CONSTRUCTING FAMILIES OF MODERATE-RANK ELLIPTIC CURVES OVER NUMBER FIELDS

DAVID MEHRLE, STEVEN J. MILLER, TOMER REITER, JOSEPH STAHL, AND DYLAN YOTT

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 Steven J. Miller, Álvaro Lozano-Robledo and Scott Arms, 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 $E/\mathbb{Q}$ is an elliptic curve, 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 have arbitrarily large rank. It is an interesting and difficult problem to find single curves 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 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

Theorem 1.1. *Let K be a number field over $\mathbb{Q}$. Then there exists an (explicitly computable) family of elliptic curves of rank 6 over K; moreover, the rank is determined by the evaluation of Legendre sums and not the construction of points on the curves and a calculation of a height matrix.*

Date: September 21, 2015.

2010 *Mathematics Subject Classification.* 11G05 (primary), 11G20, 11G40, 14G10.

Key words and phrases. Elliptic curves, rational elliptic surface, rank of the Mordell-Weil group, number fields, sums of Legendre symbols.

This work was supported by NSF grants DMS-1347804, DMS-1265673, Williams College, and the PROMYS program. The authors thank Álvaro Lozano-Robledo, Rob Pollack and Glenn Stevens for their insightful comments and support.

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

$$\mathcal{E}: \qquad y^2 + a_1(T)xy + a_3(T)y \ = \ x^3 + a_2(T)x^2 + a_4(T)x + a_6(T), \tag{2.1}$$

where $a_i(T) \in \mathcal{O}_K(T)$. By Silverman's Specialization theorem [Si2, Si3], 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 $\mathcal{O}_K$. 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 $\mathcal{O}_K$, we define the average

$$A_{\mathfrak{p}}(\mathcal{E}) \ := \ \frac{1}{N(\mathfrak{p})} \sum_{t \in \mathcal{O}_K/\mathfrak{p}} a_t(\mathfrak{p}), \tag{2.2}$$

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

$$\lim_{X \to \infty} \frac{1}{X} \sum_{\mathfrak{p}:\ N(\mathfrak{p}) \leqslant X} -A_{\mathfrak{p}}(\mathcal{E}) \log N(\mathfrak{p}) \ = \ \text{rank } \mathcal{E}(K(T)). \tag{2.3}$$

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 (2.3), 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*

$$\sum_{N(\mathfrak{p}) \leqslant X} \log(N(\mathfrak{p})) \ \sim \ X. \tag{2.4}$$

Applying this theorem to (2.3), it suffices to compute the following limit:

$$\lim_{X \to \infty} \frac{1}{X} \sum_{\mathfrak{p}: N(\mathfrak{p}) \leqslant X} -A_{\mathfrak{p}}(\mathcal{E}) \log(N(\mathfrak{p})) \tag{2.5}$$

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 (2.5) it follows that

$$\text{rank } \mathcal{E}(K(T)) \ = \ 6, \tag{2.6}$$

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

$$\begin{aligned} y^2 \ = \ f(x,T) \ &= \ x^3T^2 + 2g(x)T - h(x) \\ g(x) \ &= \ x^3 + ax^2 + bx + c \\ h(x) \ &= \ (A-1)x^3 + Bx^2 + Cx + D \\ D_T(x) \ &= \ g(x)^2 + x^3h(x). \end{aligned} \tag{2.7}$$

In order to show our claim for this elliptic curve, 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 $t \in \mathcal{O}_K$

$$\sum_{t \in \mathcal{O}_K/\mathfrak{p}} \left(\frac{at^2+bt+c}{\mathfrak{p}}\right) \;=\; \begin{cases} (N(\mathfrak{p})-1)\left(\frac{a}{\mathfrak{p}}\right) & \text{if } (b^2-4ac) \in \mathfrak{p} \\ -\left(\frac{a}{\mathfrak{p}}\right) & \text{otherwise.} \end{cases} \tag{2.8}$$

Note that (2.8) is already demonstrated for p a prime in Lemma A.2 of [AL-RM] (they give two proofs; the result also appears in [BEW]). Since in our case $\mathcal{O}_K/\mathfrak{p}$ is a finite field, it suffices to show (2.8) for $q = p^r$ for $r > 1$; we do that as Proposition 3.1 in the next section. Once this is established, by mimicking Equations 2.3 through 2.5 of [AL-RM] in the number field case we may conclude that $-N(\mathfrak{p})A_{\mathcal{E}}(\mathfrak{p}) = 6N(\mathfrak{p})$. Therefore $A_{\mathcal{E}}(\mathfrak{p}) = -6$, completing the proof of Theorem 1.1.

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 $\mathbb{F}_q$ the 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 is not zero modulo q, then*

$$\sum_{t \in \mathbb{F}_q} \left(\frac{at^2+bt+c}{q}\right) \;=\; \begin{cases} (q-1)\left(\frac{a}{q}\right) & \text{if } b^2-4ac = 0 \bmod q \\ -\left(\frac{a}{q}\right) & \text{otherwise.} \end{cases} \tag{3.1}$$

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

For the other case, we first reinterpret the sum as counting points on the conic $C : s^2 = at^2+bt+c$ in the following way:

$$\#C(\mathbb{F}_q) \;=\; \sum_{t \in \mathbb{F}_q} \left(1 + \left(\frac{at^2+bt+c}{q}\right)\right) \;=\; q + S. \tag{3.2}$$

Here S is the sum of interest. It is well known that conics over finite fields always have a rational point, and from this we can parametrize all the 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

$$q - 1 \;\leqslant\; \#C(\mathbb{F}_q) \;\leqslant\; q+1, \tag{3.3}$$

which gives

$$-1 \;\leqslant\; S \;\leqslant\; 1. \tag{3.4}$$

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

$$S \;\equiv\; \sum_{t \in \mathbb{F}_q} (at^2+bt+c)^{\frac{q-1}{2}} \;\equiv\; \sum_{t \in \mathbb{F}_q} \left(\frac{a}{q}\right) t^{q-1} + r(t) \;\equiv\; -\left(\frac{a}{q}\right) + \sum_i r_i \sum_{t \in \mathbb{F}_q} t^i, \tag{3.5}$$

where $r(t)$ is a polynomial of degree $< q-1$. 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 $S \equiv -\left(\frac{a}{q}\right) \pmod p$. Since $-1 \leqslant S \leqslant 1$, we have $S = -\left(\frac{a}{q}\right)$, as desired. □

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.

[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** (1903), no. 4, 645–670.

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

[Mes2] J. Mestre, *Courbes elliptiques de rang* $\geqslant$ *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.

[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.

[Si3] J. Silverman, *Specialization Maps and Unlikely Intersections*, talk at the 26th Journées Arithmétique Saint-Étienne, France (2009). http://www.math.brown.edu/~jhs/Presentations/JA09Talk.pdf.

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

E-mail address: dmehrle@cmu.edu

Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, PA 15289

E-mail address: sjm1@williams.edu, Steven.Miller.MC.96@aya.yale.edu

Department of Mathematics and Statistics, Williams College, Williamstown, MA 01267

E-mail address: treiter@andrew.cmu.edu

Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, PA 15289

E-mail address: jstahl@bu.edu

Department of Mathematics & Statistics, Boston University, Boston, MA 02215

E-mail address: dyott@math.berkeley.edu

Department of Mathematics, University of California, Berkeley, Berkeley, CA 94720