Constructing Elliptic Curves over $\mathbb{Q}(T)$ with Moderate Rank

Scott Arms

Department of Mathematics, The Ohio State University, Columbus, OH, 43210

Álvaro Lozano-Robledo

Department of Mathematics, Boston University, Boston, MA 02215
Current address: Department of Mathematics, Cornell University, Ithaca, NY 14853

Steven J. Miller

Department of Mathematics, The Ohio State University, Columbus, Ohio, 43210
Current address: Department of Mathematics, Brown University, Providence, RI 02912

Abstract

We give several new constructions for moderate rank elliptic curves over $\mathbb{Q}(T)$. In particular we construct infinitely many rational elliptic surfaces (not in Weierstrass form) of rank 6 over $\mathbb{Q}$ using polynomials of degree two in T. While our method generates linearly independent points, we are able to show the rank is exactly 6 *without* having to verify the points are independent. The method generalizes; however, the higher rank surfaces are not rational, and we need to check that the constructed points are linearly independent.

Key words: elliptic Curves, rational elliptic surfaces, Mordell-Weil rank
1991 MSC: 11G05 (primary), 11G20 (secondary)

Email addresses: `arms@math.ohio-state.edu` (Scott Arms), `alozano@math.cornell.edu` (Álvaro Lozano-Robledo), `sjmiller@math.brown.edu` (Steven J. Miller).

1 Introduction

Consider the elliptic curve $\mathcal{E}$ over $\mathbb{Q}(T)$:

$$y^2 + a_1(T)xy + a_3(T)y \;=\; x^3 + a_2(T)x^2 + a_4(T)x + a_6(T), \tag{1.1}$$

where $a_i(T) \in \mathbb{Z}[T]$. By evaluating these polynomials at integers, we obtain elliptic curves over $\mathbb{Q}$. By Silverman's Specialization Theorem, for large $t \in \mathbb{Z}$ the Mordell-Weil rank of the fiber $\mathcal{E}_t$ over $\mathbb{Q}$ is at least that of the curve $\mathcal{E}$ over $\mathbb{Q}(T)$.

For comparison purposes, we briefly describe other methods to construct curves with rank. Mestre [Mes1,Mes2] considers a 6-tuple of integers a_i and defines $q(x) = \prod_{i=1}^{6}(x - a_i)$ and $p(x,T) = q(x-T)q(x+T)$. There exist polynomials $g(x,T)$ of degree 6 in x and $r(x,T)$ of degree at most 5 in x such that $p(x,T) = g^2(x,T) - r(x,T)$. Consider the curve $y^2 = r(x,T)$ over $\mathbb{Q}(T)$. If $r(x,T)$ is of degree 3 or 4 in x, we obtain an elliptic curve with points $P_{\pm i}(T) = (\pm T + a_i, g(\pm T + a_i))$. If $r(x,T)$ has degree 4 we may need to change variables to make the coefficient of x^4 a perfect square (see [Mor], page 77). Two 6-tuples that work are $(-17, -16, 10, 11, 14, 17)$ and $(399, 380, 352, 47, 4, 0)$ (see [Na1]). Curves of rank up to 14 over $\mathbb{Q}(T)$ have been constructed this way, and using these methods Nagao [Na1] has found an elliptic curve of rank at least 21 and Fermigier [Fe2] one of rank at least 22 over $\mathbb{Q}$. Shioda [Sh2] gives explicit constructions for not only rational elliptic curves over $\mathbb{Q}(T)$ of rank $2, 4, 6, 7$ and 8, but generators of the Mordell-Weil groups as well, and shows in [Sh1] that 8 is the largest possible rank for a rational elliptic curve over $\mathbb{Q}(T)$.

We now describe the idea of our method. For $\mathcal{E}$ as in (1.1), define

$$A_{\mathcal{E}}(p) \;=\; \frac{1}{p}\sum_{t=0}^{p-1} a_t(p), \tag{1.2}$$

with $a_t(p) = p + 1 - N_t(p)$, where $N_t(p)$ is the number of points in $\mathcal{E}_t(\mathbb{F}_p)$ (we set $a_t(p) = 0$ when $p \mid \Delta(t)$). Rosen and Silverman [RS] prove a version of a conjecture of Nagao [Na1] which relates $A_{\mathcal{E}}(p)$ to the rank of $\mathcal{E}$ over $\mathbb{Q}(T)$. They show that if $\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$, with $A(T), B(T) \in \mathbb{Z}[T]$, and Tate's conjecture (known if $\mathcal{E}$ is a rational elliptic surface over $\mathbb{Q}$) holds for $\mathcal{E}$, then

$$\lim_{X\to\infty} \frac{1}{X}\sum_{p\le X} -A_{\mathcal{E}}(p)\log p \;=\; \text{rank } \mathcal{E}(\mathbb{Q}(T)). \tag{1.3}$$

Tate's Conjecture (for our situation; see [Ta]) states that if $L_2(\mathcal{E}/\mathbb{Q}, s)$ is the Hasse-Weil L-function of $\mathcal{E}/\mathbb{Q}$ attached to $H^2_{\text{ét}}(\mathcal{E}/\overline{\mathbb{Q}})$ and $\text{NS}(\mathcal{E}/\mathbb{Q})$ is the N*é*ron-Severi group of $\mathcal{E}/\mathbb{Q}$, then $L_2(\mathcal{E}/\mathbb{Q}, s)$ has a meromorphic continuation to $\mathbb{C}$ and has a pole at $s = 2$ of order $-\text{ord}_{s=2}L_2(\mathcal{E}/\mathbb{Q}, s) = \text{rank NS}(\mathcal{E}/\mathbb{Q})$.

An elliptic curve $\mathcal{E}$ over $\mathbb{Q}(T)$ is a rational elliptic surface over $\mathbb{Q}$ if and only if one of the following holds:

(1) $0 < \max\{3\text{deg } A(T), 2\text{deg } B(T)\} < 12$.
(2) $3\text{deg } A(T) = 2\text{deg } B(T) = 12$ and $\text{ord}_{T=0}T^{12}\Delta(T^{-1}) = 0$

(see [Mir,RS]). In this paper we construct special rational elliptic surfaces where we are able to evaluate $A_{\mathcal{E}}(p)$ exactly; see Theorem 1 for a rank 6 example. For these surfaces, we have $A_{\mathcal{E}}(p) = -r + O(\frac{1}{p})$. By Rosen and Silverman's result and the Prime Number Theorem, we can conclude that the constant r is the rank of $\mathcal{E}$ over $\mathbb{Q}(T)$.

