Constructing 1-Parameter Families of Elliptic Curves over $\mathbb{Q}(t)$ with Moderate Rank

Steven J. Miller
The Ohio State University

Boulder: October 4^{th}, 2003
http://www.math.ohio-state.edu/
$\sim$sjmiller/math/talks/talks.html

Collaborators

Theory

- Álvaro Lozano Robledo

Programs

- Jon Hsu
- Leo Goldmakher
- Stephen Lu
- Atul Pokharel

Elliptic Curves

$E/\mathbb{Q}$: For $a_i \in \mathbb{Q}$,

$$y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6.$$

Often can write as $y^2 = x^3 + Ax + B$.

One-parameter families:

$$\begin{aligned} y^2 &= x^3 + A(t)x + B(t) \\ & \quad A(t), B(t) \in \mathbb{Z}[t]. \end{aligned}$$

Elliptic Curves (cont)

Let N_p be the number of solns mod p:

$$N_p = \sum_{x(p)} \left[1 + \left(\frac{x^3 + Ax + B}{p}\right)\right] = p + \sum_{x(p)} \left(\frac{x^3 + Ax + B}{p}\right)$$

Local data: $a_p = p - N_p$.

$$L(s, E) = \prod_{p|\Delta} \left(1 - a_p p^{-s}\right)^{-1} \prod_{p \nmid \Delta} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}$$

Rational solutions a group: $E(\mathbb{Q}) = \mathbb{Z}^r \bigoplus T$.

Birch and Swinnerton-Dyer Conjecture:
Geometric rank equals the analytic rank.

Mestre's Construction

Consider 6-tuple of integers a_i.

$$\begin{aligned} q(x) &= \prod_{i=1}^{6}(x - a_i) \\ p(t, x) &= q(x - t)q(x + t). \end{aligned}$$

$\exists g(t, x)$ of degree 6 in x and $r(t, x)$ of degree at most 5 in x such that

$$p(t, x) = g^2(t, x) - r(t, x).$$

Consider

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

Rosen-Silverman Theorem

For a one-parameter family $\mathcal{E}/\mathbb{Q}(t)$, define

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

Thm [R-S]: *Let $\mathcal{E} : y^2 = x^3 + A(t)x + B(t)$, and assume Tate's conjecture (known for rational surfaces) for the surface. Then*

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

Construct $\mathcal{E}$ with $A_{\mathcal{E}}(p) = -r + O(\frac{1}{p})$.

PNT implies r is the rank over $\mathbb{Q}(t)$.

Quadratic Legendre Sums

LEMMA: Quadratic Legendre Sums: *a and b are not both zero mod p, $p > 2$. Then*

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

Moral: Can handle linear and quadratic Legendre sums; for cubic best is Hasse, giving $O(\sqrt{p})$.

Rank 6 Rational Surfaces over $\mathbb{Q}(t)$

$$y^2 = f_t(x) = x^3t^2 + 2g(x)t - h(x)$$

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

$$D_t(x) = g(x)^2 + x^3h(x).$$

$D_t(x)$ is one-fourth the discriminant of the quadratic (in t) polynomial

$$x^3t^2 + 2g(x)t - h(x).$$

Discriminant Method

The number of distinct, non-zero roots of $D_t(x)$ will control the rank.

$D_t(x_i) = 0$ gives

$$y^2 = x_i^3 \left(t - \alpha(x_i)\right)^2 .$$

If $x_i = \square$, then

$$\sum_{t(p)} \left(\frac{x_i^3 \left(t - \alpha(x_i)\right)^2}{p} \right) = p - 1.$$

Sketch of Proof

Studying $\sum_{t(p)} \sum_{x \not\equiv 0(p)} \left(\frac{x^3t^2 + 2g(x)t - h(x)}{p} \right)$.

$x = 0$, the t-sum vanishes if $c \neq 0$.

For $x \not\equiv 0$, have

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

Find coefficients a, b, c, A, B, C, D with $D_t(x)$ six distinct, non-zero perfect square roots.

Gives $6(p-1) - 1(-6) + 0 = 6p$.

