{a(a-k^2)}{2k}t^3 + \frac{a(a+k^2)}{2k}t^2 - \frac{a^2-(k^2-2)a-k^2}{2k}t \\ &\quad - \frac{a^2+(k^2+2)a+k^2}{2k} \end{aligned}$$

3b. $x + 1 = at^2$. Take $u = ktx = kt(at^2-1)$.

$$m_{3b} = \frac{a(a-k^2)}{2k}t^3 - \frac{2a-k^2}{2k}t$$

REMARK **4.4.1.** Some of these expressions are rather complicated. They all simplify nicely in the case where $a = -k^2$. Even the coordinates of the additional

point simplify nicely. After making the change of variables $t \to t/k$, we are left with:

$$\begin{aligned}
m_{1a'} &= t^3 - k^2 t - k & P_{1a'} &= (-t^2 + k^2, kt^2 - t - k^3) \\
m_{1b'} &= t^3 & P_{1b'} &= (-t^2, -t) \\
m_{2a'} &= t^3 - \Big(k^2 + \frac{3}{2}\Big)t - \frac{1}{2}k & P_{2a'} &= \Big( - t^2 + k^2 + 1, kt^2 - \frac{1}{2}t - k^3 - \frac{3}{2}k\Big) \\
m_{2b'} &= t^3 - \frac{3}{2}t & P_{2b'} &= \Big( - t^2 + 1, -\frac{1}{2}t\Big) \\
m_{3a'} &= t^3 - \Big(k^2 - \frac{3}{2}\Big)t + \frac{1}{2}k & P_{3a'} &= \Big( - t^2 - k^2 - 1, kt^2 + \frac{1}{2}t - k^3 + \frac{3}{2}k\Big) \\
m_{3b'} &= t^3 + \frac{3}{2}t & P_{3b'} &= \Big( - t^2 - 1, \frac{1}{2}t\Big)
\end{aligned}$$

Note that 1b' here is the negative of the point given in Proposition 4.1.3 at the beginning of this chapter. □

**Case C:** The only remaining case is where each of $x$, $x-1$, and $x+1$ factor, and $u$ contains one linear term from each. Using the same reasoning as above, $x$ can be written in the form $a(t-1)(t+1)$ or $at^2$. In fact, $x = at^2$ cannot happen because both $x-1$ and $x+1$ must factor, and one of these will have negative discriminant. This implies that $x = a(t-1)(t+1)$, $x - 1 = at^2 - a - 1$ and $x + 1 = at^2 - a + 1$, and both of these must factor as well. Thus $t^2 - (1 + \frac{1}{a}) = (t - v)(t + v)$, which means that $\frac{1}{a} = v^2 - 1$. Also, $t^2 - (1 - \frac{1}{a}) = (t - w)(t + w)$, so $\frac{1}{a} = 1 - w^2$. Setting these equal to each other gives $v^2 + w^2 = 2$, which has solutions parameterized by

$$v = \frac{z^2 - 2z - 1}{z^2 + 1} \qquad \text{and} \qquad w = \frac{-z^2 - 2z + 1}{z^2 + 1}.$$

This implies that

$$a = \frac{-z^4 - 2z^2 - 1}{4z^3 - 4z}.$$

Now $u$ contains a linear factor from each of $x$, $x-1$, and $x+1$, so choose $u = k(t-1)(t-v)(t-w)$. Actually, any choice of one factor from each term produces equivalent results, as in Case B above. The parameterization (4.18) gives

$$\begin{aligned} m_C &= \Big(\frac{a^3}{2k} - \frac{1}{2}k\Big)t^3 + \frac{z^2-4z+1}{z^2+1}\Big(\frac{a^3}{2k} + \frac{1}{2}k\Big)t^2 \\ &\quad - \frac{z^4+4z^3-6z^2+4z+1}{(z^2+1)^2}\Big(\frac{a^3}{2k} - \frac{1}{2}k\Big)t + vw\Big(\frac{a^3}{2k} + \frac{1}{2}k\Big) \end{aligned}$$

where $a$, $v$ and $w$ are all in terms of $z$ as above.

REMARK **4.4.2.** In all of the B cases above, the results could be simplified significantly if we could set $a = -k^2$. However, this cannot happen here. Since

$$a = \frac{-(z^2+1)^2}{4(z^3-z)}$$

the only way that $-a$ can be a square is if the denominator $z^3 - z$ is a square, which implies that $y^2 = z^3 - z$ must have a rational solution with $y \neq 0$. This is an elliptic curve with rank 0 whose only finite rational points are the three 2-torsion points $(0,0)$ and $(\pm 1, 0)$. Thus $-a$ cannot be a square in this case. □

Here we have exhausted every possible way to obtain an extra rational point on $E_{m(t)}(\mathbb{Q}(t))$ where $m(t)$ is a cubic polynomial and the extra point is of the form $(x(t), y(t))$ where $deg(x) \leq 2$ and $deg(y) \leq 3$. This leads one to believe the following:

CONJECTURE **4.4.3.** *Let $m(t) \in \mathbb{Q}[t]$ by a cubic polynomial. Then the rank of $E_{m(t)}(\mathbb{Q}(t))$ is 3 or more if and only if a linear shift of $m(t)$ meets the criteria of either A, B, or C above. Otherwise the rank of $E_{m(t)}(\mathbb{Q}(t))$ is 2.*

The steps above were used to construct a point on $E_{m(t)}(\mathbb{Q}(t))$ other than $P = (0, m(t))$ and $Q = (1, m(t))$. In every case investigated thus far, these 3

points have been independent. However, we do not have a general proof of this yet.

Also, we have not been able to rule out the possibility that there exists a cubic polynomial $m(t)$ for which no linear shift meets the criteria of A, B, or C above, and some combination of the non-rational generators forms a rational point.

# Chapter 5: Lifts In Another Family

The lifting process demonstrated above is not unique to the family $E_m$. Let $C_m$ be the family of elliptic curves given by

$$y^2 = x^3 - m^2x + 1. \tag{5.1}$$

This chapter examines how lifts work in the $C_m$ family.

## 5.1 Generators for $C_m$

As with the curve $E_m$ studied earlier, there are several obvious points on $C_m$, including $(0, 1)$, $(m, 1)$ and $(-1, m)$. These points actually generate the group $C_m(\mathbb{Q}(m))$:

THEOREM **5.1.1.** *Let $\omega$ be a primitive third root of unity, so $\omega^2 + \omega + 1 = 0$. Then the group $C_m\big(\overline{\mathbb{Q}}(m)\big)$ is generated by the points $P_1 = (0, 1)$, $P_2 = (m, 1)$, $P_3 = (-1, m)$ and $P_4 = (-\omega, \omega^2 m)$. Moreover, the group $C_m(\mathbb{Q}(m))$ is generated by $P_1$, $P_2$ and $P_3$.*

PROOF: By Theorem 2.4.4, $C_m$ has rank 4 over $\overline{\mathbb{Q}}(m)$ generated by 24 points (12 pairs of points) of the form $(x(m), y(m))$ where $deg(x) \leq 1$ and $deg(y) \leq 1$. These 24 points are listed in Table 5.1 along with their relations. Thus $P_1$, $P_2$, $P_3$ and $P_4$ generate $C_m\big(\overline{\mathbb{Q}}(m)\big)$.

