Ranks of quadratic twists of elliptic curves over $\mathbb{F}_q(t)$

Part II

Enrique Acosta and Martin Leslie
Advisor: Doug Ulmer

Department of Mathematics
University of Arizona

December 11, 2008

Elliptic Curves

Let k be a field with char $k \neq 2, 3$. An Elliptic Curve over k is:

Definition (1)

A nonsingular genus 1 curve with a point with coordinates in k.

Elliptic Curves

Let k be a field with char $k \neq 2, 3$. An Elliptic Curve over k is:

Definition (1)

A nonsingular genus 1 curve with a point with coordinates in k.

Definition (2)

A curve in $k\mathbb{P}^2$ defined by an equation of the form

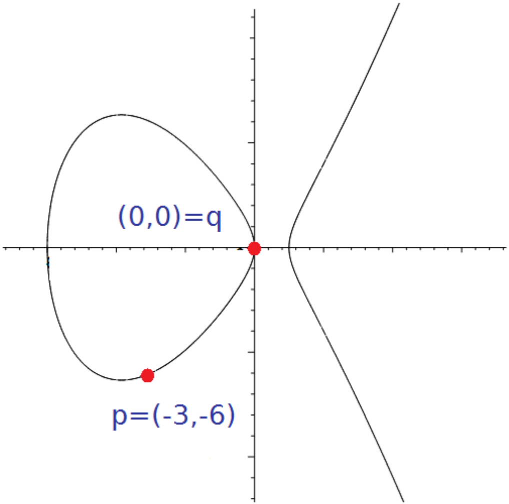
$$y^2 = x^3 + ax + b$$

where $a, b \in k$, and the cubic polynomial on the right has no repeated roots.

The Group Law

$E(k) =$The set of points with coordinates in k has a group structure.

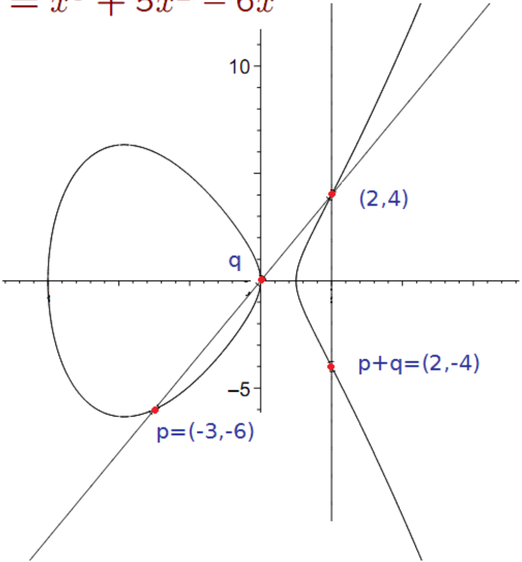
$$y^2 = x^3 + 5x^2 - 6x$$



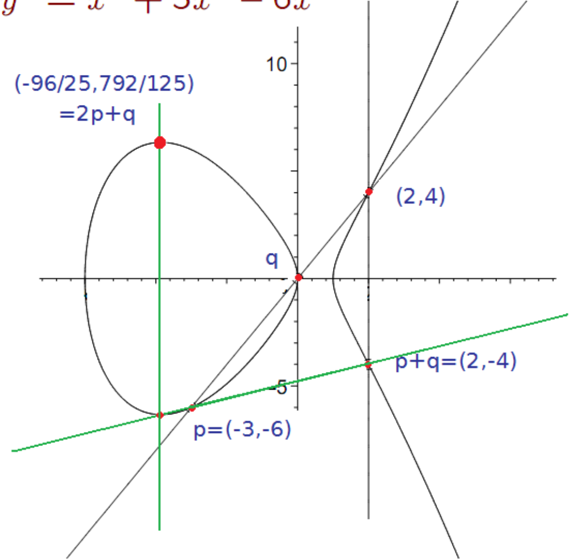
Example

$k = \mathbb{Q}$

$$y^2 = x^3 + 5x^2 - 6x$$



$$y^2 = x^3 + 5x^2 - 6x$$



Mordell's Theorem

Theorem

$E(\mathbb{Q})$ *is finitely generated.*

Consequence

$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus$ "Finite Abelian Group"

Definition

r is called the rank of the elliptic curve.

