Constructing families of moderate-rank elliptic curves over number fields

David Mehrle[1], Steven J. Miller[2], Tomer Reiter[3],
Joseph Stahl[4], and Dylan Yott[4]

[1]Cornell University
[2]Williams College
[3]Emory University
[4]University of California, Berkeley

Constructing families of moderate-rank elliptic curves over number fields

David Mehrle[* 1], Steven J. Miller[2], Tomer Reiter[3],
Joseph Stahl[4], and Dylan Yott[4]

[1]Cornell University
[2]Williams College
[3]Emory University
[4]University of California, Berkeley

ABSTRACT. We generalize a construction of families of moderate rank elliptic curves over $\mathbb{Q}$ to number fields $K/\mathbb{Q}$. The construction, originally due to Scott Arms, Álvaro Lozano-Robledo and Steven J. Miller, invokes a theorem of Rosen and Silverman to show that computing the rank of these curves can be done by controlling the average of the traces of Frobenius; the construction for number fields proceeds in essentially the same way. One novelty of this method is that we can construct families of moderate rank without having to explicitly determine points and calculating determinants of height matrices.

1. INTRODUCTION

If E is an elliptic curve over $\mathbb{Q}$, then the associated group of rational solutions, the Mordell-Weil group $E(\mathbb{Q})$, is finitely generated. The rank of this group is a very interesting and well-studied quantity in modern number theory; the famous Birch and Swinnerton-Dyer conjecture states that its rank equals the order of vanishing of the elliptic curve's L-function at the central point. We assume the reader is familiar with the basics of the subject; good references are [Kn, Si1, Si2, SiTa].

It is unknown if the rank of an elliptic curve over $\mathbb{Q}$ can be arbitrarily large. It is an interesting and difficult problem to find examples or families of curves with large rank. To date the best known results are due to Elkies, who constructed an elliptic curve of rank at least 28 (or exactly 28 subject to the Generalized Riemann Hypothesis [KSW]) and a family of elliptic curves of rank at least 18; see [BMSW] for a survey of recent results on the distribution of ranks of curves in families, and conjectures for their behavior.

Many of the constructions of high rank families of elliptic curves begin by forcing points to lie in the curves, and then calculating the associated height matrices to verify that they

---

are linearly independent (see for example [Mes1, Mes2, Na1]). We pursue an alternative approach introduced by Arms, Lozano-Robledo and Miller [AL-RM]. Briefly, their strategy is to use a result of Rosen and Silverman [RoSi], which converts the problem of constructing families of elliptic curves with large rank to finding associated Legendre sums that are large. While in general these sums are intractable, for some carefully constructed families these can be determined in closed form, which allows us to determine the rank of the families *without* having to list points and compute height matrices. Our main result is to generalize the work in [AL-RM] from elliptic curves over $\mathbb{Q}$ to elliptic curves over number fields. Specifically, we show the following.

Theorem 1.1. *Let K be a number field. Then there exists an elliptic curve $\mathcal{E}$ over $K(T)$ with $j(\mathcal{E}) \notin \mathbb{Q}(T)$ such that the rank of $\mathcal{E}$ over $K(T)$ is exactly 6.*

By specializing to $T = t$ for some $t \in K$, we obtain curves $\mathcal{E}_t$ over K from the curve $\mathcal{E}$ over $K(T)$. Silverman's specialization theorem [Si2, Theorem 11.4] tells us that for all but finitely many $t \in T$, the rank can only possibly increase.

Corollary 1.2. *Let K be a number field. There are infinitely many elliptic curves over K with rank at least 6.*

Remark. Arms et al. [AL-RM] construct infinitely many elliptic curves over $\mathbb{Q}$ with rank at least 6. By base-extending these curves to K, we may trivially obtain infinitely many elliptic curves over K with rank at least 6. Our contribution is to construct curves that are defined over K but *not* defined over $\mathbb{Q}$; this is evident because the j-invariant of curves we construct in Theorem 1.1 lies in $K(T)$ but not in $\mathbb{Q}(T)$.