Table 5.1: Minimal Points on $C_m : y^2 = x^3 - m^2x + 1$

| $deg(x) = 0$ | $deg(x) = 1$ |
|---|---|
| $P_1 = (0, 1)$ | $P_2 = (m, 1)$ |
| $P_3 = (-1, m)$ | $-P_1 - P_2 = (-m, 1)$ |
| | $P_1 + P_2 - P_3 = (m + 2, 2m + 3)$ |
| | $P_2 - P_3 = (-m + 2, 2m - 3)$ |
| $P_4 = (-\omega, \omega^2 m)$ | $P_1 + P_2 - P_4 = (m + 2\omega, 2\omega^2 m + 3)$ |
| | $P_2 - P_4 = (-m + 2\omega, 2\omega^2 m - 3)$ |
| $P_1 + 2P_2 - P_3 - P_4$ | $-P_2 + P_3 + P_4 = (m + 2\omega^2, 2\omega m + 3)$ |
| $= (-\omega^2, \omega m)$ | $-P_1 - P_2 + P_3 + P_4 = (-m + 2\omega^2, 2\omega m - 3)$ |

Here $\omega^2 + \omega + 1 = 0$, so $\omega$ is a primitive third root of unity

It is obvious that $C_m(\mathbb{Q}(m))$ contains the points $P_1$, $P_2$ and $P_3$ and so has rank at least 3. It is also clear that $P_4 \notin C_m(\mathbb{Q}(m))$. All that remains to be shown is that no power of $P_4$ can be in $C_m(\mathbb{Q}(m))$. If such a power does exist, say $aP_4 \in C_m(\mathbb{Q}(m))$ for some $a \in \mathbb{Z}$, then it must be fixed by the Galois action. In particular, if $\sigma$ is the nontrivial element of the Galois group $Gal(\mathbb{Q}(\omega)/\mathbb{Q})$, then $aP_4 = (aP_4)^\sigma = a({P_4}^\sigma)$, so $a(P_4 - {P_4}^\sigma) = O$. Since this curve has no torsion, it follows that $P_4 = {P_4}^\sigma$, which implies that $P_4 \in C_m(\mathbb{Q}(m))$, giving a contradiction. Thus $P_1$, $P_2$ and $P_3$ generate $C_m(\mathbb{Q}(m))$. ■

As the case with $E_m$, Table 5.2 shows that there are many values of $m$ for which the rank of $C_m(\mathbb{Q})$ is larger than 3. (See Appendix B for more details.) Thus it seems reasonable to believe that the lifting process may work in a similar manner (see Theorem 3.4.1).

Table 5.2: Classification of $C_m$ by Rank for $m = 1, \ldots, 500$

| Rank | First few $m$ where $C_m$ has this rank | $\#m \leq 500$ |
|---|---|---|
| 1 | 1 | 1 |
| 2 | 2, 3 | 2 |
| 3 | 4, 5, 6, 7, 9, 10, 11, 12, 15, 18, ... | 121 |
| 4 | 8, 13, 14, 16, 19, 20, 22, 23, 26, 27, ... | 209 |
| 5 | 17, 25, 36, 41, 42, 46, 53, 59, 70, 73, ... | 135 |
| 6 | 61, 107, 124, 128, 146, 148, 178, 199, 253, 262, ... | 30 |
| 7 | 347, 443, ... | 2 |

## 5.2 Lifting A Point On $C_m$

Before attempting to prove that every point on $C_m$ has a lift, we first give an example of a lift. The first positive integer such that $C_m$ has rank 4 is $m = 8$. The group $C_8(\mathbb{Q})$ is generated by the points $P_1 = (0, 1)$, $P_2 = (8, 1)$, $P_3 = (-1, 8)$ and $Q = (12, 31)$. Here we show that there exists a quadratic subfamily of $C_m$ which contains a lift of the point $Q$.

PROPOSITION **5.2.1.** *Let*

$$M(t) = \frac{2}{75}t^2 + t + 8$$
$$Q(t) = \Big(\frac{4}{75}t^2 + \frac{8}{5}t + 12,\ \frac{4}{375}t^3 + \frac{34}{75}t^2 + \frac{32}{5}t + 31\Big).$$

*Then $C_{M(t)}(\mathbb{Q}(t))$ has rank at least 4, with independent points $P_1(t) = (0, 1)$, $P_2(t) = (M(t), 1)$, $P_3(t) = (-1, M(t))$ and $Q(t)$. This is a lift of the point $(12, 31) \in C_8(\mathbb{Q})$.*

PROOF: Direct computation verifies that $P_i(t), Q(t) \in C_{M(t)}(\mathbb{Q}(t))$. To show that these points are independent, specialize to $t = 0$. This gives the four points

$P_1(0) = (0, 1)$, $P_2(0) = (8, 1)$, $P_3(0) = (-1, 8)$ and $Q(0) = (12, 31)$ listed above, which are independent on $C_8(\mathbb{Q})$. By Proposition 2.5.2, the points $P_i(t), Q(t)$ must be independent in $C_{M(t)}(\mathbb{Q}(t))$. ■

Given that such a lift exists, how does one go about finding it? Suppose that $M(t) \in \mathbb{Q}(t)$ is quadratic. By Theorem 2.4.5, the generators of $C_{M(t)}\big(\overline{\mathbb{Q}}(t)\big)$ have the form $(x(t), y(t))$ where $deg(x) \leq 2$ and $deg(y) \leq 3$. Thus a lift of the point $(12, 31) \in C_8(\mathbb{Q})$ to a point over $\mathbb{Q}(t)$ should have the form

$$M(t) = At^2 + Bt + 8 \qquad R(t) = (x_2t^2 + x_1t + 12,\ y_3t^3 + y_2t^2 + y_1t + 31).$$

Substituting this into the equation (5.1) for $C_m$ gives the following 6 relations from the coefficients of $t^1$ through $t^6$ in 7 unknowns:

$$62y_1 = -192B + 368x_1 \tag{$t^1$}$$

$${y_1}^2 + 62y_2 = 36{x_1}^2 - 16Bx_1 + 368x_2 - 192A - 12B^2 \tag{$t^2$}$$

$$2y_2y_1 + 62y_3 = {x_1}^3 + 72x_1x_2 - 16Ax_1 - B^2x_1 - 16Bx_2 - 24AB \tag{$t^3$}$$

$$2y_3y_1 + {y_2}^2 = 3{x_1}^2x_2 - 2ABx_1 + 36{x_2}^2 - 16x_2A - x_2B^2 - 12A^2 \tag{$t^4$}$$

$$2y_3y_2 = 3x_1{x_2}^2 - A^2x_1 - 2ABx_2 \tag{$t^5$}$$

$${y_3}^2 = {x_2}^3 - A^2x_2 \tag{$t^6$}$$

Note that the coefficient of $t^0$ vanishes since we have $(12, 31) \in C_8(\mathbb{Q})$. Comparing this with the analogous situation for $E_m$ in Section 3.3, it is immediately obvious that things are now much more complicated since there are more unknowns and more relations. However, it is still possible to proceed.