Mordell's Theorem

Theorem

$E(\mathbb{Q})$ *is finitely generated.*

Consequence

$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus$ "Finite Abelian Group"

Definition

r is called the rank of the elliptic curve.

- There is no known effective method to find the rank.
- Conjecture: There are elliptic curves over $\mathbb{Q}$ with arbitrary large rank.

Mordell's Theorem

Theorem
$E(\mathbb{Q})$ *is finitely generated.*

Consequence
$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus$ "Finite Abelian Group"

Definition
r is called the rank of the elliptic curve.

- There is no known effective method to find the rank.
- Conjecture: There are elliptic curves over $\mathbb{Q}$ with arbitrary large rank.
- Largest rank known (2006): At least 28.
- BSD Conjecture (1 Million): The rank of an elliptic curve E is the order of a zero at $s = 1$ of an L-series associated to E.

Mordell's Theorem over $\mathbb{F}_q(t)$

Theorem

$E(\mathbb{F}_q(t))$ is finitely generated.

$$E(\mathbb{F}_q(t)) \cong \mathbb{Z}^r \oplus \text{"Finite Abelian Group"}$$

r is called the rank of the elliptic curve.

- There is no known effective method to find the rank.
- THEOREM: There are elliptic curves over $\mathbb{F}_q(t)$ with arbitrary large rank (Shafarevich, Tate).
- BSD Conjecture: The rank of an elliptic curve E is the order of a zero at $s = 1$ of an L-series associated to E.

Twists of Elliptic Curves

$k = \mathbb{Q}$. Let E/k be an elliptic curve defined by

$$E : \quad y^2 = x^3 + ax + b.$$

Definition

Let D be a square free integer. The quadratic twist E_D of E by D is the elliptic curve defined by

$$E_D : \quad Dy^2 = x^3 + ax + b$$

Question

¿ What is the rank of E_D?

The Parity Conjecture

A consequence of two BIG ingredients:

- Conjecture: The Birch and Swinnerton-Dyer conjecture.
- THEOREM: Modularity (gives a functional equation of the associated L-series to an elliptic curve).

Parity Conjecture

Let $E/\mathbb{Q}$ be an elliptic curve with conductor C and let D be a square-free integer relatively prime to $2C$. Then the ranks of E and E_D have the same parity if and only if $\chi_D(-C) = 1$ (a congruence condition on D depending on C).

Parity Conjecture (for mortals)

There are some congruence conditions on D depending on E which determine if the twist has even or odd rank.

The Article

F. Gouvêa and B. Mazur (1991)
The Square-Free Sieve and the Rank of Elliptic Curves

Ideas

- Use the parity conjecture to make twists have rank ≥ 2.
- Use this to show there are lots of twists of a given elliptic curve with rank ≥ 2.
- Get a lower bound for the density of twists with rank ≥ 2.

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve, and let $\epsilon > 0$. Assume the parity conjecture holds. Then for sufficiently large x we have

$$x^{\frac{1}{2}-\epsilon} \leq \#\{\textit{square-free } D \mid |D| \leq x \textit{ and rank}(E_D) \geq 2\}$$

Our Goal

Prove the theorem for $\mathbb{F}_q(t)$.

Our Goal

Prove the theorem for $\mathbb{F}_q(t)$.

- Figure out what the correct statement is (RTG).
- Prove it (coming).

Our Goal

Prove the theorem for $\mathbb{F}_q(t)$.

- Figure out what the correct statement is (RTG).
- Prove it (coming).