Determining Constants $a, \ldots, D$

For $1 \leq i \leq 6$, let $r_i = \rho_i^2$.

$$
\begin{aligned}
D_t(x) &= g(x)^2 + x^3 h(x) \\
&= A\Big(x^6 + \frac{B+2a}{A}x^5 + \frac{C+a^2+2b}{A}x^4 + \frac{D+2ab+2c}{A}x^3 \\
&\quad + \frac{2ac+b^2}{A}x^2 + \frac{2bc}{A}x + \frac{c^2}{A}\Big) \\
&= A(x^6 + R_5x^5 + R_4x^4 + R_3x^3 + R_2x^2 + R_1x + R_0) \\
&= A(x-r_1)(x-r_2)(x-r_3)(x-r_4)(x-r_5)(x-r_6).
\end{aligned}
$$

Can match x^5, x^4, x^3 terms (B, C, D).

Determining Constants (cont)

We must simultaneously solve

$$\begin{aligned} 2ac + b^2 &= R_2 A \\ 2bc &= R_1 A \\ c^2 &= R_0 A. \end{aligned}$$

Send $A \to Aw^2$, rescaling b and c by w.

Take $r_i = \rho_i^2 = i^2$. Then

$$\begin{aligned} A &= 64R_0^3 &&= 89161004482560000000 \\ c &= 8R_0^2 &&= 21499084800000 \\ b &= 4R_0R_1 &&= -1603174809600 \\ a &= 4R_0R_2 - R_1^2 &&= 16660111104 \end{aligned}$$

$$\begin{aligned} B &= R_5A - 2a &&= -811365140824616222208 \\ C &= R_4A - a^2 - 2b &&= 2649749034732149352038 4 \\ D &= R_3A - 2ab - 2c &&= -343107594345448813363200 \end{aligned}$$

Increasing Rank: Cubic in t

Cubics fail: if discriminant vanishes,

$$y^2 = a(x)\,(t-\alpha(x))^3$$

$$y^2 = a(x)\,(t-\alpha(x))\,(t-\beta(x))^2\,.$$

Both vanish in

$$\sum_{t(p)} \left(\frac{*}{p}\right)$$

Increasing Rank: Quartic in t

$$y^2 = A(x)t^4 + B(x)t^2 + C(x).$$

Two ways to get points over $\mathbb{Q}(t)$:

- $B^2(x) - 4A(x)C(x) = 0$,
  $A(x)$ a square.

  $$y^2 = a^2(x)[t^2 - b(x)]^2.$$

- Two of $A(x), B(x), C(x) = 0$,
  other a square.

  $$y^2 = \left[s(x)t^i\right]^2.$$

Quartic in t (cont)

Example:

$$\begin{aligned} A(x) &= x^4 \\ B(x) &= 2x(b_3x^3 + b_2x^2 + b_1x + b_0) + b^2 \\ C(x) &= x(b_3^2x^3 + c_2x^2 + c_1x + c_0). \end{aligned}$$

Found rank 8 example.

Best possible is rank 14:

- 8 from $B^2(x) - 4A(x)C(x) = 0$.
- 6 from two of three vanish, other $\square$.

Numerically Approximating Ranks:

Cusp form f, level N, weight 2:

$$\begin{aligned} f(-1/Nz) &= -\epsilon N z^2 f(z) \\ f(i/y\sqrt{N}) &= \epsilon y^2 f(iy/\sqrt{N}). \end{aligned}$$

Define

$$\begin{aligned} L(f,s) &= (2\pi)^s \Gamma(s)^{-1} \int_0^{i\infty} (-iz)^s f(z) \frac{dz}{z} \\ \Lambda(f,s) &= (2\pi)^{-s} N^{s/2} \Gamma(s) L(f,s). \end{aligned}$$

To each E corresponds an f, write $\int_0^\infty = \int_0^1 + \int_1^\infty$ and use transformations.

Algorithm for $L^r(s, E)$:

Differentiate r times with respect to s:

$$\Lambda^{(r)}(E, 1) = (1 + \epsilon(-1)^r) \int_1^\infty f(iy/\sqrt{N})(\log\ y)^r dy.$$

Substitute series expansion, integrate by parts:

$$L^{(r)}(E, 1) = 2r! \sum_{n=1}^{\infty} \frac{a_n}{n} G_r\left(\frac{2\pi n}{\sqrt{N}}\right),$$

where

$$G_r(x) = \frac{1}{(r-1)!} \int_1^\infty e^{-xy} (\log y)^{r-1} \frac{dy}{y}.$$

Need about $\sqrt{N} \log N$ terms.

Programming Issues

- Conductors overflow C's long, pass from PARI as $c_1 10^9 + c_0$.

- Calculate a_p, then a_{p^k}. To get a_n, have file with largest prime power factor of n.

- Haven't, but could pre-compute $G_r(x)$.

Have C Program and PARI package available for downloading.