The novelty of this approach is that by forcing $A_{\mathcal{E}}(p)$ to be essentially constant, provided $\mathcal{E}$ is a rational elliptic surface over $\mathbb{Q}$, we can immediately calculate the Mordell-Weil rank *without* having to specialize points and calculate height matrices. Further, we obtain an exact answer for the rank, and not a lower bound. Finally, it is often useful to have elliptic curves over $\mathbb{Q}(T)$ with exact formulas for $A_{\mathcal{E}}(p)$; see [Mil2] for applications to lower order density terms in the Katz-Sarnak Density Conjecture for one-parameter families of elliptic curves.

If the degrees of the defining polynomials of $\mathcal{E}$ are too large, our results are conditional on Tate's conjecture if we are able to evaluate $A_{\mathcal{E}}(p)$. In many cases, however, we are unable to evaluate $A_{\mathcal{E}}(p)$ to the needed accuracy. Our method does generate candidate points, which upon specialization yield lower bounds for the rank. In this manner, curves of rank up to 8 over $\mathbb{Q}(T)$ have been found.

Modifications of our method may yield curves with higher rank over $\mathbb{Q}(T)$, though to *find* such curves requires solving very intractable non-linear Diophantine equations and then specializing the points and calculating the height matrices to see that they are independent over $\mathbb{Q}(T)$.

For additional constructions, especially for lower rank curves over $\mathbb{Q}(T)$, see [Fe2]. For a good survey on ranks of elliptic curves, see [RuS]. For applications of quadratic polynomials to primitive root producing polynomials, see [Moree].

2 Constructing Rank 6 Rational Surfaces over $\mathbb{Q}(T)$

2.1 Idea of the Construction

The main idea is as follows: we can explicitly evaluate linear and quadratic Legendre sums; for cubic and higher sums, we cannot in general explicitly evaluate the sums. Instead, we have bounds (Hasse, Weil) exhibiting large cancellation.

The goal is to cook up curves $\mathcal{E}$ over $\mathbb{Q}(T)$ where we have linear and quadratic expressions in T. We can evaluate these expressions exactly by a standard lemma on quadratic Legendre sums (see Lemma 5 of the appendix for a proof), which states that if a and b are not both zero mod p and $p > 2$, then for $t \in \mathbb{Z}$

$$\sum_{t=0}^{p-1} \left(\frac{at^2+bt+c}{p}\right) \ = \ \begin{cases} (p-1)\left(\frac{a}{p}\right) & \text{if } p|(b^2-4ac) \\ -\left(\frac{a}{p}\right) & \text{otherwise.} \end{cases} \tag{2.1}$$

Thus if $p|(b^2-4ac)$, the summands are $\left(\frac{a(t-t')^2}{p}\right) = \left(\frac{a}{p}\right)$, and the t-sum is large. Later when we generalize the method we study special curves that are quartic in T. Let

$$\begin{aligned} y^2 \ = \ f(x,T) \ &= \ x^3T^2 + 2g(x)T - h(x) \\ g(x) \ &= \ x^3 + ax^2 + bx + c, \ \ c \neq 0 \\ h(x) \ &= \ (A-1)x^3 + Bx^2 + Cx + D \\ D_T(x) \ &= \ g(x)^2 + x^3h(x). \end{aligned} \tag{2.2}$$

Note that $D_T(x)$ is one-fourth of the discriminant of the quadratic (in T) polynomial $f(x,T)$. When we specialize T to t, we write $D_t(x)$ for one-fourth of the discriminant of the quadratic (in t) polynomial $f(x,t)$. We will see that the number of distinct, non-zero roots of the $D_T(x)$ control the rank. We write $A-1$ as the leading coefficient of $h(x)$, and not A, to simplify future computations by making the coefficient of x^6 in $D_T(x)$ equal A.

Our elliptic curve $\mathcal{E}$ is not written in standard form, as the coefficient of x^3 is $T^2-2T+A-1$. This is harmless, and later we rewrite the curve in Weierstrass form. As $y^2 = f(x,T)$, for the fiber at $T=t$ we have

$$a_t(p) \ = \ -\sum_{x(p)} \left(\frac{f(x,t)}{p}\right) \ = \ -\sum_{x(p)} \left(\frac{x^3t^2+2g(x)t-h(x)}{p}\right), \tag{2.3}$$

where $\left(\frac{*}{p}\right)$ is the Legendre symbol. We study $-pA_{\mathcal{E}}(p) = \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f(x,t)}{p}\right)$.

When $x \equiv 0$ the t-sum vanishes if $c \not\equiv 0$, as it is just $\sum_{t=0}^{p-1} \left(\frac{2ct-D}{p}\right)$. Assume now $x \not\equiv 0$. By the lemma on quadratic Legendre sums (Lemma 5)

$$\sum_{t=0}^{p-1} \left(\frac{x^3t^2 + 2g(x)t - h(x)}{p}\right) = \begin{cases} (p-1)\left(\frac{x^3}{p}\right) & \text{if } p|D_t(x) \\ -\left(\frac{x^3}{p}\right) & \text{otherwise.} \end{cases} \tag{2.4}$$

Our goal is to find integer coefficients a, b, c, A, B, C, D so that $D_T(x)$ has six distinct, non-zero integer roots. We want the roots $r_1, \dots, r_6$ to be squares in $\mathbb{Z}$, as their contribution is $(p-1)\left(\frac{r_i^3}{p}\right)$. If r_i is not a square, $\left(\frac{r_i}{p}\right)$ will be 1 for half the primes and -1 for the other half, yielding no net contribution to the rank. Thus, for $1 \le i \le 6$, let $r_i = \rho_i^2$.