Theorem (conjectured)

Let $E/\mathbb{F}_q(t)$ be an elliptic curve, and let $\epsilon > 0$. Assume the parity conjecture holds. Then for sufficiently large x we have

$$x^{\frac{1}{2}-\epsilon} \leq \#\{\textit{square-free polynomial } D \mid q^{\deg D} \leq x \textit{ and rank}(E_D) \geq 2\}$$

Structure of the original proof

Theorem

If the parity conjecture holds then for sufficiently large x:

$$x^{\frac{1}{2}-\epsilon} \leq \#\{\textit{square-free } D \mid |D| \leq x \textit{ and rank}(E_D) \geq 2\}$$

- $\{$Twists with rank $\geq 2\} \supseteq \{$Twists with rank ≥ 2 and EVEN$\}$
- $\{\dots\} \supseteq \{$square-free D satisfying the right congruence conditions for the rank of E_D to be even, and $rank(E_D) \geq 1\}$

Structure of the original proof

Take the equation of $E : y^2 = x^3 + ax + b$ to have integral coefficients.

- Plug in an integer n on the RHS....get $D\hat{n}^2$ with $D \in \mathbb{Z}$ square-free.
- $(x, y) = (n, \hat{n})$ is a point on the twist E_D.
- Theorem (Shafarevich): Only finitely many twists have points of finite order > 2.
- Therefore, this point on this twist will in general have infinite order, so rank$(E_D) \geq 1$.
- NOW: Make sure D is in the right congruence classes to get rank$(E_D) \geq 2$.

Structure of the original proof

Homogenize the RHS of the equation of $E : y^2 = x^3 + ax + b$ to get $f(X, Z) = X^3 + aXZ + bZ^3$.

- Define $F(X, Z) = Z(X^3 + aXZ + bZ^3)$.
- Any square-free value $D = F(u, v)$ with $u, v \in \mathbb{Z}$ gives you a point on E_D which in general has infinite order.
- Place congruence conditions on u, v so that the $D's$ you get are in the right congruence classes.
- Asymptotics of square-free values of binary integral forms subject to the entries belonging to some fixed congruence classes.

Asymptotics

$$F(X,Z) = Z(X^3 + aXZ + bZ^3)$$

$$\left\{ \begin{array}{c} (u,v) \in \mathbb{Z}^2 \text{ such that } D = F(v,u) \text{ is square-free} \\ \text{and are in the right congruence classes} \end{array} \right\}$$

$$\downarrow$$

$$\left\{ \text{square-free } D \;\middle|\; \text{rank}(E_D) \geq 2 \right\}$$

Show the bottom is large by:

- Showing the fibers are not that large (easy).
- Showing the top is large (hard).

Asymptotics

Setup

- $F(X, Z)$ binary form with integral coefficients and irreducible factors of degree ≤ 3.
- Let M be a positive integer, a_0, b_0 integers that are relatively prime to M.
- $N(x) =$ set of $(a, b) \in \mathbb{Z}^2$ with:
  - $0 \leq a, b \leq x$
  - $a \equiv a_0 \pmod M$, $b \equiv b_0 \pmod M$
  - $F(a, b)$ square-free

Theorem

As $x \to \infty$,

$$\#N(x) = Ax^2 + O(x^2/log^{1/2}x)$$

for an explicitly given constant A.

The translation?

Theorem (Acosta/Leslie, 2009?)

Let $F(u,v)$ *be a homogeneous square-free polynomial with coefficients in* $\mathbb{F}_q[t]$ *such that all of its irreducible factors are of degree* ≤ 3*. Let* $M, a_0, b_0 \in \mathbb{F}_q[t]$ *with* a_0, b_0 *both relatively prime to* M*. Let* $N(x)$ *denote the number of pairs of monic polynomials* (a,b) *satisfying* $q^{\deg(a)}, q^{\deg(b)} \leq x$ *with* $(a,b) \equiv (a_0, b_0) \pmod{M}$ *for which* $F(a,b)$ *is square-free.*
Then as $x \to \infty$*, we have*

$$N(x) = A \cdot x^2 + O(x^2/\log^{1/2}(x))$$

where A *is given by*

$$A = (1/q^{2\deg(M)}) \prod_p (1 - r(p^2)/q^{4\deg(p)})$$

with the product taken over all monic irreducible p*.*