If $B = 0$, this forces all of the other coefficients to be 0, which does not really give a lift. Thus we can assume that $B \neq 0$. Notice that a linear shift of $t$ would

affect the constant terms, but changing $t$ by a constant multiple would not. This can be used to make $B = 1$. Now there are 6 relations and 6 unknowns. Solving $(t^1)$ for $y_1$, $(t^2)$ for $y_2$ and $(t^3)$ for $y_3$ gives:

$$\begin{aligned}
y_1 &= \frac{184}{31}x_1 - \frac{96}{31} \\
y_2 &= -\frac{96}{31}A + \frac{184}{31}x_2 + \frac{370}{31^3}x_1^2 + \frac{9976}{31^3}x_1 - \frac{10374}{31^3} \\
y_3 &= \frac{9976}{31^3}x_1A - \frac{20748}{31^3}A + \frac{740}{31^3}x_1x_2 + \frac{9976}{31^3}x_2 + \frac{787361}{2\cdot 31^5}x_1^3 - \frac{1800064}{31^5}x_1^2 \\
&\quad + \frac{4809503}{2\cdot 31^5}x_1 - \frac{995904}{31^5}
\end{aligned}$$

Substituting these into $(t^4)$ through $(t^6)$ leaves 3 polynomial relations in 3 unknowns, namely $A$, $x_1$ and $x_2$. Let $p_n$ denote the result of substituting the $y_i$'s into the relation $(t^n)$. None of these relations are linear, but resultants can be used to find solutions. The basic process is to compute resultants as follows:

$$R_1 = res_A(p_4, p_5)$$

$$R_2 = res_A(p_4, p_6)$$

$$R_3 = res_{x_2}(R_1, R_2)$$

where $res_v(p_i, p_j)$ denotes the resultant of the polynomials $p_i$ and $p_j$ with respect to the variable $v$. Then $R_1$ and $R_2$ are polynomials in $x_1$ and $x_2$, and $R_3$ is a polynomial in $x_1$ (of degree 60). Using `Pari` to factor $R_3$ gives 6 linear factors, 9 irreducible quadratic factors, and two higher degree irreducible factors of degrees 6 and 30. Since rational points are desired here, only the 6 linear factors are used. These give 6 distinct rational values of $x_1$, each of which can be substituted back into $R_1$ and $R_2$ to find $x_2$ and into the $p_n$'s to find $A$. This gives 6 lifts of the point $(12, 31)$ on $C_8$, which are listed in Table 5.3.

Each row of Table 5.3 gives a subfamily $C_{M(t)}$ that has four independent points $P_1 = (0, 1)$, $P_2 = (M(t), 1)$, $P_3 = (-1, M(t))$ and $R(t)$ in $C_{M(t)}(\mathbb{Q}(t))$. The first

Table 5.3: Lifts of the point $(12, 31)$ on $C_8$

| $M(t) = At^2 + t + 8$ | $R(t) = (x_2t^2 + x_1t + 12, y_3t^3 + y_2t^2 + y_1t + 31)$ |
|---|---|
| $\frac{2}{75}t^2 + t + 8$ | $(\frac{4}{75}t^2 + \frac{8}{5}t + 12, \frac{4}{375}t^3 + \frac{34}{75}t^2 + \frac{32}{5}t + 31)$ |
| $\frac{6}{13^2}t^2 + t + 8$ | $(\frac{18}{13^2}t^2 + \frac{27}{13}t + 12, \frac{72}{13^3}t^3 + \frac{12}{13}t^2 + \frac{120}{13}t + 31)$ |
| $\frac{210}{89^2}t^2 + t + 8$ | $(\frac{490}{89^2}t^2 + \frac{161}{89}t + 12, \frac{9800}{89^3}t^3 + \frac{4620}{89^2}t^2 + \frac{680}{89}t + 31)$ |
| $\frac{5814}{559^2}t^2 + t + 8$ | $(\frac{6498}{559^2}t^2 + \frac{665}{559}t + 12, \frac{233928}{559^3}t^3 + \frac{41724}{559^2}t^2 + \frac{2216}{559}t + 31)$ |
| $\frac{155610}{1433^2}t^2 + t + 8$ | $(\frac{212940}{1433^2}t^2 + \frac{2392}{1433}t + 12, \frac{67076100}{1433^3}t^3 + \frac{1285830}{1433^2}t^2 + \frac{9760}{1433}t + 31)$ |
| $\frac{101010}{2267^2}t^2 + t + 8$ | $(\frac{112554}{2267^2}t^2 + \frac{2691}{2267}t + 12, \frac{16657992}{2267^3}t^3 + \frac{698412}{2267^2}t^2 + \frac{8952}{2267}t + 31)$ |

row is the same as the lift in Proposition 5.2.1. To verify the independence, specialize to $t = 0$. In each of the 6 cases, this gives $M(0) = 8$ and the four points $(0, 1)$, $(8, 1)$, $(-1, 8)$ and $R(0) = (12, 31)$. These are independent in $C_8(\mathbb{Q})$ since the determinant of the height matrix for these four points is nonzero. By Proposition 2.5.2, the four points $P_1 = (0, 1)$, $P_2 = (M(t), 1)$, $P_3 = (-1, M(t))$ and $R(t)$ are independent in $C_{M(t)}(\mathbb{Q}(t))$ for each of the 6 cases.

The major differences between the results here and the lifts on $E_m$ are the number of relations and the number of unknowns. With fewer unknowns in the $E_m$ case, things just work out much nicer. For example, the top coefficient $(t^4)$ in the $E_m$ case is $A^2 - {y_2}^2$, which has the rather nice solutions $A = y_2$ and $A = -y_2$. In the $C_m$ case, the top coefficient $(t^6)$ is ${y_3}^2 = {x_2}^3 - A^2x_2$, which is itself a family of elliptic curves. These are the congruent number curves [K, Ch. 1].

## 5.3 Parameterizing Points on $C_m$

In Section 4.1, the curve $E_m$ was rearranged into a very nice form (4.1) which allowed for the parameterization of $y$ and $m$ in terms of $x$ and an additional parameter $u$. The curve $C_m$ again has an analogous result, but as above the situation is a bit more complicated.

Consider the equation (5.1) for $C_m$ in terms of the variables $y$ and $m$, with $x$ treated as a fixed constant:

$$y^2 + xm^2 = x^3 + 1 \tag{5.2}$$

This is now a quadratic equation for each $x$, and any one solution $(y_0, m_0)$ for a given $x_0$ can be used to parameterize all solutions $(y, m)$ for $x_0$. Fortunately, for every $x$, there is a solution $(y, m) = (1, x)$. Making the substitution

$$y = k(m - x) + 1 \tag{5.3}$$

leads to the parameterization

$$m(x, k) = \frac{xk^2 - 2k - x^2}{k^2 + x} \tag{5.4}$$

$$y(x, k) = \frac{-k^2 - 2x^2k + x}{k^2 + x} \tag{5.5}$$

This parameterization for $C_m$ is not nearly as nice as the one for $E_m$ given by (4.2) and (4.3). There were obvious symmetries in the $E_m$ parameterization, and none appear to be obvious here. Thus the task of constructing lifts is much more difficult.

Suppose we wish to use this parameterization to find $m(x, k)$ such that $C_{m(x,k)}$ contains an additional rational generator, where $m(x, k)$ is a quadratic polynomial in $t$. By Theorem 2.4.5, we search for points $(x(t), y(t))$ that have $deg(x) \leq 2$ and

$deg(y) \leq 3$. But what form should $k$ have as a function of $t$ to make $m(x(t), k(t))$ be a quadratic polynomial in $t$? It is not clear that this is even possible. From (5.3), it seems like a good choice would be to take $k(t)$ as a linear polynomial. However, $k(t)$ could also be a rational polynomial with numerator of degree 3 and denominator of degree 2. This case becomes much too complicated, so the only case considered here is where $k(t)$ is linear. In this case, a linear shift of $t$ can make $k(t) = t$. Set $x(t) = x_2t^2 + x_1t + x_0$, substitute into $m(x(t), k(t))$, and perform the long division to compute the quotient and remainder:

$$\begin{aligned} & m(x(t), t) \\ = \; & \frac{-x_2(x_2-1)t^4 - x_1(2x_2-1)t^3 - (2x_0x_2 + x_1^2 - x_0)t^2 - 2(x_0x_1+1)t - x_0^2}{(x_2+1)t^2 + x_1t + x_0} \\ = \; & \frac{-x_2(x_2-1)}{x_2+1}t^2 - \frac{x_1(x_2^2+2x_2-1)}{(x_2+1)^2}t - \frac{x_0(x_2^3+3x_2^2+x_2-1)+2x_1^2}{(x_2+1)^3} \\ & \quad - \frac{2((x_2+1)^3 + 2x_0x_1(x_2+1) - x_1^3)t + 2(x_0^2(x_2+1) - x_0x_1^2)}{(x_2+1)^3((x_2+1)t^2 + x_1t + x_0)} \end{aligned}$$