Assume we can find such coefficients. Then for large p

$$\begin{aligned} -pA_{\mathcal{E}}(p) &= \sum_{x=0}^{p-1}\sum_{t=0}^{p-1} \left(\frac{f(x,t)}{p}\right) = \sum_{x=0}^{p-1}\sum_{t=0}^{p-1} \left(\frac{x^3t^2 + 2g(x)t - h(x)}{p}\right) \\ &= \sum_{x=0}\sum_{t=0}^{p-1} \left(\frac{f(x,t)}{p}\right) + \sum_{x:D_t(x)\equiv 0}\sum_{t=0}^{p-1} \left(\frac{f(x,t)}{p}\right) + \sum_{x:xD_t(x)\not\equiv 0}\sum_{t=0}^{p-1} \left(\frac{f(x,t)}{p}\right) \\ &= 0 + 6(p-1) - \sum_{x:xD_t(x)\not\equiv 0} \left(\frac{x^3}{p}\right) = 6p. \end{aligned} \tag{2.5}$$

We must find $a, \dots, D$ such that $D_T(x)$ has six distinct, non-zero roots ρ_i^2:

$$\begin{aligned} D_T(x) &= g(x)^2 + x^3h(x) \\ &= Ax^6 + (B+2a)x^5 + (C+a^2+2b)x^4 + (D+2ab+2c)x^3 \\ &\quad + (2ac+b^2)x^2 + (2bc)x + c^2 \\ &= A(x^6 + R_5x^5 + R_4x^4 + R_3x^3 + R_2x^2 + R_1x + R_0) \\ &= A(x-\rho_1^2)(x-\rho_2^2)(x-\rho_3^2)(x-\rho_4^2)(x-\rho_5^2)(x-\rho_6^2). \end{aligned} \tag{2.6}$$

2.2 Determining Admissible Constants $a, \dots, D$

Because of the freedom to choose B, C, D there is no problem matching coefficients for the x^5, x^4, x^3 terms. We must simultaneously solve in integers

$$\begin{aligned} 2ac + b^2 &= R_2A \\ 2bc &= R_1A \\ c^2 &= R_0A. \end{aligned} \tag{2.7}$$

For simplicity, take $A = 64R_0^3$. Then

$$\begin{aligned}
c^2 &= 64R_0^4 & \longrightarrow \quad c &= 8R_0^2 \\
2bc &= 64R_0^3R_1 & \longrightarrow \quad b &= 4R_0R_1 \\
2ac+b^2 &= 64R_0^3R_2 & \longrightarrow \quad a &= 4R_0R_2 - R_1^2.
\end{aligned} \tag{2.8}$$

For an explicit example, take $r_i = \rho_i^2 = i^2$. For these choices of roots,

$$R_0 = 518400, \; R_1 = -773136, \; R_2 = 296296. \tag{2.9}$$

Solving for a through D yields

$$\begin{aligned}
A &= 64R_0^3 &=& \; 8916100448256000000 \\
c &= 8R_0^2 &=& \; 2149908480000 \\
b &= 4R_0R_1 &=& \; -1603174809600 \\
a &= 4R_0R_2 - R_1^2 &=& \; 16660111104 \\
B &= R_5A - 2a &=& \; -811365140824616222208 \\
C &= R_4A - a^2 - 2b &=& \; 26497490347321493520384 \\
D &= R_3A - 2ab - 2c &=& \; -343107594345448813363200
\end{aligned} \tag{2.10}$$

We convert $y^2 = f(x,T)$ to $y^2 = F(x,T)$, which is in Weierstrass normal form. We send $y \to \frac{y}{T^2+2T-A+1}$, $x \to \frac{x}{T^2+2T-A+1}$, and then multiply both sides by $(T^2+2T-A+1)^2$. For future reference, we note that

$$\begin{aligned}
T^2+2T-A+1 &= (T+1-\sqrt{A})(T+1+\sqrt{A}) \\
&= (T-t_1)(T-t_2) \\
&= (T-2985983999)(T+2985984001).
\end{aligned} \tag{2.11}$$

We have

$$\begin{aligned}
f(x,T) &= T^2x^3 + (2x^3+2ax^2+2bx+2c)T - (A-1)x^3 - Bx^2 - Cx - D \\
&= (T^2+2T-A+1)x^3 + (2aT-B)x^2 + (2bT-C)x + (2cT-D) \\
F(x,T) &= x^3 + (2aT-B)x^2 + (2bT-C)(T^2+2T-A+1)x \\
&\quad +(2cT-D)(T^2+2T-A+1)^2.
\end{aligned} \tag{2.12}$$

We now study the $-pA_{\mathcal{E}}(p)$ arising from $y^2 = F(x,T)$. It is enough to show this is $6p+O(1)$ for all p greater than some p_0. Recall that t_1, t_2 are the unique roots of $T^2+2T-A+1 \equiv 0 \bmod p$. We find

$$-pA_{\mathcal{E}}(p) \;=\; \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{F(x,t)}{p}\right) \;=\; \sum_{t\neq t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{F(x,t)}{p}\right) + \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{F(x,t)}{p}\right). \tag{2.13}$$

For $t \neq t_1, t_2$, send $x \longrightarrow (t^2+2t-A+1)x$. As $(t^2+2t-A+1) \not\equiv 0$, $\left(\frac{(t^2+2t-A+1)^2}{p}\right) = 1$ and by (2.12) the sum over $t \neq t_1, t_2$ in (2.13) is now of $f(x,t)$ instead of $F(x,T)$. Simple algebra yields

$$\begin{aligned}
-pA_{\mathcal{E}}(p) &= \sum_{t\neq t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{f(x,t)}{p}\right) + \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{x^3+(2at-B)x^2+0x+0}{p}\right) \\
&= \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{f(x,t)}{p}\right) + \sum_{t=t_1,t_2}\sum_{x=1}^{p-1}\left(\frac{x+2at-B}{p}\right) - \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{f(x,t)}{p}\right) \\
&= 6p + O(1) + \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{(2at-B)x^2+(2bt-C)x+(2ct-D)}{p}\right),
\end{aligned} \tag{2.14}$$

where the main term (the $6p$) follows from (2.5). By the lemma on quadratic Legendre sums, the x-sum in (2.14) is negligible (i.e., is $O(1)$) if

$$\phi(t) \;=\; (2bt-C)^2 - 4(2at-B)(2ct-D) \tag{2.15}$$

is not congruent to zero modulo p when $t = t_1$ or t_2. Calculating yields

$$\begin{aligned}
\phi(t_1) &= 4291243480243836561123092143580209905401856 \\
&= 2^{32}\cdot 3^{25}\cdot 7^5\cdot 11^2\cdot 13\cdot 19\cdot 29\cdot 31\cdot 47\cdot 67\cdot 83\cdot 97\cdot 103 \\
\phi(t_2) &= 4291243816662452751895093255391719515488256 \\
&= 2^{33}\cdot 3^{12}\cdot 7\cdot 11\cdot 13\cdot 41\cdot 173\cdot 17389\cdot 805873\cdot 9447850813.
\end{aligned} \tag{2.16}$$

