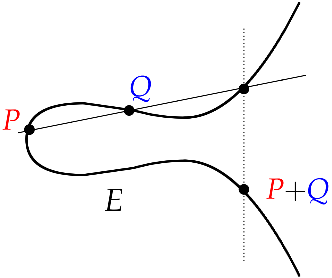
A Family of Rank Six Elliptic Curves over Number Fields

David Mehrle & Tomer Reiter
Carnegie Mellon University

August 22, 2014

ELLIPTIC CURVES

- Elliptic curve $\quad E : y^2 = x^3 + ax^2 + bx + c$
- "Adding" points on E makes group $E(\mathbb{Q})$



Group Structure

<u>Mordell-Weil Theorem:</u> $E(\mathbb{Q})$ finitely generated

$$\Downarrow$$

$$E(\mathbb{Q}) \cong \mathbb{Z}^{r} \oplus T$$

"rank" "torsion"

- Rank $< \infty$, hard to compute!
- Torsion = points of finite order

Rank

<u>Conjecture:</u> rank is unbounded

- Noam Elkies: $28 \leq \text{rank}\,(E) \leq 32 \leftarrow$ World Record!
- High rank curves are *hard* to find!
- Much interest in modern number theory
- Applications to cryptography

<u>Goal:</u> Find family of curves of moderate rank

NUMBER FIELDS

- Number field K = finite field extension of $\mathbb{Q}$
- e.g. $K = \mathbb{Q}\left(\sqrt{-5}\right) = \left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Q}\right\}$
- Many analogies with $\mathbb{Q}$

	$\mathbb{Q}$		K
integers	$\mathbb{Z}$	$\longrightarrow$	$\mathcal{O}_K$
primes	$0, 2, 3, 5, \ldots$	$\longrightarrow$	prime ideals $\mathfrak{p} \subset \mathcal{O}_K$
factorization	integers	$\longrightarrow$	ideals
norm	$\lvert p\rvert = \left\lvert {}^{\mathbb{Z}}/_{(p)} \right\rvert$	$\longrightarrow$	$N(\mathfrak{p}) := \left\lvert {}^{\mathcal{O}_K}/_{\mathfrak{p}} \right\rvert$

Elliptic Surfaces

- Elliptic surface $\mathcal{E} \approx$ elliptic curve / $K(T)$
- Specialization:

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{\text{plug in } T=t} & \mathcal{E}_t \\ \uparrow & & \uparrow \\ \text{curve}/K(T) & & \text{curve}/K \end{array}$$

<u>Silverman Specialization Theorem:</u>
If $\mathcal{E}$ is an elliptic surface, then for almost all $t \in \mathcal{O}_K$,

$$\operatorname{rank}(\mathcal{E}_t) \geq \operatorname{rank}(\mathcal{E})$$

Important Theorem

Rosen & Silverman Theorem: $\mathcal{E}$ an elliptic surface

$$\lim_{X\to\infty} \frac{1}{X} \sum_{N(\mathfrak{p})\le X} -A_{\mathcal{E}}(\mathfrak{p}) \log N(\mathfrak{p}) \;=\; \operatorname{rank}(\mathcal{E})$$

- $a_t(\mathfrak{p}) \;=\; N(\mathfrak{p}) + 1 - \#\mathcal{E}_t\left({}^{\mathcal{O}_K}/_{\mathfrak{p}}\right)$
- $A_{\mathcal{E}}(\mathfrak{p}) \;=\; \dfrac{1}{N(\mathfrak{p})} \displaystyle\sum_{t\in\mathcal{O}_K/\mathfrak{p}} a_t(\mathfrak{p})$

$$\mathcal{E} \xrightarrow{\text{specialize}} \mathcal{E}_t \xrightarrow{\text{reduce mod } \mathfrak{p}} \mathcal{E}_t\left({}^{\mathcal{O}_K}/_{\mathfrak{p}}\right) \xrightarrow{\text{count points}} a_t(\mathfrak{p}) \xrightarrow{\text{average}} A_{\mathcal{E}}(\mathfrak{p})$$