To make $m$ be a polynomial in $t$, the remainder term above must be zero. This gives

$$(x_2+1)^3 + 2x_0x_1(x_2+1) - x_1^3 = 0$$

$$x_0^2(x_2+1) - x_0x_1^2 = 0.$$

Computing the resultant of these two polynomials with respect to $x_0$ gives

$$(x_2+1)\big((x_2+1)^3 - x_1^3\big)\big((x_2+1)^3 + x_1^3\big) = 0.$$

The only rational solutions to this are $x_2+1 = 0$ and $x_2+1 = \pm x_1$, giving several cases:

(1.) $x_2 + 1 = -x_1 \neq 0$. This leads to $x_0 = -x_1$. Setting $c = x_1$ gives $x(t) = (-c-1)t^2 + ct - c$, giving a quadratic family of lifts parameterized by $c$ as

follows:

$$m(t) = \frac{(c+2)(c+1)}{c}t^2 - \frac{c^2-2}{c}t + c \tag{5.6}$$

$$(x,y) = \Big((-c-1)t^2+ct-c,\ \frac{2(c+1)^2}{c}t^3 - \frac{2(c-1)(c+1)}{c}t^2+2ct+1\Big) \tag{5.7}$$

This is a lift of the point $(-c,1) \in C_c(\mathbb{Q})$.

(2.) $x_2 + 1 = x_1 \neq 0$. This leads to $x_0 = 0$. Making the substitution $c = -\frac{2}{x_1}$ gives:

$$m(t) = \frac{(c+2)(c+1)}{c}t^2 - \frac{c^2-2}{c}t + c \tag{5.8}$$

$$(x,y) = \Big(\big(-\frac{2}{c}-1\big)t^2 - \frac{2}{c}t,\ \frac{c^2+4c+4}{c}t^3 - \frac{c^2-4}{c}t^2 + ct + 1\Big) \tag{5.9}$$

This is a lift of the point $(0,1) \in C_c(\mathbb{Q})$.

(3.) $x_2 = -1$ and $x_1 \neq 0$. This actually makes the leading term in the denominator of $m(x(t),t)$ vanish, and the polynomial division above must be redone.

$$\begin{aligned} m(x(t),t) &= \frac{-2t^4 + 3x_1t^3 + (3x_0 - x_1^2)t^2 - 2(x_0x_1+1)t - x_0^2}{x_1t + x_0} \\ &= -\frac{2}{x_1}t^3 + \frac{3x_1^2+2x_0}{x_1^2}t^2 - \frac{x_1^4+2x_0^2}{x_1^3}t - \frac{x_0x_1^4+2x_1^3-2x_0^3}{x_1^4} \\ &\quad + \frac{2x_0(x_1^3-x_0^3)}{x_1^4(x_1t+x_0)} \end{aligned}$$

The last term here must vanish to make $m(t)$ a polynomial, which gives the cases $x_1 = x_0$ and $x_0 = 0$:

(a.) $x_1 = x_0 = -c$. This gives $x(t) = -t^2 - ct - c$, which gives the lift

$$m(t) = \frac{2}{c}t^3 + \frac{3c-2}{c}t^2 + \frac{c^2+2}{c}t + c$$

$$(x,y) = \Big(-t^2 - ct - c,\ \frac{2}{c}t^4 + \frac{4c-2}{c}t^3 + \frac{2c^2+2}{c}t^2 + 2ct + 1\Big)$$

This is a (cubic) lift of the point $(-c,1) \in C_c(\mathbb{Q})$.

(b.) $x_0 = 0$, so we set $c = -\frac{2}{x_1}$. This gives the lift

$$m(t) = ct^3 + 3t^2 + \frac{2}{c}t + c$$

$$(x, y) = \Big( -t^2 - \frac{2}{c}t,\ ct^4 + 4t^3 + \frac{4}{c}t^2 + ct + 1 \Big)$$

This is a (cubic) lift of the point $(0, 1) \in C_c(\mathbb{Q})$.

(4.) $x_2 = -1$ and $x_1 = 0$. Now the denominator of $m(x(t), t)$ is reduced to just $x_0$, giving a quartic lift. Setting $c = -x_0$ gives:

$$m(t) = \frac{2}{c}t^4 + 3t^2 + \frac{2}{c}t + c$$

$$(x, y) = \Big( -t^2 - c,\ \frac{2}{c}t^5 + 4t^3 + \frac{2}{c}t^2 + 2ct + 1 \Big)$$

This is a (quartic) lift of the point $(-c, 1) \in C_c(\mathbb{Q})$.

Only the first two lifts here are quadratic; the others are included for completeness. Notice that (5.6) and (5.8) are identical. In fact, the sum of the points (5.7) and (5.9) is the point $(m(t), -1) \in C_{m(t)}(\mathbb{Q}(t))$, giving a dependency relation between these points.

Thus when $k(t)$ is linear in $t$, the only points that we get lifts of are $(0, 1)$ and $(-m, 1)$ in $C_m(\mathbb{Q})$. For all other lifts, $k(t)$ is a rational polynomial. For example, take the first lift in Table 5.3 of the point $(12, 31) \in C_8(\mathbb{Q})$. Substituting into equation (5.3) and solving for $k$, we get

$$k(t) = \frac{4t^3 + 170t^2 + 2400t + 11250}{-10t^2 - 225t - 1500}$$

Working with a general $k(t)$ of this form is very cumbersome.

## 5.4 Generalizing the Lift

In Section 5.2, a technique was demonstrated which lifts a specific point on $C_m$ yielding a quadratic subfamily of rank 4. This section outlines a few attempts to generalize this lifting process, analogous to the one for the family $E_m$ given in Theorem 3.4.1.

Fix $m_0 \in \mathbb{Q}$ and a point $(p, q) \in C_{m_0}(\mathbb{Q})$. The goal is to find a quadratic polynomial $M(t)$ and a point $R(t) \in C_{M(t)}(\mathbb{Q}(t))$ of the form

$$M(t) = At^2 + Bt + m_0$$

$$R(t) = (x_2t^2 + x_1t + p,\ y_3t^3 + y_2t^2 + y_1t + q).$$

As before, a linear shift of $t$ changes the constant terms, but changing $t$ by a constant multiple does not. Thus if $B \neq 0$ we can take $B = 1$ by this technique. Treating $p$, $q$ and $m_0$ as constants, we are left with 6 relations from the coefficients of $t^1$ through $t^6$ and 6 variables. (Note that the coefficient of $t^0$ merely implies that $(p, q)$ lies on the curve $C_{m_0}$.)

As in Section 5.2, the coefficients of $t^1$ through $t^3$ are linear in the $y_i$'s. Solving and substituting leaves 3 relations in the unknowns $A$, $x_1$ and $x_2$. However, all coefficients of these unknowns are now in terms of $p$, $q$ and $m_0$:

$$\begin{aligned} y_1 &= \frac{3p^2 - {m_0}^2}{2q}x_1 - \frac{m_0p}{q} \\ y_2 &= \frac{3p^2 - {m_0}^2}{2q}x_2 + \frac{12q^2p - (3p^2 - {m_0}^2)^2}{8q^3}x_1^2 + \frac{(3p^2 - {m_0}^2)m_0p - 2q^2m_0}{2q^3}x_1 \\ &\quad -\frac{m_0p}{q}A - \frac{{m_0}^2p^2}{2q^3} - \frac{p}{2q} \end{aligned}$$

The $y_3$ term is not printed here, as the equation would take up about 5 lines. The remaining 3 relations in 3 unknowns would take up several pages. Attempting

to compute just one of the resultants from here using `Pari` causes a memory overflow.