Hence, except for finitely many primes (coming from factors of $\phi(t_i)$, $a, \dots, D$, t_1 and t_2), $-pA_{\mathcal{E}}(p) = 6p + O(1)$ as desired. We have shown the following result:

Theorem 1 *There exist integers a, b, c, A, B, C, D so that the curve $\mathcal{E} : y^2 = x^3T^2 + 2g(x)T - h(x)$ over $\mathbb{Q}(T)$, with $g(x) = x^3 + ax^2 + bx + c$ and $h(x) = (A-1)x^3 + Bx^2 + Cx + D$, has rank 6 over $\mathbb{Q}(T)$. In particular, with the choices of a through D above, $\mathcal{E}$ is a rational elliptic surface and has Weierstrass form*

$$y^2 = x^3 + (2aT-B)x^2 + (2bT-C)(T^2+2T-A+1)x + (2cT-D)(T^2+2T-A+1)^2.$$

Proof: We show $\mathcal{E}$ is a rational elliptic surface by translating $x \mapsto x - (2aT - B)/3$, which yields $y^2 = x^3 + A(T)x + B(T)$ with $\deg(A) = 3, \deg(B) = 5$. Therefore the Rosen-Silverman theorem is applicable, and because we can compute $A_{\mathcal{E}}(p)$, we know the rank is exactly 6 (and we never need to calculate height matrices). $\square$

Remark 2 *We can construct infinitely many $\mathcal{E}$ over $\mathbb{Q}(T)$ with rank 6 using* (2.10)*, as for generic choices of roots $\rho_1^2, \dots, \rho_6^2$,* (2.15) *holds.*

For concreteness, we explicitly list a curve of rank at least 6. Doing a better job of choosing coefficients a through D (but still being crude) yields

Theorem 3 *The elliptic curve $y^2 = x^3 + Ax + B$ has rank at least 6 over $\mathbb{Q}$, where*

$$
\begin{aligned}
A &= 1123187040185717205972 \\
B &= 50786893859117937639786031372848.
\end{aligned}
$$

Six points on the curve are:

$$
\begin{array}{llll}
(67585071288, & 20866449849961716) & (60673071396, & 18500949214922664) \\
(49153071576, & 14991664661755236) & (33025071828, & 11131001682078096) \\
(12289072152, & 8151425152633980) & (-13054927452, & 5822267813027064).
\end{array}
\tag{2.17}
$$

As the determinant of the height matrix is approximately $880,000$, the points are independent and therefore generate the group. A trivial modification of this procedure yields rational elliptic surfaces of any rank $r \leq 6$. For more constructions along these lines, see [Mil1].

3 More Attempts for Curves with rank 6, 7 and 8 over $\mathbb{Q}(T)$

3.1 Curves of Rank 6

We sketch another construction for a curve of rank 6 over $\mathbb{Q}(T)$ by modifying our previous arguments. We define a curve $\mathcal{E}$ over $\mathbb{Q}(T)$ by

$$
\begin{aligned}
y^2 \;=\; f(x,T) &= x^4T^2 + 2g(x)T - h(x) \\
g(x) &= x^4 + ax^3 + bx^2 + cx + d, \;\; d \neq 0 \\
h(x) &= -x^4 + Ax^3 + Bx^2 + Cx + D \\
D_T(x) &= g(x)^2 + x^4 h(x).
\end{aligned}
\tag{3.1}
$$

We must find choices of the free coefficients such that $D_T(x) = \prod_{i=1}^{7}(\alpha^2 x - \rho_i)$, with each root non-zero. For $x = 0$, we have $\sum_t \left(\frac{2dt-D}{p}\right) = 0$. By Lemma 5, for x a root of D_T we have a contribution of $(p-1)\left(\frac{x^4}{p}\right) = (p-1)\left(\frac{\rho_i^4\alpha^{-8}}{p}\right) = p-1$; for all other x a contribution of $-\left(\frac{x^4\alpha^{-8}}{p}\right) = -1$. Hence summing over x and t yields $7(p-1) + \sum_{x\neq\rho_i,0} -1 = 6p$. Similar reasoning as before shows we can find integer solutions (we included the factor of α^2 to facilitate finding such solutions). We chose the coefficient of the x^4 term to be $T^2+2T+1 = (T+1)^2$, as this implies each curve E_t is isomorphic over $\mathbb{Q}$ to an elliptic curve E_t' (see Appendix B). As $\mathcal{E}$ is almost certainly not rational, the rank is exactly 6 if Tate's conjecture is true for the surface. If we only desire a lower bound for the rank, we can list the 6 points and calculate the determinant of the height matrix and see if they are independent.

3.2 Probable Rank 7, 8 Curves

We modify the previous construction to

$$\begin{aligned} y^2 &= x^3T^2 + 2g(x)T - h(x) \\ g(x) &= x^4 + ax^3 + bx^2 + cx + d, \ d \neq 0 \\ h(x) &= Ax^4 + Bx^3 + Cx^2 + Dx + E \end{aligned} \tag{3.2}$$

to obtain what should be higher rank curves over $\mathbb{Q}(T)$. Choosing appropriate quartics for $g(x), h(x)$ such that $D_T(x) = g^2(x)+x^3h(x)$ has eight distinct non-zero perfect square roots should yield a contribution of $8p$. As the coefficient of T^2 is x^3, we do not lose p from summing over non-roots of $D_T(x)$. By specializing to $T = a_2S^2+a_1S+a_0$ for some constants, we can arrange it so $y^2 = k^2(S)x^4 + \cdots$, and by the previous arguments obtain a cubic. Unfortunately, we can no longer explicitly evaluate $pA_{\mathcal{E}}(p)$ (because of the replacement $T \to a_2S^2 + a_1S + a_0$). As the method yields eight points for all s, we need only specialize and compute the height matrix. As we construct a rank 8 curve over $\mathbb{Q}(T)$ in §4 (when we generalize our construction), we do not provide the details here. Note, however, that sometimes there are obstructions and the rank is lower than one would expect (see §5).