Construction

Step 1: surface $\mathcal{E}$ with $A_{\mathcal{E}}(\mathfrak{p}) = -6, \ \forall\, \mathfrak{p}$

$$\Big\downarrow \ \text{Rosen \& Silverman}$$

Step 2: evaluate limit $\implies$ rank $(\mathcal{E}) = 6$

$$\Big\downarrow \ \text{Silverman Specialization}$$

Family of rank 6 curves $\mathcal{E}_t$

Step 1 : Equations

- Define surface $\mathcal{E} : y^2 = f(x, T)$

$$\begin{aligned} y^2 \;=\; f(x,T) &\;=\; T^2x^3 + T\,g(x) - h(x) \\ g(x) &\;=\; x^3 + ax^2 + bx + c, \quad c \neq 0 \\ h(x) &\;=\; Ax^3 + Bx^2 + Cx + D \end{aligned}$$

- Discriminant of f in T

$$\Delta_T(x) \;=\; g(x)^2 + 4\,x^3 h(x)$$

Step 1 : Key Idea

<u>Key Idea:</u> make roots of $\Delta_T(x)$ distinct perfect squares

- Choose roots ρ_i^2 of $\Delta_T(x)$

$$\Delta_T(x) \;=\; (4A+1)\prod_{i=1}^{6}\left(x-\rho_i^2\right)$$

- Equate coefficients

$$\Delta_T(x) \;=\; (4A+1)\prod_{i=1}^{6}\left(x-\rho_i^2\right) \;=\; g(x)^2+4\,x^3h(x)$$

- Solve nonlinear system for a, b, c, A, B, C, D

Step 1 : Legendre Symbol

<u>Lemma:</u> $-A_{\mathcal{E}}(\mathfrak{p}) = \#\{\text{perfect-square roots of } \Delta_T(x)\}$

- Legendre Symbol:

$$\left(\frac{a}{\mathfrak{p}}\right) = \begin{cases} +1 & a \text{ is a square mod } \mathfrak{p} \\ -1 & a \text{ not a square mod } \mathfrak{p} \\ 0 & a \in \mathfrak{p} \end{cases}$$

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

- $A_{\mathcal{E}}(\mathfrak{p}) = \frac{1}{N(\mathfrak{p})} \sum_{t \in \mathcal{O}_K/\mathfrak{p}} a_t(\mathfrak{p}) = \frac{-1}{N(\mathfrak{p})} \sum_{t \in \mathcal{O}_K/\mathfrak{p}} \sum_{x \in \mathcal{O}_K/\mathfrak{p}} \left(\frac{f(x,t)}{\mathfrak{p}}\right)$

Step 1 : Legendre Sums

Lemma: $-A_{\mathcal{E}}(\mathfrak{p}) = \#\{\text{perfect-square roots of } \Delta_T(x)\}$

- Evaluate Legendre sum

$$-N(\mathfrak{p})A_{\mathcal{E}}(\mathfrak{p}) = \sum_{x,t\in\mathcal{O}_K/\mathfrak{p}} \left(\frac{f(x,t)}{\mathfrak{p}}\right)$$

- Quadratic Legendre sum in t

$$\sum_{t\in\mathcal{O}_K/\mathfrak{p}} \left(\frac{f(x,t)}{\mathfrak{p}}\right) = \begin{cases} (N(\mathfrak{p})-1)\left(\frac{x}{\mathfrak{p}}\right) & x \text{ root of } \Delta_T(x) \\ -\left(\frac{x}{\mathfrak{p}}\right) & \text{else} \end{cases}$$

Step 1 : Computing $A_{\mathcal{E}}(\mathfrak{p})$

Lemma: $-A_{\mathcal{E}}(\mathfrak{p}) = \#\{\text{perfect-square roots of } \Delta_T(x)\}$

- Evaluate Legendre sum

$$
\begin{aligned}
-N(\mathfrak{p})A_{\mathcal{E}}(\mathfrak{p}) &= \sum_{x,t\,\in\mathcal{O}_K/\mathfrak{p}} \left(\frac{f(x,t)}{\mathfrak{p}}\right) \\
&= \sum_{\substack{x \text{ root of } \Delta_T(x) \\ t\in\mathcal{O}_K/\mathfrak{p}}} \left(\frac{f(x,t)}{\mathfrak{p}}\right) + \sum_{\substack{x \text{ nonroot} \\ t\in\mathcal{O}_K/\mathfrak{p}}} \left(\frac{f(x,t)}{\mathfrak{p}}\right) \\
&= N(\mathfrak{p}) \left(\begin{matrix}\#\text{perfect-square} \\ \text{roots of } \Delta_T(x)\end{matrix}\right) = 6N(\mathfrak{p})
\end{aligned}
$$