The situation is almost identical when $p$, $q$ and $m_0$ are replaced by the parameterization $x$, $y(x,k)$ and $m(x,k)$ given in (5.4) and (5.5). The coefficients become so large that they overflow the memory. All that is left is the belief that the lift exists.

CONJECTURE **5.4.1.** *Let $m_0 \in \mathbb{Q}$ and $(p,q) \in C_{m_0}(\mathbb{Q})$. Then there exists a quadratic polynomial $M(t)$ such that $M(0) = m_0$, and a point $R(t) \in C_{M(t)}(\mathbb{Q}(t))$ such that $R(0) = (p,q)$, where the points $P_1 = (0,1)$, $P_2 = (M(t),1)$, $P_3 = (-1,M(t))$ and $R(t)$ are independent in the group $C_{M(t)}(\mathbb{Q}(t))$.*

If the calculations outlined in this section could be completed, this should lead to a proof of the above conjecture. Proposition 5.2.1 shows that this conjecture is true for the point $(12,31) \in C_8(\mathbb{Q})$. Given that the degrees of the polynomials are the same as in Section 5.2, there should actually be 6 distinct quadratic lifts.

## 5.5 Subfamilies of Higher Rank

As in Section 3.5, lifts on $C_m$ can be intersected to give curves of higher rank. The smallest integer $m$ such that $C_m(\mathbb{Q})$ has rank 6 is $m = 61$. In this case, the group $C_{61}(\mathbb{Q})$ is generated by the points $P_1 = (0,1)$, $P_2 = (61,1)$, $P_3 = (-1,61)$, $P_4 = (65,181)$, $P_5 = (-9,181)$, and $P_6 = (-11,199)$. Each of the points $P_4$, $P_5$ and $P_6$ can be lifted using the methods described in Section 5.2, and one lift for each point is given in Table 5.4. (In each case, $t$ has been changed by a constant multiple to make the coefficients become integers.)

Setting $m_4(t_4) = m_5(t_5)$ gives a conic section which contains the obvious

Table 5.4: Lifts of $P_4$, $P_5$ and $P_6$ on $C_{61}$

| | |
|---|---|
| $P_4 = (65, 181)$ | $m_4(t_4) = 2730t_4^2 + 743t_4 + 61$ |
| $R_4(t_4) = (3150t_4^2 + 825t_4 + 65, 88200t_4^3 + 31920t_4^2 + 4130t_4 + 181)$ | |
| $P_5 = (-9, 181)$ | $m_5(t_5) = 30t_5^2 + 87t_5 + 61$ |
| $R_5(t_5) = (-6t_5^2 - 15t_5 - 9, 72t_5^3 + 300t_5^2 + 408t_5 + 181)$ | |
| $P_6 = (-11, 199)$ | $m_6(t_6) = 84t_6^2 + 137t_6 + 61$ |
| $R_6(t_6) = (-12t_6^2 - 23t_6 - 11, 288t_6^3 + 744t_6^2 + 656t_6 + 199)$ | |

solution $t_4 = 0 = t_5$. Substituting $t_5 = kt_4$ yields the following parameterization:

$$t_4 = \frac{-87k + 743}{30(k^2 - 91)} \tag{5.10}$$

$$t_5 = kt_4 = \frac{-87k^2 + 743k}{30(k^2 - 91)} \tag{5.11}$$

and $m_4(t_4) = m_5(t_5)$ is given by:

$$M_{4,5} = \frac{1830k^4 - 64641k^3 + 907768k^2 - 5882331k + 15154230}{30(k^2 - 91)^2} \tag{5.12}$$

THEOREM **5.5.1.** *Let $M_{4,5}$ be as defined in (5.12). Then the elliptic curve $C_{M_{4,5}}$ contains the five $\mathbb{Q}(k)$-rational points $R_1 = (0, 1)$, $R_2 = (M_{4,5}, 1)$, $R_3 = (-1, M_{4,5})$, $R_4(t_4)$ and $R_5(t_5)$, where $R_4$, $R_5$, $t_4$ and $t_5$ are given above. Moreover, these points are independent in the group $C_{M_{4,5}}(\mathbb{Q}(k))$.*

PROOF: Specializing to $k = \frac{743}{87}$ gives $t_4 = 0 = t_5$ and $M_{4,5} = 61$. This reduces $R_1, \ldots, R_5$ to the points $P_1, \ldots, P_5$ above, which are independent on $C_{61}(\mathbb{Q})$. By Proposition 2.5.2, the $R_i$ must be independent in $C_{M_{4,5}}(\mathbb{Q}(k))$. ■

Now we intersect all three subfamilies. This amounts to setting $m_6(t_6) = M_{4,5}$. As in Section 3.5, making an appropriate change of variables gives a quartic

equation which can be changed into an elliptic curve. Set

$$t_6 = \frac{v}{840(k^2-91)} - \frac{137}{168}. \tag{5.13}$$

This gives the quartic equation

$$C' : v^2 = 469225k^4 - 18099480k^3 + 262032890k^2 - 1647052680k + 62335^2 \tag{5.14}$$

which can be transformed by a rational change of variables into an elliptic curve with minimal Weierstrass model

$$E' : y^2 = x^3 - x^2 - 23078881317508x + 11109083924058691012. \tag{5.15}$$

The program `mwrank` indicates that this elliptic curve has rank 4 generated by the points $A = (-4187772, 5857933334)$, $B = (-3680063, 6797221200)$, $C = (-2533218, 7301833000)$ and $D = (-1678052, 6716508546)$, and also has torsion subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

THEOREM **5.5.2.** *Let $(k, v)$ run through the points on $C'$ as given by (5.14). Let $M_{4,5}$ be given by (5.12) and let $S$ be the elliptic surface over $C'$ given by $E_{M_{4,5}}$. Let $R_1, \ldots, R_5$ be as in Theorem 5.5.1, and let $R_6 = R_6(t_6)$ where $t_6$ is given by (5.13) and $R_6$ is given in Table 5.4. Then $R_1, \ldots, R_6$ are independent points in the Mordell–Weil group of $S$.*

PROOF: Let $P' = (k, v) = \left(\frac{743}{87}, -\frac{93660050}{7569}\right) \in C'$. Then specializing the six $R_i$ to $P'$ gives the original six independent points $P_1 = (0, 1)$, $P_2 = (61, 1)$, $P_3 = (-1, 61)$, $P_4 = (65, 181)$, $P_5 = (-9, 181)$, and $P_6 = (-11, 199)$ in the group $C_{61}(\mathbb{Q})$. Proposition 2.5.2 implies the desired result. ■

THEOREM **5.5.3.** *There are infinitely many values of $m \in \mathbb{Q}$ such that $C_m(\mathbb{Q})$ has rank at least 6.*

PROOF: Since $C'(\mathbb{Q})$ has rank 4, it has infinitely many rational points. Specializing the six points in Theorem 5.5.2 to any point $P_0 = (k_0, v_0) \in C'(\mathbb{Q})$ gives six rational points in the group $C_{M_{4,5}(k_0)}(\mathbb{Q})$. By Theorem 2.5.1 (Silverman's Specialization Theorem), these points remain independent under all but finitely many specializations. ■