4 Using Cubics and Quartics in T

Previously we used $y^2 = f(x,T)$, with f quadratic in T. The reason is that, for special x, we obtain $y_i^2 = s_i(x_i)^2(T-t_i)^2$. For such x, the t-sum is large (of size p); we then show for other x that the t-sum is small.

4.1 Idea of Construction

The natural generalization of our Discriminant Method is to consider $y^2 = f(x, T)$, with f of higher order in T. We first consider polynomials cubic in T. For a fixed x_i, we have the t-sum $\sum_{t(p)} \left(\frac{f(x_i,t)}{p}\right)$, and there are several possibilities:

(1) $f(x_i, T) = a(T - t_1)^3$. In this case, the t-sum will vanish, as $\left(\frac{(t-t_1)^3}{p}\right) = \left(\frac{t-t_1}{p}\right)$.
(2) $f(x_i, T) = a(T - t_1)^2(T - t_2)$. The t-sum will be $O(1)$, as for $t \neq t_1$ we have $\left(\frac{(t-t_1)^2(t-t_2)}{p}\right) = \left(\frac{t-t_2}{p}\right)$.
(3) $f(x_i, T) = a(T - t_1)(T - t_2)(T - t_3)$. This will in general be of size $\sqrt{p}$.
(4) $f(x_i, T) = a(T - t_1)(T^2 + bT + c)$, with the quadratic irreducible over $\mathbb{Z}/p\mathbb{Z}$. This happens when $b^2 - 4c$ is not a square mod p. This will in general be of size $\sqrt{p}$.
(5) $f(x_i, T) = aT^3 + bT^2 + cT + d$, with the cubic irreducible over $\mathbb{Z}/p\mathbb{Z}$. Again, this will in general be of size $\sqrt{p}$.

Thus, our method does not generalize to $f(x, T)$ cubic in T. The problem is we cannot reduce to $\left(\frac{(t-t_1)^{2n_1}\cdots(t-t_i)^{2n_i}}{p}\right)$. We therefore investigate $f(x, T)$ quartic in T. Consider, for simplicity, a curve $\mathcal{E}$ over $\mathbb{Q}(T)$ of the form:

$$y^2 \;=\; f(x, T) \;=\; A(x)T^4 + B(x)T^2 + C(x), \tag{4.3}$$

$A(x), B(x), C(x) \in \mathbb{Z}[x]$ of degree at most 4. The polynomial $AT^4 + BT^2 + C$ has discriminant $16AC(4AC - B^2)^2$. There are several possibilities for special choices of x giving rise to large t-sums (sums of size p):

(1) $A(x_i), B(x_i) \equiv 0 \bmod p$, $C(x_i)$ a non-zero square mod p. Then the t-summand is of the form c^2, contributing p.
(2) $A(x_i), C(x_i) \equiv 0 \bmod p$, $B(x_i)$ a non-zero square mod p. Then the t-summand is of the form $(bt)^2$, contributing $p - 1$.
(3) $B(x_i), C(x_i) \equiv 0 \bmod p$, $A(x_i)$ a non-zero square mod p. Then the t-summand is of the form $(at^2)^2$, contributing $p - 1$.
(4) $A(x_i)$ is a non-zero square mod p and $B(x_i)^2 - 4A(x_i)C(x_i) \equiv 0 \bmod p$. Then the t-summand is of the form $a^2(t^2 - t_1)^2$, contributing $p - 1$.

In the above construction, we are no longer able to calculate $A_{\mathcal{E}}(p)$ exactly. Instead, we construct curves where we believe $A_{\mathcal{E}}(p)$ is large. This is accomplished by forcing points to be on $\mathcal{E}$ which satisfy any of (1) through (4) above. As we are unable to evaluate the $A_{\mathcal{E}}(p)$ sums, we specialize and calculate height matrices to show the points are independent. Unfortunately, some of our constructions yielded 9 and 10 points on $\mathcal{E}$, but some of these points were linearly dependent on the others, or torsion points (see §5).

This method, with a quartic in T, can force a maximum number of 12 points on $\mathcal{E}$. It is possible to have 8 points from the vanishing of the discriminant (in t), and an additional 6 points from the simultaneous vanishing of pairs of $A(x), B(x), C(x)$; however, any common root of A or C with B is also a root of $B^2 - 4AC$, so there are at most 4 new roots arising from simultaneous vanishing, for a total of 12 possible points.

4.2 Rank (at least) 7 Curve

For appropriate choices of the parameters, the curve $\mathcal{E} : y^2 = A(x)T^4 + 4B(x)T^2 + 4C(x)$ over $\mathbb{Q}(T)$ with

$$\begin{aligned} A(x) &= a_1a_2a_3a_4(x-a_1)(x-a_2)(x-a_3)(x-a_4) \\ C(x) &= a_1a_2c_1c_2(x-a_1)(x-a_2)(x-c_1)(x-c_2) \\ B(x) &= a_1^2a_2^2(x-c_1)(x-c_2)(x-a_3)(x-a_4) \end{aligned} \tag{4.4}$$

has rank at least 7. We get 6 points from the common vanishing of A, B, C in pairs and an additional point from a factor of $B^2 - AC$. Choosing $a_1 = -25, a_2 = -5, a_3 = -10, a_4 = -1, c_1 = -9, c_2 = 15$ we find that the points

$$\begin{aligned} &(-25, 120000T),\ (-5, 10000T),\ (-10, 11250),\ (-1, 28800), \\ &(-9, 800T^2),\ (15, 20000T^2),\ (65/7, (540000T^2 - 2880000)/49) \end{aligned} \tag{4.5}$$

all lie on $\mathcal{E}$. Upon transforming to a cubic (see Appendix B), specializing to $T = 20$, and considering the minimal model, we found that these points are linearly independent (PARI calculates the determinant of the height matrix is approximately 37472). Note this is not a rational surface, as the coefficient of x in Weierstrass form is of degree 8.