Construction

✓ <u>Step 1:</u> surface $\mathcal{E}$ with $A_{\mathcal{E}}(\mathfrak{p}) = -6, \ \forall \ \mathfrak{p}$

$$\Big\downarrow \ \text{Rosen \& Silverman}$$

<u>Step 2:</u> evaluate limit $\implies$ rank $(\mathcal{E}) = 6$

$$\Big\downarrow \ \text{Silverman Specialization}$$

Family of rank 6 curves $\mathcal{E}_t$

Step 2 : Use Previous Step

Rosen & Silverman Theorem:

$$\lim_{X\to\infty} \frac{1}{X} \sum_{N(\mathfrak{p})\le X} -A_{\mathcal{E}}(\mathfrak{p}) \log N(\mathfrak{p}) \;=\; \operatorname{rank}(\mathcal{E})$$

- Step 1: $A_{\mathcal{E}}(\mathfrak{p}) = -6$

$$\left({}^{1}\!/_{6}\right) \operatorname{rank}(\mathcal{E}) \;=\; \lim_{X\to\infty} \frac{1}{X} \sum_{N(\mathfrak{p})\le X} \log N(\mathfrak{p})$$

- Hope $\lim\limits_{X\to\infty} (\ldots) \;=\; 1$

Step 2 : Evaluate Limit

<u>Landau Prime Ideal Theorem:</u>

$$\sum_{N(\mathfrak{p}) \leq X} \log N(\mathfrak{p}) \ \approx \ X$$

$$\left({}^{1}\!/_{6}\right) \operatorname{rank}(E) \ = \ \lim_{X \to \infty} \frac{1}{X} \sum_{N(\mathfrak{p}) \leq X} \log N(\mathfrak{p}) \ = \ 1$$

$$\Downarrow$$

$$\operatorname{rank}(\mathcal{E}) = 6$$

$\blacksquare$

Example

- $K = \mathbb{Q}$

- $\mathcal{E} : y^2 = f(x,T)$
$$\begin{aligned} f(x,T) &= T^2x^3 + T\,g(x) + h(x) \\ g(x) &= x^3 + ax^2 + bx + c \\ h(x) &= Ax^3 + Bx^2 + Cx + D \end{aligned}$$

- Choose roots $1^2, \ldots, 6^2$, $\quad \Delta_T(x) = (4A+1)\prod_{i=1}^{6}(x - i^2)$

$$\begin{aligned} a &= 16660111104 & \qquad A &\approx 8.9161 \times 10^{18} \\ b &= -1603174809600 & B &\approx -8.1137 \times 10^{20} \\ c &= 2149908480000 & C &\approx 2.6497 \times 10^{22} \\ & & D &\approx -3.4311 \times 10^{23} \end{aligned}$$

The non-Galois case

$$\begin{array}{ccc} L & & \mathcal{E}(L) \\ \cup\!| & & \\ K & & \mathcal{E}(K) \\ \cup\!| & & \\ \mathbb{Q} & & \mathcal{E}(\mathbb{Q}) \end{array}$$

- $K/\mathbb{Q}$ **not** Galois
- $L/\mathbb{Q}$ Galois

<u>Theorem:</u> rank $\mathcal{E}(L) \geq$ rank $\mathcal{E}(K) \geq$ rank $\mathcal{E}(\mathbb{Q})$

<u>Corollary:</u> If $\mathcal{E}/K$ has coefficients in $\mathbb{Q}$, then rank $(\mathcal{E}) = 6$

Credits

PRESENTED BY:

David Mehrle dmehrle@cmu.edu
Tomer Reiter tomer.reiter@gmail.com

JOINT WORK WITH:

Joseph Stahl josephmichaelstahl@gmail.com
Dylan Yott dtyott@gmail.com

ADVISED BY:

Steven J. Miller sjm1@williams.edu
Alvaro Lozano-Robledo alozano@math.uconn.edu

SPECIAL THANKS TO:

The PROMYS Program Boston University
The SMALL REU Williams College

FUNDED BY:

NSF Grants DMS1347804, DMS1265673,
the PROMYS Program, and Williams College