2. The Construction

Let K be a number field and $\mathcal{O}_K$ its ring of integers. Let $\mathcal{E}$ be the elliptic curve over $K(T)$ defined by

$$\mathcal{E}: \quad y^2 + a_1(T)xy + a_3(T)y = x^3 + a_2(T)x^2 + a_4(T)x + a_6(T),$$

where $a_i(T) \in \mathcal{O}_K(T)$. By Silverman's specialization theorem [Si2, Theorem 11.4], for all but finitely many $t \in \mathcal{O}_K$ the Mordell-Weil rank of the fiber $\mathcal{E}_t$ over K is at least that of the rank of $\mathcal{E}$ over $\mathcal{O}_K(T)$. Therefore, if we can compute the rank of $\mathcal{E}$, we have a family of infinitely many curves $\mathcal{E}_t$ over K with at least the rank of $\mathcal{E}$.

To that end, for $\mathcal{E}$ as above and $\mathfrak{p}$ a prime of good reduction in $\mathcal{O}_K$ (we do not consider the bad primes here), we define the average

$$A_{\mathcal{E}}(\mathfrak{p}) := \frac{1}{N(\mathfrak{p})} \sum_{t \in \mathcal{O}_K/\mathfrak{p}} a_t(\mathfrak{p}), \tag{1}$$

where $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ and $a_t(\mathfrak{p}) = N(\mathfrak{p}) + 1 - \#\mathcal{E}_t(\mathcal{O}_K/\mathfrak{p})$. Nagao [Na2] conjectured that these sums are related to the rank of the family of elliptic curves. Rosen and Silverman proved this conjecture when $\mathcal{E}$ is a rational elliptic surface [RoSi]. Specifically, whenever Tate's conjecture holds (which is known for $K3$ surfaces over certain fields [Sr]) we have

$$\lim_{X \to \infty} \frac{1}{X} \sum_{\mathfrak{p}: N(\mathfrak{p}) \leq X} -A_{\mathcal{E}}(\mathfrak{p}) \log(N(\mathfrak{p})) = \operatorname{rank} \mathcal{E}(K(T)). \tag{2}$$

Below we study certain carefully chosen families where we are able to prove that $A_{\mathcal{E}}(\mathfrak{p}) = -6$ for almost all primes $\mathfrak{p}$, thus proving these families have rank 6. To calculate the limit (2), we appeal to the Landau Prime Ideal Theorem, a generalization of the Prime Number Theorem.

Theorem 2.1 (Landau Prime Ideal Theorem [Lan]). *We have*

$$\sum_{\mathfrak{p}:\, N(\mathfrak{p}) \leq X} \log(N(\mathfrak{p})) \sim X.$$

Assuming we can produce $\mathcal{E}$ such that $A_{\mathcal{E}}(\mathfrak{p}) = -6$ for almost all $\mathfrak{p}$, then combining the Landau Prime Ideal Theorem with equation (2) it follows that

$$\text{rank } \mathcal{E}(K(T)) \;=\; 6,$$

which completes the proof of Theorem 1.1.

So it remains to show that we can produce an $\mathcal{E}$ such that $A_{\mathcal{E}}(\mathfrak{p}) = -6$. As in Equation 2.2 of [AL-RM], define

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

Notice that $D_T(x)$ is one-quarter of the discriminant of $f(x,T)$, considered as a quadratic polynomial in T. When we specialize to a particular $t \in \mathcal{O}_K$, we write $D_t(x)$ for the one-quarter of the discriminant of $f(x,t)$. As a degree six polynomial in x, write $r_1, r_2, \ldots, r_6$ for the roots of $D_T(x)$. We will see that the number of distinct, nonzero roots of $D_T(x)$ control the rank of the curve.

In order to show our claim for the elliptic curve $y^2 = f(x,T)$, we must pick six distinct, nonzero roots of $D_T(x)$ which are squares in $\mathcal{O}_K$. We also need the analogue of equation 2.1 from [AL-RM] for number fields, which can be stated as follows. For a, b both not zero mod $\mathfrak{p}$ and $N(\mathfrak{p}) > 2$, then for $t \in \mathcal{O}_K$

$$
\sum_{t \in \mathcal{O}_K/\mathfrak{p}} \left(\frac{at^2 + bt + c}{\mathfrak{p}} \right) =
\begin{cases}
(N(\mathfrak{p}) - 1)\left(\frac{a}{\mathfrak{p}} \right) & \text{if } (b^2 - 4ac) \in \mathfrak{p} \\
-\left(\frac{a}{\mathfrak{p}} \right) & \text{otherwise.}
\end{cases}
\tag{4}
$$

Note that (4) is already demonstrated when $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_p$ is a finite field of prime order p in Lemma A.2 of [AL-RM] (they give two proofs; the result also appears in [BEW]). Therefore, it suffices to show (4) when $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_q$ is a finite field of order $q = p^r$ for p prime and $r > 1$; we do so in Proposition 3.1 in the next section.

