The Sato-Tate Conjecture with Non-Zero Rank

Narin Dickerson*

January 24, 2002

Mathematics Department
Princeton University
Princeton, NJ 08544

Abstract

This paper discusses how the distribution predicted by the Sato-Tate Conjecture is dependent upon the rank of an elliptic curve. I provide a theoretical basis for expecting a bias in the distribution as well as experimental results in which the bias can be seen. A more definitive discussion of this bias would include an analysis of the error term causing the bias, but that will not be included here. The data so far gathered has not been precise enough to make a claim beyond the mere existence of the bias.

*E-mail: `ndickers@princeton.edu`

1 First Section: Elliptic Curves and a_p

1.1 Introduction

Before delving into the Sato-Tate Conjecture, I introduce the terminology which I will use, and the general concepts to which the conjecture pertains. First of all, the idea is to study the rational solutions of an elliptic curve, which is a curve E that can be written in the Weierstrass form:

$$E : y^2 = x^3 + ax^2 + bx + c \tag{1.1}$$

These rational solutions are particularly interesting since they form a finitely-generated abelian group by Mordell's Theorem. [Knapp 14]

1.2 a_p and θ_p

Closely related to the rational solutions are the integer solutions to E modulo a prime p. If there are no solutions to a curve E modulo p, for some prime p, then there are no integer solutions to the curve. Presumably, we can learn something worthwhile about the curve by seeing how the number of solutions modulo a prime p are related to the prime p. One way to write the number of such solutions is as follows:

$$N_p = 1 + p - a_p \tag{1.2}$$

In this equation, N_p is the number of solutions satisfying $E \mod p$. The addition of 1 represents the projective solution at infinity. According to the Hasse-Weil Theorem, the number a_p is bounded in terms of p.

Theorem 1.1 (Hasse-Weil) *If E is a non-singular irreducible curve of genus g defined over the finite field F_p, then the number of points on E with coordinates in F_p is $p + 1 + \epsilon$, where ϵ satisfies $|\epsilon| \leq 2g\sqrt{p}$.*

The proof for $g = 1$ is due to Hasse, and the proof for arbitrary g is due to Weil. [Silverman 110] The proofs are too complicated to include here. Elliptic curves are curves of genus 1 so that this simplifies to give the bound $|a_p| \leq 2\sqrt{p}$. We can therefore write $a_p = \alpha_p + \beta_p$ where α_p and β_p are complex numbers satisfying

$$\begin{aligned} \alpha_p &= \bar{\beta}_p \\ \alpha_p \beta_p &= p \end{aligned}$$

We take the angle of α_p, which is between 0 and π and call it θ_p. We can also write $\theta_p = \arccos(\frac{a_p}{2\sqrt{p}})$. The Sato-Tate Conjecture concerns the distribution of these angles θ_p.

2 Sato-Tate and Complex Multiplication

Conjecture 2.1 (Sato-Tate) *Assume that the cubic curve E does not have complex multiplication. For any fixed angles $0 \leq \gamma \leq \omega \leq \pi$,*

$$\lim_{x\to\infty} \frac{\#\{p \leq X : \gamma \leq \theta_p \leq \omega\}}{\#\{p \leq X\}} = \frac{2}{\pi}\int_\gamma^\omega \sin^2 t dt$$

[Silverman 120]

The conjecture stems from a similar and proven result in function field theory. Since the conjecture only applies to curves without complex multiplication, I include a discussion of complex multiplication. Happily, the case for complex multiplication (CM) curves is actually nicer and was proven by Weil and Deuring. [Katz 273]

Definition 2.1 (complex multiplication) *The complex sulutions of an elliptic curve form a complex torus $\mathbb{C}/L$ generated by a lattice L. An elliptic curve E is said to have complex multiplication when there is a map from $\mathbb{C}$ to itself $\varphi : x \to \varphi x$ such that φ is not integer multiplication and preserves the lattice L. [Katz 273]*

By integer multiplication, we mean repeated application of the group addition law for rational solutions. Such a map clearly maps points on the curve to other points on the curve. An example of a map that is not integer multiplication and thus complex multiplication occurs with the curve $E : y^2 = x^3 - 1$. Take $\varphi : (x, y) \to \left(e^{2\pi i/3}, y\right)$. Any (x, y) solving the curve are mapped to another (x, y) solving the curve and E is said to have complex multiplication. Now, let's see what happens with a_p. Another example of a curve with complex multiplication is $E : y^2 = x^3 - x$. It turns out that there is another way of writing a_p which lends itself to our situation. This method involves the Legendre symbol, which I now define.