4.3 Rank (at least) 8 Curve

For appropriate choices of the parameters, the curve $\mathcal{E} : y^2 = A(x)T^4 + B(x)T^2 + C(x)$ over $\mathbb{Q}(T)$ with

$$A(x) = x^4,\ B(x) = 2x(b_3x^3+b_2x^2+b_1x+b_0)+b^2,\ C(x) = x(b_3^2x^3+c_2x^2+c_1x+c_0)$$

has rank at least 8. As the coefficient of x^4 is $T^4 + 2b_3T^2 + b_3^2$, a perfect square, $\mathcal{E}$ can easily be transformed into Weierstrass form (see Appendix B). The common vanishing of A and C at $x = 0$ produces a point $S_0 = (0, bT)$ on $\mathcal{E}/\mathbb{Q}(T)$. Also notice that as before, if $B^2 - 4AC$ vanishes at $x = x_i$ then we can rewrite:

$$A(x_i)T^4 + B(x_i)T^2 + C(x_i) \;=\; A(x_i)\left(T^2 + \frac{B(x_i)}{2A(x_i)}\right)^2 \;=\; x_i^4\left(T^2 + \frac{B(x_i)}{2x_i^4}\right)^2 \tag{4.6}$$

Thus we obtain a point $P_{x_i} = (x_i, x_i^2(T^2 + B(x_i)/2x_i^4))$ on $\mathcal{E}$. We chose constants b_i, b an c_i so that

$$B^2 - 4AC \;=\; (x-1)(x+1)(x-4)(x+4)(x-9)(x+9)(x-16), \tag{4.7}$$

and obtain a curve $\mathcal{E}$ over $\mathbb{Q}(T)$ with coefficients:

$$\begin{aligned} A \;&=\; x^4, \quad B(x) = -\frac{5852770213}{382205952}x^4 + \frac{89071}{36864}x^3 - \frac{89233}{1152}x^2 - \frac{9}{2}x + 144, \\ C(x) \;&=\; \frac{34254919166180065369}{584325558976905216}x^4 - \frac{528356915749387}{28179280429056}x^3 \\ &\quad + \frac{527067904642903}{880602513408}x^2 - \frac{5881576729}{169869312}x. \end{aligned} \tag{4.8}$$

As discussed above, the curve $\mathcal{E}$ given by (4.8) has 8 rational points over $\mathbb{Q}(T)$, namely S_0 and P_{x_i} for $x_i = \pm 1,\ \pm 4,\ \pm 9, 16$. As $\mathcal{E}$ is not a rational surface, and as we cannot evaluate $A_{\mathcal{E}}(p)$ exactly, we need to make sure the points are linearly independent. Specializing to $T = 1$ yields the elliptic curve with minimal model

$$\begin{aligned} E_1:\ y^2 \;&=\; x^3 - x^2 - \alpha x + \beta \\ \alpha \;&=\; 357917711928106838175050781865 \\ \beta \;&=\; 8790806811671574287759992288018136706011725. \end{aligned} \tag{4.9}$$

The eight points of E_T at $T = 1$ are linearly independent on $E_1/\mathbb{Q}$ (PARI calculates the determinant of the height matrix to be about 124079248627.08), proving $\mathcal{E}$ does have rank at least 8 over $\mathbb{Q}(T)$.

5 Linear Dependencies Among Points

Not all choices of $A(x), B(x), C(x)$ which yield r points on the curve $\mathcal{E} : y^2 = A(x)T^4 + 4B(x)T^2 + 4C(x)$ actually give a curve of rank at least r over $\mathbb{Q}(T)$. We found many examples giving 9 and 10 points by choosing $A(x) = C(x)$ so that $B^2 - AC$ factors nicely, and then searching through prospective roots of this quantity as well as roots of $A(x) = C(x)$. One such curve giving 10 points arises from

$$
\begin{aligned}
A(x) &= C(x) = (x-1)^2(2x-1)^2 \\
B(x) &= 12316x^4 + 2346x^3 - 239x^2 - 24x + 1,
\end{aligned} \tag{5.10}
$$

and has the following points on it

$$
\begin{gathered}
(0, T^2+2),\ \left(\frac{-1}{19}, \frac{420}{361}(T^2+2)\right),\ \left(\frac{-1}{4}, \frac{15}{8}(T^2+2)\right), \\
\left(\frac{1}{9}, \frac{56}{81}(T^2+2)\right),\ \left(\frac{-1}{7}, \frac{72}{49}(T^2-2)\right),\ \left(\frac{-1}{5}, \frac{42}{25}(T^2-2)\right), \\
\left(\frac{1}{11}, \frac{90}{121}(T^2-2)\right),\ \left(\frac{1}{16}, \frac{105}{128}(T^2-2)\right),\ (1, 240T),\ \left(\frac{1}{2}, 63T\right).
\end{gathered} \tag{5.11}
$$

It can be shown, however, that upon translating to a cubic only the (translated versions of the) second, third, fifth, sixth, and ninth of these points are independent over $\mathbb{Q}(T)$. While the contribution from these points makes $A_{\mathcal{E}}(p)$ want to be large, this is not reflected by a large rank.

6 Using Higher Degree Polynomials

Let $f(x,T)$ be a polynomial of degree 3 or 4 in x and arbitrary degree in T and let $\mathcal{E}$ be the elliptic curve over $\mathbb{Q}(T)$ given by $y^2 = f(x,T)$ (with the coefficient of x^4 a perfect square or zero). The remarks at the beginning of Section 4 about cubics suggest that we should look for polynomials $f(x,T)$ with even degree in T, say $\deg_T(f) = 2n$.

The nice feature of quadratics and biquadratics that we used in the previous constructions was the fact that a zero of the discriminant indicates that the polynomial $f(x,T)$ factors as a perfect square. However, when f is of arbitrary degree $2n$ in T this is no longer true: a zero of the discriminant $D_T(x)$ indicates just a multiple root. However, in the most general case, there exist n quantities $D_{i,T}(x)$ such that their common vanishing at $x = x_0$ implies that $f(x,T)$ factors as a perfect square. As an example we look at a quartic of the form $f(x,T) = A^2T^4 + BT^3 + CT^2 + DT + E^2$, where $\deg_x(A,E) \le 2$ and $\deg_x(B,C,D) \le 4$. This can be rewritten as:

$$
\begin{aligned}
& A^2T^4 + 2AT^2\left(\frac{Bt}{2A} + \frac{C}{2A} - \frac{B^2}{8A^3}\right) + \left(\frac{BT}{2A} + \frac{C}{2A} - \frac{B^2}{8A^3}\right)^2 \\
& \quad + \left(D - \frac{B}{A}\left(\frac{C}{2A} - \frac{B^2}{8A^3}\right)\right)T - \left(\frac{C}{2A} - \frac{B^2}{8A^3}\right)^2 + E^2.
\end{aligned} \tag{6.12}
$$