Write $\mathbb{F}_q = \mathcal{O}_K/\mathfrak{p}$ for the residue field of $\mathcal{O}_K$ at $\mathfrak{p}$. We have for the fiber of the elliptic surface $y^2 = f(x,T)$ at $T = t$

$$
a_t(\mathfrak{p}) = - \sum_{x \in \mathcal{O}_K/\mathfrak{p}} \left(\frac{f(x,t)}{\mathfrak{p}} \right) = - \sum_{x \in \mathcal{O}_K/\mathfrak{p}} \left(\frac{x^3 t^2 + 2g(x)t - h(x)}{\mathfrak{p}} \right),
$$

where $\left(\frac{\cdot}{\mathfrak{p}}\right)$ is the Legendre symbol of the residue field $\mathcal{O}_K/\mathfrak{p}$.

Now we study $-N(\mathfrak{p})A_{\mathcal{E}}(p) = \sum_{t\in\mathcal{O}_K/\mathfrak{p}} a_t(\mathfrak{p}) = \sum_{x,t\in\mathcal{O}_K/\mathfrak{p}}\left(\frac{f(x,t)}{\mathfrak{p}}\right)$ to calculate $A_{\mathcal{E}}(\mathfrak{p})$, as in equation (1). When $x\in\mathfrak{p}$, the t-sum vanishes unless $c\in\mathfrak{p}$ — it is just $\sum_{t\in\mathcal{O}_K/\mathfrak{p}}\left(\frac{2ct-D}{\mathfrak{p}}\right)$.

Assume now $x\notin\mathfrak{p}$. Then by (4), we have

$$\sum_{t\in\mathcal{O}_K/\mathfrak{p}}\left(\frac{x^3t^2+2g(x)t-h(x)}{\mathfrak{p}}\right) = \begin{cases}(N(\mathfrak{p})-1)\left(\frac{x^3}{\mathfrak{p}}\right) & \text{if } D_t(x)\in\mathfrak{p}\\ -\left(\frac{x^3}{\mathfrak{p}}\right) & \text{otherwise.}\end{cases}$$

If the roots $r_1, r_2, \ldots, r_6$ are squares in $\mathcal{O}_K$, then their contribution to the rank will be

$$(N(\mathfrak{p})-1)\left(\frac{r_i^3}{\mathfrak{p}}\right).$$

If the r_i are not squares, then $\left(\frac{r_i}{\mathfrak{p}}\right)$ will be 1 for half of the primes of $\mathcal{O}_K$ and -1 for the other half, and therefore yield no net contribution to the rank.

So assume that we may choose coefficients a,b,c,A,B,C,D such that $D_T(x)$ has six distinct, non-zero roots $r_i\in\mathcal{O}_K$, each of which is a square. Write $r_i=\rho_i^2$ for $i=1,\ldots,6$. Then

$$-N(\mathfrak{p})A_{\mathcal{E}}(\mathfrak{p}) = \sum_{\substack{x\in\mathcal{O}_K/\mathfrak{p}\\t\in\mathcal{O}_K/\mathfrak{p}}}\left(\frac{f(x,t)}{\mathfrak{p}}\right) = \sum_{\substack{x\in\mathcal{O}_K/\mathfrak{p}\\t\in\mathcal{O}_K/\mathfrak{p}}}\left(\frac{x^3t^2+2g(x)t-h(x)}{\mathfrak{p}}\right)$$

$$= \sum_{\substack{x:\,D_t(x)\in\mathfrak{p}\\t\in\mathcal{O}_K/\mathfrak{p}}}\left(\frac{f(x,t)}{\mathfrak{p}}\right) + \sum_{\substack{x:\,D_t(x)\notin\mathfrak{p}\\t\in\mathcal{O}_K/\mathfrak{p}}}\left(\frac{f(x,t)}{\mathfrak{p}}\right)$$

$$= 6(N(\mathfrak{p})-1) - \sum_{x:\,D_t(x)\notin\mathfrak{p}}\left(\frac{x^3}{\mathfrak{p}}\right)$$

$$= 6(N(\mathfrak{p})-1)+6 = 6N(\mathfrak{p})$$

Hence, $-N(\mathfrak{p})A_{\mathcal{E}}(\mathfrak{p}) = 6N(\mathfrak{p})$. Therefore $A_{\mathcal{E}}(\mathfrak{p}) = -6$, completing the proof of Theorem 1.1.