EXAMPLE **5.5.4.** Two of the generators of the curve $E'(\mathbb{Q})$ in (5.15) are

$$A = (-4187772, 5857933334) \qquad B = (-3680063, 6797221200)$$

These correspond to the following points on the quartic $C'(\mathbb{Q})$ in (5.14):

$$(k_A, v_A) = \Big(\frac{455}{44}, -\frac{29049475}{1936}\Big) \qquad (k_B, v_B) = \Big(\frac{16653}{1520}, -\frac{7328930609}{462080}\Big)$$

Substituting these values of $k$ into (5.12) to compute $M_{4,5}$ gives

$$M_{4,5}^{(A)} = \frac{2989}{27} \qquad M_{4,5}^{(B)} = \frac{14301877}{351649}$$

Substituting $k$ into (5.10) and (5.11), and $(k, v)$ into (5.13) gives

$$t_4^{(A)} = -\frac{1342}{4095} \qquad t_4^{(B)} = -\frac{39064}{161889}$$
$$t_5^{(A)} = -\frac{61}{18} \qquad t_5^{(B)} = -\frac{15677}{5930}$$
$$t_6^{(A)} = -\frac{122}{63} \qquad t_6^{(B)} = -\frac{3477}{2372}$$

This gives the following 6 points on the curve $C_{M_{4,5}}$:

$$R_1^{(A)} = (0,1) \qquad R_1^{(B)} = (0,1)$$

$$R_2^{(A)} = \Big(\frac{2989}{27}, 1\Big) \qquad R_2^{(B)} = \Big(\frac{14301877}{351649}, 1\Big)$$

$$R_3^{(A)} = \Big(-1, \frac{2989}{27}\Big) \qquad R_3^{(B)} = \Big(-1, \frac{14301877}{351649}\Big)$$

$$R_4^{(A)} = \Big(\frac{202199}{1521}, -\frac{151018411}{177957}\Big) \qquad R_4^{(B)} = \Big(\frac{2932164465}{59428681}, -\frac{89889542839591}{458135701829}\Big)$$

$$R_5^{(A)} = \Big(-\frac{731}{27}, -\frac{45241}{81}\Big) \qquad R_5^{(B)} = \Big(-\frac{99156231}{8791225}, -\frac{3420802919897}{26065982125}\Big)$$

$$R_6^{(A)} = \Big(-\frac{15163}{1323}, -\frac{10356559}{27783}\Big) \qquad R_6^{(B)} = \Big(-\frac{1079585}{351649}, -\frac{14819160517}{208527857}\Big)$$

The determinants of the height matrices for these points (on the corresponding minimal models of $C_{M_{4,5}^{(A)}}$ or $C_{M_{4,5}^{(B)}}$) are:

$$det_A = 26076.7371 \qquad det_B = 1495320.1665$$

Since these determinants are nonzero, the points listed above are independent on the curves $C_{M_{4,5}^{(A)}}(\mathbb{Q})$ and $C_{M_{4,5}^{(B)}}(\mathbb{Q})$ respectively. Thus each of these curves has rank at least 6. $\square$

# Chapter 6: A Double Lift

## 6.1 A New Family

Given that lifts can be computed on both the $E_m$ and $C_m$ families of elliptic curves, it makes sense to at least take a quick look at another family. Consider the following family of elliptic curves:

$$D_m : y^2 = x^3 - m^2x + m^2 \tag{6.1}$$

The classification of rational elliptic surfaces [OS] implies the following:

THEOREM **6.1.1.** *The Mordell–Weil group $D_m\big(\overline{\mathbb{Q}}(m)\big)$ has rank 2 with trivial torsion subgroup, generated by the points $P = (m, m)$ and $Q = (0, m)$.*

Since both of the generators for this group are rational, the entire group must be defined over $\mathbb{Q}$.

COROLLARY **6.1.2.** *$D_m(\mathbb{Q}(m))$ has rank 2 generated by the points $P = (m, m)$ and $Q = (0, m)$.*

## 6.2 Finding a Lift

The first positive integer $m_0$ such that $D_{m_0}(\mathbb{Q})$ has rank 3 or more is $m_0 = 14$. The generators for the group $D_{14}(\mathbb{Q})$ are $P = (14, 14)$, $Q = (0, 14)$ and $R = (-7, 35)$.

Using the same process described in Section 5.2, we now attempt to lift the third generator $R = (-7, 35)$ to a quadratic subfamily.

If $m(t)$ is quadratic, then $D_{m(t)}(\mathbb{Q}(t))$ is a rational elliptic surface with Mordell–Weil group isomorphic to a lattice of type $A_2^* \oplus A_2^*$, which has rank 4. The generators of this lattice are points $(x(t), y(t))$ with $deg(x) \leq 2$ and $deg(y) \leq 3$, so we will search for the following:

$$m(t) = At^2 + Bt + 14 \qquad R(t) = (x_2t^2 + x_1t - 7,\ y_3t^3 + y_2t^2 + y_1t + 35)$$

Substituting this into (6.1) and equating coefficients gives:

$$70y_1 = -49x_1 + 224B \tag{$t^1$}$$

$$70y_2 + {y_1}^2 = -21{x_1}^2 - 49x_0 - 28Bx_1 + 8B^2 + 224A \tag{$t^2$}$$

$$70y_3 + 2y_1y_2 = {x_1}^3 - 42x_1x_0 - 28Bx_0 - B^2x_1 - 28Ax_1 + 16ABx_0 \tag{$t^3$}$$

$${y_2}^2 + 2y_1y_3 = 3{x_1}^2x_0 - 21{x_0}^2 - B^2x_0 - 2ABx_1 - 28Ax_0 + 8A^2 \tag{$t^4$}$$

$$2y_2y_3 = 3x_1{x_0}^2 - 2ABx_0 - A^2x_1 \tag{$t^5$}$$

$${y_3}^2 = {x_0}^3 - A^2x_0 \tag{$t^6$}$$

Again $B \neq 0$, otherwise all other coefficients are 0. Thus changing $t$ by a constant multiple can make $B = 1$. Solving and computing resultants as described in Section 5.2 gives rather interesting results. The final resultant polynomial in $x_1$ (of degree 60) factors into **seven** linear factors (6 of them to the $3^{rd}$ power and one of them to the $9^{th}$ power), and irreducible factors of degrees 3 and 30. Recall that in Section 5.2 there were only 6 linear factors, none of which were multiple roots.

Using these linear terms to solve for the remaining coefficients gives the seven lifts of $R = (-7, 35)$ given in Table 6.1. Let $m_i(t)$ and $R_i(t)$ denote the values in

Table 6.1: Lifts of the point $(-7, 35)$ on $D_{14}$

| $m(t) = At^2 + t + 14$ | $R(t) = (x_2t^2 + x_1t - 7, y_3t^3 + y_2t^2 + y_1t + 35)$ |
|---|---|
| $\frac{3}{200}t^2 + t + 14$ | $\left( -\frac{3}{400}t^2 - \frac{1}{2}t - 7,\ \frac{9}{8000}t^3 + \frac{9}{80}t^2 + \frac{71}{20}t + 35 \right)$ |
| $\frac{30}{2023}t^2 + t + 14$ | $\left( -\frac{12}{2023}t^2 - \frac{8}{17}t - 7,\ \frac{36}{34391}t^3 + \frac{222}{2023}t^2 + \frac{60}{17}t + 35 \right)$ |
| $\frac{30}{2023}t^2 + t + 14$ | $\left( -\frac{15}{1156}t^2 - \frac{13}{17}t - 7,\ \frac{225}{275128}t^3 + \frac{825}{8092}t^2 + \frac{127}{34}t + 35 \right)$ |
| $\frac{15}{841}t^2 + t + 14$ | $\left( -\frac{15}{3364}t^2 - \frac{11}{29}t - 7,\ \frac{225}{195112}t^3 + \frac{375}{3364}t^2 + \frac{201}{58}t + 35 \right)$ |
| $\frac{30}{1681}t^2 + t + 14$ | $\left( -\frac{20}{1681}t^2 - \frac{24}{41}t - 7,\ \frac{100}{68921}t^3 + \frac{210}{1681}t^2 + \frac{148}{41}t + 35 \right)$ |
| $\frac{20}{1849}t^2 + t + 14$ | $\left( -\frac{16}{1849}t^2 - \frac{32}{43}t - 7,\ \frac{48}{79507}t^3 + \frac{164}{1849}t^2 + \frac{160}{43}t + 35 \right)$ |
| $\frac{660}{37303}t^2 + t + 14$ | $\left( -\frac{240}{37303}t^2 - \frac{32}{73}t - 7,\ \frac{3600}{2723119}t^3 + \frac{60}{511}t^2 + \frac{256}{73}t + 35 \right)$ |

