Title here

Daniel Miller

28 April 2017

Cornell University

Outline

Motivation

Sato–Tate Conjecture

Equation of the form $E : y^2 = x^3 + ax + b$.

Sato–Tate Conjecture

Equation of the form $E : y^2 = x^3 + ax + b$.

Simplify: assume $a, b \in \mathbf{Z}$.

Sato–Tate Conjecture

Equation of the form $E : y^2 = x^3 + ax + b$.

Simplify: assume $a, b \in \mathbf{Z}$.

Non-singular: $4a^3 + 27b^2 \neq 0$.

Sato–Tate Conjecture

Equation of the form $E : y^2 = x^3 + ax + b$.

Simplify: assume $a, b \in \mathbf{Z}$.

Non-singular: $4a^3 + 27b^2 \neq 0$.

Count points modulo p:

$$\#E(\mathbf{F}_p) = \#\{(x, y) \in (\mathbf{F}_p)^2 : x^2 = y^3 + ax + b\} + 1.$$

Sato–Tate Conjecture

Equation of the form $E : y^2 = x^3 + ax + b$.

Simplify: assume $a, b \in \mathbf{Z}$.

Non-singular: $4a^3 + 27b^2 \neq 0$.

Count points modulo p:

$$\#E(\mathbf{F}_p) = \#\{(x, y) \in (\mathbf{F}_p)^2 : x^2 = y^3 + ax + b\} + 1.$$

$+1 =$ "point at infinity."

Sato–Tate Conjecture

Equation of the form $E : y^2 = x^3 + ax + b$.

Simplify: assume $a, b \in \mathbf{Z}$.

Non-singular: $4a^3 + 27b^2 \neq 0$.

Count points modulo p:

$$\#E(\mathbf{F}_p) = \#\{(x, y) \in (\mathbf{F}_p)^2 : x^2 = y^3 + ax + b\} + 1.$$

$+1 =$ "point at infinity."

Geometric structure of $E(\mathbf{C})$