Now we must find $a,b,c,A,B,C,D\in\mathcal{O}_K$ such that $D_T(x)$ has six distinct, nonzero roots $r_i=\rho_i^2$:

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

In practice, we will choose roots ρ_i^2 and then determine the polynomial $D_T(x)$; and from it, the coefficients a,b,c,A,B,C,D. Note that in the above we are free to choose B,C,D, so

matching coefficients for the x^5, x^4 and x^3 terms do not add any additional constraints. So we must simultaneously solve the following three equations in $\mathcal{O}_K$:

$$2ac + b^2 = R_2 A,$$
$$2bc = R_1 A,$$
$$c^2 = R_0 A.$$

So long as this system of Diophantine equations is solvable in $\mathcal{O}_K$, we may construct such an elliptic surface. In section 4 below, we provide some examples of elliptic surfaces over number fields.

3. Quadratic Legendre Sums

The following proposition on quadratic Legendre sums in finite fields is the generalization of Lemma A.1 from [AL-RM] to number fields (see also [BEW]). Let $q = p^r$ be an odd prime power, and assume $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_q$ is a finite field with q elements. Let $\left(\frac{\cdot}{q}\right)$ denote the $\mathbb{F}_q$-Legendre symbol which indicates whether or not an element of $\mathbb{F}_q$ is a square.

Proposition 3.1. *If $a \in \mathcal{O}_K$ is not zero modulo $\mathfrak{p}$, then*

$$\sum_{t \in \mathbb{F}_q} \left(\frac{at^2 + bt + c}{q} \right) = \begin{cases} (q-1)\left(\frac{a}{q}\right) & \text{if } b^2 - 4ac \equiv 0 \text{ mod } p \\ -\left(\frac{a}{q}\right) & \text{otherwise.} \end{cases}$$

Proof. The first case is straightforward, as if $b^2 - 4ac \equiv 0$ mod $\mathfrak{p}$, then $at^2 + bt + c = a(t - t')^2$ for some $t' \in \mathbb{F}_q$, and each of the terms in the sum except t' contribute $\left(\frac{a}{q}\right)$, and t' contributes 0.

For the other case, when $b^2 - 4ac \not\equiv 0$ mod $\mathfrak{p}$, we first reinterpret the sum as counting points on the conic $C : s^2 = at^2 + bt + c$ in the following way:

$$\#C(\mathbb{F}_q) = \sum_{t \in \mathbb{F}_q} \left(1 + \left(\frac{at^2 + bt + c}{q} \right) \right) = q + S.$$

Here S is the sum of interest. It is well-known that a nondegenerate conic of this particular form always has a rational point over $\mathbb{F}_q$ when q is a power of an odd prime [E], [Su, Theorem 3.4]. From this, we may parameterize all rational points using some line that does not meet the original rational point. This gives at most $q + 1$ points on the curve. However, this parametrization introduces a denominator that is possibly quadratic in t, which means at most 2 rational points on the line might not correspond to rational points on the curve. Thus we have

$$q - 1 \ \leq \ \#C(\mathbb{F}_q) \ \leq \ q + 1,$$

which gives

$$-1 \ \leq \ S \ \leq \ 1.$$

To determine the value of S, we compute it modulo p. By Euler's criterion in finite fields:

$$S \equiv \sum_{t \in \mathbb{F}_q} (at^2 + bt + c)^{\frac{q-1}{2}} \equiv \sum_{t \in \mathbb{F}_q} \left(\frac{a}{q}\right) t^{q-1} + r(t) \equiv -\left(\frac{a}{q}\right) + \sum_i r_i \sum_{t \in \mathbb{F}_q} t^i,$$

where $r(t)$ is a polynomial of degree $< q - 1$, and r_i are the roots of $D_t(\mathfrak{p})$, as above. Each of the inner sums $\sum_{t \in \mathbb{F}_q} t^i$ is 0, since $i < q - 1$, so one of the terms is nonzero, but the sum is stable under multiplication by any of its summands. Thus $S \equiv -\left(\frac{a}{q}\right)$ (mod p). Since $-1 \le S \le 1$, we have $S = -\left(\frac{a}{q}\right)$, as desired. $\square$

4. Examples

Let K be an arbitrary number field. Theorem 1.1 claims that we may produce elliptic curves of rank 6 over K; we provide a recipe to produce these curves over number fields in this section.