The last two terms are the ones which are keeping the polynomial from being a perfect square. Thus, if

$$D - \frac{B}{A}\left(\frac{C}{2A} - \frac{B^2}{8A^3}\right) \ = \ 0, \quad E^2 - \left(\frac{C}{2A} - \frac{B^2}{8A^3}\right)^2 \ = \ 0 \tag{6.13}$$

then the polynomial f will be a square. This is equivalent to

$$\begin{aligned} D_{1,T} &= 8A^4D - 4A^2BC + B^3 = 0 \\ D_{2,T} &= 64A^6E^2 - 16A^4C^2 - B^4 + 8A^2CB^2 = 0. \end{aligned} \tag{6.14}$$

Note that if B=D=0, the conditions that these polynomials impose reduce to the usual discriminant. Also, $\deg_x(D_{1,T}) \leq 12$, $\deg_x(D_{2,T}) \leq 16$, so we could get up to 12 points of common vanishing of the D_i. The authors have tried to find suitable constants without success, due to the complexity of the Diophantine equations.

Acknowledgements

We thank Vitaly Bergelson, Michael Hunt, James Mailhot, David Rohrlich, Mustafa Sahin, and Warren Sinnott for many enlightening conversations, and the referee for a very careful reading of the manuscript. The third named author also wishes to thank Boston University for its hospitality, where much of the final write-up was prepared.

A Sums of Legendre Symbols

For completeness, we provide proofs of the quadratic Legendre sums that are used in our constructions.

A.1 Factorizable Quadratics in Sums of Legendre Symbols

Lemma 4 *For $p > 2$*

$$S(n) \ = \ \sum_{x=0}^{p-1}\left(\frac{n_1+x}{p}\right)\left(\frac{n_2+x}{p}\right) \ = \ \begin{cases} p-1 & \text{if } p|(n_1-n_2) \\ -1 & \text{otherwise.} \end{cases} \tag{A.1}$$

Proof: Translating x by $-n_2$, we need only prove the lemma when $n_2 = 0$. Assume $(n,p) = 1$ as otherwise the result is trivial. For $(a,p) = 1$ we have:

$$\begin{aligned}
S(n) &= \sum_{x=0}^{p-1} \left(\frac{n+x}{p}\right)\left(\frac{x}{p}\right) \\
&= \sum_{x=0}^{p-1} \left(\frac{n+a^{-1}x}{p}\right)\left(\frac{a^{-1}x}{p}\right) \\
&= \sum_{x=0}^{p-1} \left(\frac{an+x}{p}\right)\left(\frac{x}{p}\right) \ = \ S(an)
\end{aligned} \tag{A.2}$$

Hence

$$\begin{aligned}
S(n) &= \frac{1}{p-1}\sum_{a=1}^{p-1}\sum_{x=0}^{p-1} \left(\frac{an+x}{p}\right)\left(\frac{x}{p}\right) \\
&= \frac{1}{p-1}\sum_{a=0}^{p-1}\sum_{x=0}^{p-1} \left(\frac{an+x}{p}\right)\left(\frac{x}{p}\right) - \frac{1}{p-1}\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)^2 \\
&= \frac{1}{p-1}\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)\sum_{a=0}^{p-1}\left(\frac{an+x}{p}\right) - 1 \\
&= 0 - 1 \ = \ -1.
\end{aligned} \tag{A.3}$$

□

We need $p > 2$ as we used $\sum_{a=0}^{p-1}\left(\frac{an+x}{p}\right) = 0$ for $(n,p) = 1$. This is true for all odd primes (as there are $\frac{p-1}{2}$ quadratic residues, $\frac{p-1}{2}$ non-residues, and 0); for $p = 2$, there is one quadratic residue, no non-residues, and 0.

A.2 General Quadratics in Sums of Legendre Symbols

Lemma 5 (Quadratic Legendre Sums) *Assume a and b are not both zero mod p and $p > 2$. Then*

$$\sum_{t=0}^{p-1}\left(\frac{at^2+bt+c}{p}\right) \ = \ \begin{cases} (p-1)\left(\frac{a}{p}\right) & \text{if } p|(b^2-4ac) \\ -\left(\frac{a}{p}\right) & \text{otherwise.}\end{cases} \tag{A.4}$$

Proof: Assume $a \not\equiv 0(p)$ as otherwise the proof is trivial. By translating t, we reduce to the case $\sum_{t(p)}\left(\frac{t^2-\delta}{p}\right)$, where $\delta = b^2 - 4ac$ is the discriminant. If $p|\delta$, the claim is clear. For $p \not|\delta$ the claim is equivalent to counting the number of solutions to $t^2 - \delta \equiv y^2 \bmod p$, or $(t-y)(t+y) \equiv \delta \bmod p$. Letting $u = t - y$

and $v = t + y$ we see there are $p-1$ pairs (u,v) with $\delta \equiv uv \bmod p$ (as $\delta \not\equiv 0$). Using that the pairs (u,v) are in bijection with the pairs (t,y), the proof is then easily completed on distinguishing between the case $\left(\frac{-\delta}{p}\right) = -1$ and $\left(\frac{-\delta}{p}\right) = 1$. $\square$

Proof: Assume $a \not\equiv 0(p)$ as otherwise the proof is trivial. Let $\delta = 4^{-1}(b^2 - 4ac)$. Then

$$\begin{aligned}
\sum_{t=0}^{p-1} \left(\frac{at^2+bt+c}{p}\right) &= \sum_{t=0}^{p-1} \left(\frac{a^{-1}}{p}\right)\left(\frac{a^2t^2+bat+ac}{p}\right) \\
&= \sum_{t=0}^{p-1} \left(\frac{a}{p}\right)\left(\frac{t^2+bt+ac}{p}\right) \\
&= \sum_{t=0}^{p-1} \left(\frac{a}{p}\right)\left(\frac{(t+2^{-1}b)^2 - 4^{-1}(b^2-4ac)}{p}\right) \\
&= \left(\frac{a}{p}\right) \sum_{t=0}^{p-1} \left(\frac{t^2-\delta}{p}\right) \qquad \text{(A.5)}
\end{aligned}$$