the $i^{th}$ row of this table. Notice that $m_2(t) = m_3(t)$. Hence there are still only 6 distinct subfamilies to which this point can be lifted, but one of these contains two different lifts of the point. Each lift also contains the points $P_i(t) = (m_i(t), m_i(t))$ and $Q_i(t) = (0, m_i(t))$. For any $i = 1, \ldots, 7$, specializing $P_i(t)$, $Q_i(t)$ and $R_i(t)$ to $t = 0$ gives three independent points on $D_{14}(\mathbb{Q})$. However, there is actually a stronger result here.

THEOREM **6.2.1.** *The points $P_2(t)$, $Q_2(t)$, $R_2(t)$, $R_3(t) \in D_{m_2(t)}(\mathbb{Q}(t))$ are independent. Therefore, these points form a subgroup of finite index in the Mordell–Weil group.*

PROOF: Specializing these points at $t = 1$ gives $m_2(1) = \frac{30375}{2023}$ and the points:

$$\begin{aligned} P_2(1) &= \Big(\frac{30375}{2023}, \frac{30375}{2023}\Big) \\ Q_2(1) &= \Big(0, \frac{30375}{2023}\Big) \\ R_2(1) &= \Big(-\frac{15125}{2023}, \frac{1328875}{34391}\Big) \\ R_3(1) &= \Big(-\frac{8991}{1156}, \frac{10685439}{275128}\Big) \end{aligned}$$

The determinant of the height matrix for these points (after changing to the minimal model for $D_{\frac{30375}{2023}}$) is 168.098, so these four points are independent. By Proposition 2.5.2, the points $P_2(t)$, $Q_2(t)$, $R_2(t)$ and $R_3(t)$ are independent in $D_{m_2(t)}(\mathbb{Q}(t))$. As mentioned above, the Mordell–Weil group has rank 4. Therefore these points generate a subgroup of finite index. ■

This result is a bit different than any of the results for $E_m$ or $C_m$. For $E_m$, which has rank 2 over $\mathbb{Q}(m)$, Theorem 3.4.1 yields a subfamily $E_{m(t)}$ of rank 3 over $\mathbb{Q}(t)$. Similarly for $C_m$, the rank was increased by 1. Here, the rank is increased by 2. It is not clear exactly what caused this *double lift* to occur. In a separate example, starting with the point $(-9, 39) \in D_{15}(\mathbb{Q})$ (which has rank 3) produced seven distinct polynomials $m(t)$. For each of these, the rank is only increased by 1.

REMARK **6.2.2.** For $E_m$, we could try to generate a similar *double lift* by setting two distinct lifts from Section 3.4 (Remark 3.4.2 on p. 26) equal to each other. However this should not work, because all points of minimal degree over $\overline{\mathbb{Q}}(t)$ have already been found (see Theorem 4.3.1). If any of these could be equal to each other, this would produce too many points of minimal degree. □

# Appendix A: Rank of $E_m(\mathbb{Q})$ for $m = 1, \ldots, 500$

Let $E_m$ be the elliptic curve given by $y^2 = x^3 - x + m^2$. The program `mwrank` was used to compute the rank of $E_m(\mathbb{Q})$ for integer values of $m$ from 1 to 500. The results are summarized in the table below.

For some elliptic curves, `mwrank` gives a range of possible values for the rank. In particular, for $m = 234,494$, `mwrank` gives the range 2 to 4. In these cases (indicated by numbers in *italics*) the lower bound on the rank has been used.

| |
|---|
| **Values of $m$ for which $E_m(\mathbb{Q})$ has rank 1:** 1 |
| **Values of $m$ for which $E_m(\mathbb{Q})$ has rank 2:** 2, 3, 4, 6, 9, 10, 18, 21, 26, 30, 32, 34, 35, 38, 52, 54, 56, 68, 69, 72, 76, 78, 79, 81, 84, 91, 95, 104, 105, 106, 115, 126, 130, 132, 133, 135, 137, 138, 143, 144, 147, 149, 156, 158, 168, 170, 171, 172, 174, 191, 205, 208, 212, 217, 219, 220, 224, 229, *234*, 243, 247, 250, 256, 257, 258, 260, 267, 270, 272, 280, 285, 288, 299, 301, 306, 308, 315, 319, 322, 333, 336, 339, 340, 342, 348, 351, 353, 356, 360, 361, 362, 363, 364, 369, 373, 376, 378, 382, 384, 389, 390, 397, 403, 410, 415, 420, 425, 438, 450, 451, 453, 454, 458, 459, 460, 470, 476, 477, 484, 485, 487, 492, *494*, 496, 498 |
| **Values of $m$ for which $E_m(\mathbb{Q})$ has rank 3:** 5, 7, 8, 11, 12, 13, 14, 15, 16, 17, 19, 20, 22, 23, 28, 29, 33, 37, 39, 40, 42, 43, 44, 45, 47, 48, 49, 50, 51, 53, 55, 57, 59, 60, 62, 64, 65, 66, 67, 73, 75, 77, 80, 82, 86, 87, 88, 89, 90, 93, 94, |

| |
|---|
| 96, 98, 99, 100, 101, 103, 108, 109, 110, 111, 114, 117, 118, 119, 120, 121, 122, 123, 129, 134, 136, 140, 141, 142, 148, 150, 151, 152, 153, 154, 155, 157, 161, 162, 164, 166, 167, 169, 177, 178, 180, 183, 185, 186, 187, 188, 189, 192, 193, 194, 195, 196, 197, 198, 200, 201, 202, 203, 206, 211, 216, 218, 223, 226, 227, 228, 231, 232, 235, 237, 238, 239, 241, 242, 244, 249, 252, 253, 254, 259, 261, 262, 265, 266, 268, 273, 274, 276, 281, 282, 284, 289, 293, 294, 295, 296, 297, 298, 300, 302, 303, 307, 309, 310, 313, 314, 320, 321, 323, 324, 327, 328, 330, 332, 334, 338, 341, 344, 345, 346, 354, 355, 357, 358, 359, 366, 367, 368, 370, 374, 375, 377, 381, 383, 387, 388, 392, 393, 395, 396, 401, 402, 404, 406, 407, 412, 413, 414, 416, 418, 422, 423, 424, 426, 427, 429, 432, 433, 435, 436, 437, 440, 441, 442, 444, 446, 447, 448, 455, 456, 464, 465, 466, 468, 471, 472, 474, 475, 478, 479, 480, 482, 483, 486, 488, 490, 491, 495, 497 |
| **Values of $m$ for which $E_m(\mathbb{Q})$ has rank 4:** 24, 25, 27, 31, 36, 41, 46, 58, 61, 63, 70, 71, 74, 83, 85, 92, 97, 102, 107, 112, 116, 124, 125, 128, 131, 139, 145, 146, 159, 160, 165, 173, 175, 179, 182, 184, 190, 199, 204, 207, 210, 213, 214, 221, 222, 225, 230, 233, 236, 240, 246, 248, 251, 255, 263, 264, 269, 271, 275, 277, 278, 279, 286, 287, 290, 291, 292, 304, 305, 311, 313, 316, 318, 325, 326, 329, 331, 335, 343, 347, 349, 352, 371, 372, 379, 391, 398, 399, 400, 405, 408, 409, 417, 419, 421, 428, 430, 434, 439, 443, 445, 449, 457, 461, 462, 463, 467, 469, 473, 481, 489, 499 |
| **Values of $m$ for which $E_m(\mathbb{Q})$ has rank 5:** 113, 127, 163, 176, 181, 209, 215, 245, 283, 317, 350, 365, 380, 385, 386, 394, 411, 431, 452, 493, 500 |
| **Values of $m$ for which $E_m(\mathbb{Q})$ has rank 6:** 337 |