As in [AL-RM, Section 2.2], we choose $A = 64R_0^3$ for simplicity. This choice is convenient, because it allows us to solve

$$
\begin{aligned}
c^2 &= 64R_0^3 &\Rightarrow c &= 8R_0^3 \\
2bc &= 64R_0^3 R_1 &\Rightarrow b &= 4R_0 R_1 \\
2ac + b^2 &= 64R_0^3 R_2 &\Rightarrow a &= 4R_0 R_2 - R_1^2.
\end{aligned}
$$

Additionally, we may solve for B, C, D in terms of $R_0, \dots, R_5$. Altogether, we have

$$
\begin{aligned}
a &= 4R_0 R_2 - R_1^2 \\
b &= 4R_0 R_1 \\
c &= 8R_0^2 \\
A &= 64R_0^3 \\
B &= AR_5 - 2a \\
C &= AR_4 - a^2 - 2b \\
D &= AR_3 - 2ab - 2c
\end{aligned}
\tag{6}
$$

The above determines the coefficients of the elliptic curve defined by the equations (3) in terms of the roots $r_i = \rho_i^2$ of the discriminant $D_T(x)$, as in (5).

Expanding the first line of (3), we arrive at the following equation for the elliptic curve.

$$y^2 = x^3 + (2aT - B)x^2 + (2bT - C)(T^2 + 2T - A + 1)x + (2cT - D)(T^2 + 2T - A + 1)^2 \tag{7}$$

To produce curves over K, we may use the following recipe:

- choose six squares $r_1 = \rho_1^2, \dots, r_6 = \rho_6^2$ in K to be the roots of $D_T(x)$;

- solve for $R_0, \dots, R_5$ as the coefficients of the degree-six polynomial $D_T(x)$;

- use (6) to find a, b, c, A, B, C, D;

- plug these values into (7) to determine the equation for the elliptic curve.

- Specialize at $T = t$ for some $t \in K$. For generic choices of t, this specializes to an elliptic curve of rank at least 6, by Silverman's specialization theorem [Si2, Theorem 11.4].

We carry out this procedure for a few choices of number fields below. The interested reader may find a Sage [S] worksheet for these computations in the attached data files.

Example 4.1. Let $K = \mathbb{Q}$. In [AL-RM, Theorem 2.1], a rank 6 elliptic surface $\mathcal{E}$ over $\mathbb{Q}(T)$ with equation as in (7) and $r_\ell = \ell^2$, for $\ell = 1, 2, \ldots, 6$.

$$
\begin{aligned}
a &= 166601111104, & A &= 8916100448256000000, \\
b &= -1603174809600, & B &= -811365140824616222208, \\
c &= 2149908480000, & C &= 26497490347321493520384, \\
& & D &= -3431075943454488813363200.
\end{aligned}
$$

Example 4.2. Choose $K = \mathbb{Q}(i)$, $i = \sqrt{-1}$. Then with the choices $\rho_1 = 1 + i$, $\rho_s = s$ for $s = 2, 3, \ldots, 6$; $r_\ell = \rho_\ell^2$, we find

$$
\begin{aligned}
a &= -353892105216 + 528220569600i \\
b &= 2112882278400 - 2149908480000i \\
c &= -8599633920000 \\
A &= -71328803586048000000i \\
B &= 153634690402938169196544 + 380285771115321439027200i \\
C &= 166616532655598905196544 + 166085373946419295027200i \\
D &= -1191348658308947587891200 - 789381960170093936640000i
\end{aligned}
$$

Via (7), this determines a rank 6 elliptic curve $\mathcal{E}$ over $K(T) = \mathbb{Q}(i)(T)$. The j-invariant of this curve is $j(\mathcal{E}) = p(T)/q(T)$, where $p(T)$ and $q(T)$ are degree 9 and 10 polynomials in T, respectively. The leading coefficient of $p(T)$ is

$$
\begin{aligned}
p_9 = {}& 17575652563096624654081015917110624256000000 \\
& + 166827764000346382053533572770299904000000000i.
\end{aligned}
$$

In particular, $j(\mathcal{E}) \in K(T)$, but $j(\mathcal{E}) \notin \mathbb{Q}(T)$. The complete j-invariant can be found in the attached data files.