If $\delta \equiv 0(p)$ we get $p-1$. If $\delta \equiv \eta^2, \eta \neq 0$, then by Lemma 4

$$\sum_{t=0}^{p-1} \left(\frac{t^2-\delta}{p}\right) = \sum_{t=0}^{p-1} \left(\frac{t-\eta}{p}\right)\left(\frac{t+\eta}{p}\right) = -1. \qquad \text{(A.6)}$$

We note that $\sum_{t=0}^{p-1} \left(\frac{t^2-\delta}{p}\right)$ is the same for all non-square δ's (let g be a generator of the multiplicative group, $\delta = g^{2k+1}$, change variables by $t \to g^k t$). Denote this sum by S, the set of non-zero squares mod p by $\mathcal{R}$, and the non-squares mod p by $\mathcal{N}$. Since $\sum_{\delta=0}^{p-1} \left(\frac{t^2-\delta}{p}\right) = 0$ we have

$$\begin{aligned}
\sum_{\delta=0}^{p-1}\sum_{t=0}^{p-1} \left(\frac{t^2-\delta}{p}\right) &= \sum_{t=0}^{p-1} \left(\frac{t^2}{p}\right) + \sum_{\delta\in\mathcal{R}}\sum_{t=0}^{p-1} \left(\frac{t^2-\delta}{p}\right) + \sum_{\delta\in\mathcal{N}}\sum_{t=0}^{p-1} \left(\frac{t^2-\delta}{p}\right) \\
&= (p-1) + \frac{p-1}{2}(-1) + \frac{p-1}{2} S = 0 \qquad \text{(A.7)}
\end{aligned}$$

Hence $S = -1$, proving the lemma. $\square$

B Converting from Quartics to Cubics

We record two useful transformations from quartics to cubics. In all theorems below, all quantities are rational.

Theorem 6 *If the quartic curve* $y^2 = x^4 - 6cx^2 + 4dx + e$ *has a rational point, then it is equivalent to the cubic curve* $Y^2 = 4X^3 - g_2X - g_3$*, where*

$$g_2 \;=\; e + 3c^2, \qquad g_3 \;=\; -ce - d^2 + c^3, \tag{B.1}$$

and

$$2x \;=\; (Y - d)/(X - c), \qquad y \;=\; -x^2 + 2X + c. \tag{B.2}$$

See [Mor], page 77. Note that if the leading term of the quartic is a^2x^4, one can send $y \to y/a$ and $x \to x/a$.

Theorem 7 *The quartic* $v^2 = au^4 + bu^3 + cu^2 + du + q^2$ *is equivalent to the cubic* $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$*, where*

$$a_1 = d/q, \quad a_2 = c - (d^2/4q^2), \quad a_3 = 2qb, \quad a_4 = -4q^2a, \quad a_6 = a_2a_4 \tag{B.3}$$

and

$$x \;=\; \frac{2q(v+q)+du}{u^2}, \qquad y \;=\; \frac{4q^2(v+q)+2q(du+cu^2)-(d^2u^2/2q)}{u^3}. \tag{B.4}$$

The point $(u, v) = (0, q)$ *corresponds to* $(x, y) = \infty$ *and* $(u, v) = (0, -q)$ *corresponds to* $(x, y) = (-a_2, a_1a_2 - a_3)$*.*

See [Wa], page 37.

References

[Fe1] S. Fermigier, *Étude expérimentale du rang de familles de courbes elliptiques sur* $\mathbb{Q}$, Exper. Math. **5** (1996), 119–130.

[Fe2] S. Fermigier, *Une courbe elliptique définie sur* $\mathbb{Q}$ *de rang* ≥ 22, Acta Arith. **82** (1997), no. 4, 359-363.

[Mes1] J. Mestre, *Courbes elliptiques de rang* $\geq$ *11 sur* $\mathbb{Q}(T)$, C. R. Acad. Sci. Paris, ser. 1, **313** (1991), 139–142.

[Mes2] J. Mestre, *Courbes elliptiques de rang* $\geq$ *12 sur* $\mathbb{Q}(T)$, C. R. Acad. Sci. Paris, ser. 1, **313** (1991), 171–174.

[Mil1] S. J. Miller, 1- *and* 2-*Level Densities for Families of Elliptic Curves: Evidence for the Underlying Group Symmetries*, Ph.D. Thesis, Princeton University, 2002.
`http://www.math.princeton.edu/~sjmiller/thesis/thesis.html`

[Mil2] S. J. Miller, *Variation in the number of points on elliptic curves and applications to excess rank*, to appear in Comptes Rendus Mathématiques.

[Mir] R. Miranda, *The Basic Theory of Elliptic Surfaces*, Dottorato di Ricerca in Matematica, Dipartmento di Matematica dell'Universit'a di Pisa, ETS Editrice, 1989.

[Mor] Mordell, *Diophantine Equations*, Academic Press, New York, 1969,

[Moree] P. Moree, *Primitive root producing quadratics*, preprint. `http://arxiv.org/pdf/math.NT/0406033`

[Na1] K. Nagao, *Construction of high-rank elliptic curves*, Kobe J. Math. **11** (1994), 211–219.

[Na2] K. Nagao, $\mathbb{Q}(T)$*-rank of elliptic curves and certain limit coming from the local points*, Manuscr. Math. **92** (1997), 13–32.

[RS] M. Rosen and J. Silverman, *On the rank of an elliptic surface*, Invent. Math. **133** (1998), 43–67.

[RuS] K. Rubin and A. Silverberg, *Ranks of elliptic curves*, Bulletin of the American Mathematical Society **39** (2002), no. 4, 455–474.

[Sh1] T. Shioda, *On the Mordell-Weil Lattices*, Comment. Math. Univ. St. Pauli **39** (1990), 211–240.

[Sh2] T. Shioda, *Construction of elliptic curves with high-rank via the invariants of the Weyl groups*, J. Math. Soc. Japan **43** (1991), 673–719.

[Si1] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, Berlin - New York, 1986.

[Si2] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, Berlin - New York, 1994.

[Ta] J. Tate, *Algebraic cycles and the pole of zeta functions*, Arithmetical Algebraic Geometry, Harper and Row, New York, 1965, 93–110.

[Wa] L. Washington, *Elliptic Curves: Number Theory and Cryptography (Discrete Mathematics and Its Applications)*, Chapman & Hall, 2003.