Handling conductors of size $4 \cdot 10^9$, couple hundred in an hour.

Excess Rank Calculations
Families with $y^2 = f_t(x)$; $D(t)$ SqFree

Family	t Range	Num t	r	$r/\mathbb{Q}(t)$	$r+1$	$r+2$	$r+3$
$+4(4t+2)$	$[2, 2002]$	1622	0		95.44		4.56
$-4(4t+2)$	$[2, 2002]$	1622	0	70.53		29.35	
$9t+1$	$[2, 247]$	169	0	71.01		28.99	
t^2+9t+1	$[2, 272]$	169	1	71.60		27.81	
$t(t-1)$	$[2, 2002]$	643	0	40.44	48.68	10.26	0.62
$(6t+1)x^2$	$[2, 101]$	93	1	34.41	47.31	17.20	1.08
$(6t+1)x$	$[2, 77]$	66	2	30.30	50.00	16.67	3.03

1. $x^3 + 4(4t+2)x$, $4t+2$ Sq-Free, odd.
2. $x^3 - 4(4t+2)x$, $4t+2$ Sq-Free, even.
3. $x^3 + 2^4(-3)^3(9t+1)^2$, $9t+1$ Sq-Free, even.
4. $x^3 + tx^2 - (t+3)x + 1$, t^2+3t+9 Sq-Free, odd.
5. $x^3 + (t+1)x^2 + tx$, $t(t-1)$ Sq-Free, rank 0.
6. $x^3 + (6t+1)x^2 + 1$, $4(6t+1)^3 + 27$ Sq-Free, rank 1.
7. $x^3 - (6t+1)^2x + (6t+1)^2$, $(6t+1)[4(6t+1)^2 - 27]$ Sq-Free, rank 2.

Excess Rank Calculations
Families with $y^2 = f_t(x)$; All $D(t)$

Family	t Range	Num t	r	$r/\mathbb{Q}(t)$	$r+1$	$r+2$	$r+3$
$+4(4t+2)$	$[2, 2002]$	2001	0	6.45	85.76	3.95	3.85
$-4(4t+2)$	$[2, 2002]$	2001	0	63.52	9.90	25.99	.50
$9t+1$	$[2, 247]$	247	0	55.28	23.98	20.73	
t^2+9t+1	$[2, 272]$	271	1	73.80		25.83	
$t(t-1)$	$[2, 2002]$	2001	0	42.03	48.43	9.25	0.30
$(6t+1)x^2$	$[2, 101]$	100	1	32.00	50.00	17.00	1.00
$(6t+1)x$	$[2, 77]$	76	2	32.89	50.00	14.47	2.63

1. $x^3 + 4(4t+2)x$, $4t+2$.
2. $x^3 - 4(4t+2)x$, $4t+2$.
3. $x^3 + 2^4(-3)^3(9t+1)^2$.
4. $x^3 + tx^2 - (t+3)x + 1$.
5. $x^3 + (t+1)x^2 + tx$.
6. $x^3 + (6t+1)x^2 + 1$.
7. $x^3 - (6t+1)^2x + (6t+1)^2$.

Appendix: Standard Conjectures

Generalized Riemann Hypothesis (for Elliptic Curves): *Let $L(s, E)$ be the (normalized) L-function of the elliptic curve E. Then the non-trivial zeros of $L(s, E)$ satisfy Re$(s) = \frac{1}{2}$.*

Birch and Swinnerton-Dyer Conjecture [BSD1], [BSD2]: *Let E be an elliptic curve of geometric rank r over $\mathbb{Q}$ (the Mordell-Weil group is $\mathbb{Z}^r \oplus T$, T is the subset of torsion points). Then the analytic rank (the order of vanishing of the L-function at the critical point) is also r.*

Tate's Conjecture for Elliptic Surfaces [Ta]: *Let $\mathcal{E}/\mathbb{Q}$ be an elliptic surface and $L_2(\mathcal{E}, s)$ be the L-series attached to $H^2_{\acute{e}t}(\mathcal{E}/\overline{\mathbb{Q}}, \mathbb{Q}_l)$. Then $L_2(\mathcal{E}, s)$ has a meromorphic continuation to* **C** *and satisfies $-ord_{s=2}L_2(\mathcal{E}, s)$ $=$ rank $NS(\mathcal{E}/\mathbb{Q})$, where $NS(\mathcal{E}/\mathbb{Q})$ is the $\mathbb{Q}$-rational part of the Néron-Severi group of $\mathcal{E}$. Further, $L_2(\mathcal{E}, s)$ does not vanish on the line Re$(s) = 2$.*

Bibliography

[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, Inc., New York, 1998.