# Appendix B: Rank of $C_m(\mathbb{Q})$ for $m = 1, \ldots, 500$

Let $C_m$ be the elliptic curve given by $y^2 = x^3 - m^2x + 1$. The program `mwrank` was used to compute the rank of $C_m(\mathbb{Q})$ for integer values of $m$ from 1 to 500. The results are summarized in the table below.

For some elliptic curves, `mwrank` gives a range of possible values for the rank. In particular, for $m = 285, 455$, `mwrank` gives the range 3 to 5, and for $m = 210, 375$ it gives the range 4 to 6. In these cases (indicated by numbers in *italics*) the lower bound on the rank has been used.

| |
|---|
| **Values of $m$ for which $C_m(\mathbb{Q})$ has rank 1:** 1 |
| **Values of $m$ for which $C_m(\mathbb{Q})$ has rank 2:** 2, 3 |
| **Values of $m$ for which $C_m(\mathbb{Q})$ has rank 3:** 4, 5, 6, 7, 9, 10, 11, 12, 15, 18, 21, 24, 30, 33, 34, 35, 38, 39, 43, 50, 54, 60, 64, 65, 76, 84, 87, 90, 91, 96, 97, 100, 104, 108, 109, 126, 136, 145, 150, 154, 165, 167, 173, 176, 181, 183, 187, 194, 195, 200, 202, 205, 213, 221, 231, 234, 237, 242, 245, 246, 247, 252, 255, 267, 273, 275, 276, 281, 283, *285*, 290, 294, 298, 300, 304, 305, 306, 309, 315, 319, 321, 323, 325, 326, 329, 333, 339, 344, 357, 362, 366, 381, 386, 387, 392, 404, 412, 414, 415, 419, 422, 435, 436, 438, 449, 451, *455*, 459, 460, 462, 465, 468, 470, 471, 477, 481, 482, 484, 485, 486, 494 |
| **Values of $m$ for which $C_m(\mathbb{Q})$ has rank 4:** 8, 13, 14, 16, 19, 20, 22, 23, 26, |

| |
|---|
| 27, 28, 29, 31, 32, 37, 40, 44, 45, 47, 48, 49, 51, 52, 55, 56, 57, 58, 62, 63, 66, 67, 68, 69, 71, 72, 74, 75, 77, 79, 81, 82, 85, 88, 89, 92, 95, 101, 103, 105, 106, 110, 111, 112, 114, 115, 117, 118, 120, 121, 122, 123, 125, 129, 130, 133, 135, 138, 139, 141, 142, 143, 144, 149, 153, 155, 156, 159, 161, 162, 163, 169, 171, 172, 174, 175, 177, 180, 182, 185, 186, 189, 190, 198, 201, 203, 204, 207, 208, 209, *210*, 214, 215, 216, 218, 219, 223, 227, 228, 229, 230, 235, 240, 244, 248, 249, 250, 254, 256, 258, 260, 263, 265, 266, 268, 269, 270, 277, 278, 282, 284, 286, 289, 292, 293, 297, 299, 301, 303, 312, 313, 316, 318, 320, 322, 324, 327, 330, 331, 334, 338, 340, 341, 342, 345, 348, 350, 351, 354, 355, 358, 360, 361, 364, 368, 369, 371, 373, *375*, 377, 378, 379, 380, 382, 384, 390, 391, 397, 400, 403, 407, 408, 409, 411, 413, 416, 417, 421, 424, 425, 429, 432, 433, 437, 440, 441, 442, 448, 457, 461, 467, 472, 478, 480, 488, 491, 492, 493, 495, 499 |
| **Values of $m$ for which $C_m(\mathbb{Q})$ has rank 5:** 17, 25, 36, 41, 42, 46, 53, 59, 70, 73, 78, 80, 83, 86, 93, 94, 98, 99, 102, 113, 116, 119, 127, 131, 132, 134, 137, 140, 147, 151, 152, 157, 158, 160, 164, 166, 168, 170, 179, 184, 188, 191, 192, 193, 196, 197, 206, 211, 212, 217, 220, 222, 224, 225, 226, 232, 233, 236, 238, 239, 241, 243, 251, 257, 259, 261, 271, 272, 274, 279, 287, 288, 291, 296, 302, 307, 310, 311, 314, 317, 328, 336, 337, 343, 346, 349, 352, 353, 356, 363, 367, 370, 372, 374, 383, 385, 388, 389, 395, 396, 401, 402, 405, 406, 410, 420, 423, 426, 427, 428, 430, 434, 439, 444, 445, 446, 450, 453, 454, 456, 458, 463, 464, 466, 469, 473, 475, 476, 483, 487, 489, 490, 497, 498, 500 |
| **Values of $m$ for which $C_m(\mathbb{Q})$ has rank 6:** 61, 107, 124, 128, 146, 148, 178, 199, 253, 262, 264, 280, 295, 308, 332, 335, 359, 365, 376, 393, 394, 398, 399, 418, 431, 447, 452, 474, 479, 496 |
| **Values of $m$ for which $C_m(\mathbb{Q})$ has rank 7:** 347, 443 |

# BIBLIOGRAPHY


[BM] Ezra A. Brown and Bruce T. Myers, *Elliptic Curves from Mordell To Diophantus and Back*, Amer. Math. Monthly **109** (2002), 639-649.

[CS] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer, Third Edition, 1999.

[DF] David S. Dummit and Richard M. Foote, *Abstract Algebra*, John Wiley & Sons, Inc., 1999.

[H] Robin Hartshorne, *Algebraic Geometry*, Springer–Verlag, 1977.

[K] Neal Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer–Verlag, 1993.

[mwrank] `http://www.maths.nott.ac.uk/personal/jec/ftp/progs`

[OS] Keiji Oguiso and Tetsuji Shioda, *The Mordell–Weil Lattices of a Rational Elliptic Surface*, Comment. Math. Univ. St Pauli **40** (1991), 83-99.

[Pari/GP] `http://pari.math.u-bordeaux.fr`

[Shi1] Tetsuji Shioda, *Mordell–Weil Lattices and Galois Representation I, II, III*, Proc. Japan Acad. 65A (1989), 268-271, 296-299, 300-303.

[Shi2] Tetsuji Shioda, *On the Mordell–Weil Lattices*, Comment. Math. Univ. St Pauli **39** (1990), 211-240.

[Shi3] Tetsuji Shioda, *Construction of Elliptic Curves with High Rank via the Invariants of the Weyl Groups*, J. Math. Soc. Japan, Vol. 43, No. 4 (1991), 673-719.

[Sil1] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer–Verlag, 1986.

[Sil2] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer–Verlag, 1994.

[W] Lawrence C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman & Hall/CRC, 2003.