Example 4.3. Choose $K = \mathbb{Q}(\zeta_5)$, where ζ_5 is a fifth root of unity. Then with the choices $r_\ell = \rho_\ell^2$,

$$
\rho_1 = \zeta_5, \quad \rho_2 = \zeta_5^2, \quad \rho_3 = \zeta_5^3, \quad \rho_4 = 1 + \zeta_5, \quad \rho_5 = 1 + \zeta_5^2, \quad \rho_6 = 1 + \zeta_5^3.
$$

the coefficients are

$$a = 55\zeta_5^3 - 8\zeta_5^2 + 41\zeta_5 + 25$$
$$b = -12\zeta_5^3 - 40\zeta_5^2 + 20\zeta_5 - 48$$
$$c = -24\zeta_5^2 + 16\zeta_5 - 24$$
$$A = -832\zeta_5^3 - 320\zeta_5^2 - 320\zeta_5 - 832$$
$$B = 2312\zeta_5^3 + 3693\zeta_5^2 - 861\zeta_5 + 5117$$
$$C = -2040\zeta_5^3 + 1837\zeta_5^2 - 2397\zeta_5 + 573$$
$$D = 2440\zeta_5^3 + 152\zeta_5^2 + 1408\zeta_5 + 1664$$

This determines a rank 6 elliptic curve $\mathcal{E}$ over $K(T) = \mathbb{Q}(\zeta_5)(T)$ via (7). The j-invariant for this elliptic curve is

$$j(\mathcal{E}) = \frac{p(T)}{q(T)}$$

where $p(T)$ and $q(T)$ are degree 9 and 10 polynomials in T, respectively. The leading coefficient of $p(T)$ is

$$p_9 = -120367420933700619964515942 4\zeta_5^3 + 470942041084292914570780672\zeta_5^2$$
$$- 1034969760873268271839698944\zeta_5 - 272969531667632951696109568.$$

Notice that $j(\mathcal{E}) \in K(T)$, but $j(\mathcal{E}) \notin \mathbb{Q}(T)$. The complete j-invariant can be found in the attached data files.

5. Acknowledgments

References

[AL-RM]   S. Arms, Á Lozano-Robledo and S. J. Miller, *Constructing one-parameter families of elliptic curves with moderate rank*, Journal of Number Theory **123** (2007), no. 2, 388–402.

[BEW]   B. Berndt, R. Evans and K. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Vol. 21, Wiley-Interscience Publications, John Wiley & Sons, New York, 1998.

[BMSW]   B. Bektemirov, B. Mazur, W. Stein and M. Watkins, *Average ranks of elliptic curves: Tension between data and conjecture*, Bull. Amer. Math. Soc. **44** (2007), 233–254.

[E]   N. Elkies, *The rationality of conics over finite fields*, online lecture notes (2013). Retrieved 23 April 2017. http://www.math.harvard.edu/~elkies/M256.13/conicfq.pdf

[KSW]   Z. Klagsbrun, T. Sherman and J. Weigandt, *The Elkies Curve has Rank 28 Subject only to GRH*, arXiv preprint (2016). https://arxiv.org/abs/1606.07178.

[Kn]   A. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, NJ, 1992.

[Lan]   E. Landau, *Neuer beweis des primzahlsatzes und beweis des primidealsatzes*, Mathematische Annalen **56** no. 4 (1903), 645–670.

[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.

[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.

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

[S]   SageMath, the Sage Mathematics Software System (Version 7.6.0), The Sage Developers, 2017, http://www.sagemath.org.

[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.

[SiTa]   J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.

[Su]   A. Sutherland, *Introduction to Arithmetic Geometry*, course notes, MIT OpenCourseWare (2013). https://ocw.mit.edu/courses/mathematics/18-782-introduction-to-arithmetic-geometry-fall-2013/lecture-notes/

[Sr]   V. Srinivas, *The Tate conjecture for K3 surfaces: a survey of some recent progress.* Acta Math. Viet. **39** no. 4 (2014), 69–85.

Student biographies

David Mehrle: (*Corresponding author:* dmehrle@math.cornell.edu) is currently a graduate student at Cornell University.

Tomer Reiter graduated Carnegie Mellon University to spend a year studying at Cambridge University as a Gates-Cambridge scholar. He is now a graduate student at Emory University, where he studies number theory with Ken Ono.

Joseph Stahl is now a graduate student at Berkeley, where he intends to study number theory. Prior to that, he spent a year at Bonn on a Fulbright scholarship.

Dylan Yott is a graduate student at Berkeley studying number theory with Xinyi Yuan.