[Bi] B. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. **43**, 1968, $57 - 60$.

[BS] B. Birch and N. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology **5**, 1966, $295 - 299$.

[BSD1] B. Birch and H. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. reine angew. Math. **212**, 1963, $7 - 25$.

[BSD2] B. Birch and H. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. reine angew. Math. **218**, 1965, $79 - 108$.

[BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\boldsymbol{Q}$*: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14**, no. 4, 2001, $843 - 939$.

[BM] A. Brumer and O. McGuinness, *The behaviour of the Mordell-Weil group of elliptic curves*, Bull. AMS **23**, 1991, $375 - 382$.

[Cr] Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992.

[Di] F. Diamond, *On deformation rings and Hecke rings*, Ann. Math. **144**, 1996, $137 - 166$.

[Fe1] S. Fermigier, *Zéros des fonctions* L *de courbes elliptiques*, Exper. Math. **1**, 1992, $167 - 173$.

[Fe2] S. Fermigier, *Étude expérimentale du rang de familles de courbes elliptiques sur* $\mathbb{Q}$, Exper. Math. **5**, 1996, $119 - 130$.

[FP] E. Fouvrey and J. Pomykala, *Rang des courbes elliptiques et sommes d'exponentelles*, Monat. Math. **116**, 1993, $111 - 125$.

[GM] F. Gouvéa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4**, 1991, $45 - 65$.

[Go] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number Theory (Proc. Conf. in Carbondale, 1979), Lecture Notes in Math. **751**, Springer-Verlag, 1979, $108 - 118$.

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

[Ko] V. Kolyvagin, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), Math. Soc. Japan, Tokyo, 1991, $429 - 436$.

[Mai] L. Mai, *The analytic rank of a family of elliptic curves*, Canadian Journal of Mathematics **45**, 1993, $847 - 862$.

[Mes1] J. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Mathematica **58**, 1986, $209 - 232$.

[Mes2] J. Mestre, *Courbes elliptiques de rang* $\geq$ *11 sur* $\boldsymbol{Q}(t)$, C. R. Acad. Sci. Paris, ser. 1, **313**, 1991, $139 - 142$.

[Mes3] J. Mestre, *Courbes elliptiques de rang* $\geq$ *12 sur* $\boldsymbol{Q}(t)$, C. R. Acad. Sci. Paris, ser. 1, **313**, 1991, $171 - 174$.

[Mi] P. Michel, *Rang moyen de familles de courbes elliptiques et lois de Sato-Tate*, Monat. Math. **120**, 1995, $127 - 136$.

[Mil] S. J. Miller, 1- *and* 2*-Level Densities for Families of Elliptic Curves: Evidence for the Underlying Group Symmetries*, P.H.D. Thesis, Princeton University, 2002, http://www.math.princeton.edu/$\sim$sjmiller/thesis/thesis.pdf.

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

[Na1] K. Nagao, *On the rank of elliptic curve* $y^2 = x^3 - kx$, Kobe J. Math. **11**, 1994, $205 - 210$.

[Na2] K. Nagao, *Construction of high-rank elliptic curves*, Kobe J. Math. **11**, 1994, $211 - 219$.

[Na3] K. Nagao, $\mathbb{Q}(t)$*-rank of elliptic curves and certain limit coming from the local points*, Manuscr. Math. **92**, 1997, $13 - 32$.

[RSi] M. Rosen and J. Silverman, *On the rank of an elliptic surface*, Invent. Math. **133**, 1998, $43 - 67$.

[RS] Z. Rudnick and P. Sarnak, *Zeros of principal* L*-functions and random matrix theory*, Duke Journal of Math. **81**, 1996, $269 - 322$.

[Sh] 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.

[Si3] J. Silverman, *The average rank of an algebraic family of elliptic curves*, J. reine angew. Math. **504**, 1998, $227 - 236$.

[St1] N. Stephens, *A corollary to a conjecture of Birch and Swinnerton-Dyer*, J. London Math. Soc. **43**, 1968, $146 - 148$.

[St2] N. Stephens, *The diophantine equation* $X^3 + Y^3 = DZ^3$ *and the conjectures of Birch and Swinnerton-Dyer*, J. reine angew. Math. **231**, 1968, $16 - 162$.

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

[TW] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **141**, 1995, $553 - 572$.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math **141**, 1995, $443 - 551$.