Definition 2.2 (Legendre symbol) *The Legendre symbol represents the* *following function based on quadratic residues. For m and n integers,*

$$\left(\frac{m}{n}\right) = \begin{cases} 0 & \text{if } m|n. \\ 1 & \text{if there exists an integer } x \text{ such that } x^2 \equiv m \mod n. \\ -1 & \text{if such } x \text{ does not exist.} \end{cases} \tag{2.1}$$

If we write E as $y^2 = f(x)$, we can now write

$$a_p = - \sum_{x \mod p} \left(\frac{f(x)}{p}\right) \tag{2.2}$$

The two definitions can be seen as equivalent. Substituting into our original equation for the number of solutions, we get

$$\begin{aligned} N_p &= 1 + p + \sum_{x \mod p} \left(\frac{f(x)}{p}\right) \\ &= 1 + \sum_{x \mod p} \left(\left(\frac{f(x)}{p}\right) + 1\right) \end{aligned} \tag{2.3}$$

This makes sense. We still have the 1 solution at infinity. We get two more solutions when $f(x)$ is a square modulo p. We get one more when $f(x) \equiv 0 \mod p$(equivalently, that $f(x)|p$. Otherwise, we get no solutions. All of the solutions are accounted for in equation 2.3. Now, let's remember again the equation with CM, $f(x) = x^3 - x$. The complex multiplication in this case is $\varphi : (x, y) \to (-x, iy)$. We have then:

$$\begin{aligned} \sum_{x \mod p} \left(\frac{x^3 - x}{p}\right) &= \sum_{x \mod p} \left(\frac{(-x)^3 - (-x)}{p}\right) \\ &= \sum_{x \mod p} \left(\frac{-(x^3 - x)}{p}\right) \\ &= \sum_{x \mod p} \left(\frac{x^3 - x}{p}\right)\left(\frac{-1}{p}\right) \\ &= \sum_{x \mod p} \left(\frac{x^3 - x}{p}\right)(-1)^{(p-1)/2} \\ &= (-1)^{(p-1)/2} \sum_{x \mod p} \left(\frac{x^3 - x}{p}\right) \end{aligned} \tag{2.4}$$

For $p \equiv 3 \mod 4$, this simplifies to

$$\sum_{x \mod p} \left(\frac{x^3 - x}{p}\right) = - \sum_{x \mod p} \left(\frac{x^3 - x}{p}\right) \tag{2.5}$$

This implies that the sums are both 0 and that $a_p = 0$. This clearly leads to a different distribution than Sato-Tate. Additionally, for this choice of E, primes such that $p \equiv 1 \mod 4$ can be written as $p = \pi\bar{\pi}$ in $\mathbb{Z}[i]$. It turns out that $\{\pi, \bar{\pi}\}$ is the same as $\{\alpha_p, \beta_p\}$. [Katz 279]

3 Expecting a Rank Bias in Sato-Tate

I will first provide a definition of rank. I will then give an intuitive reason behind this paper followed by a much more mathematical one. Recall from the first section that the rational solutions of an elliptic curve E form a finitely-generated abelian group. $E(\mathbb{Q})$.

Definition 3.1 (geometric rank of an elliptic curve) *We can write $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus F$, where F is referred to as the torsion group and is both finite and abelian.*

The rank of the group $E(\mathbb{Q})$ is r. [Knapp 102]

Intuitively, an increased rank indicates an increased number solutions modulo p. Hence we mightexpect a bias toward a_p being negative. If N_p is affected by the rank, so is a_p. Something more convincing in favor of a bias comes in the form of the Silverman-Rosen Theorem. This theorem provides us with a concrete relationship between rank and a_p. However, the relation is with the rank of a family rather than the rank of a particular curve. Therefore, another definition is required, that of a family. For this paper, the discussion of families of elliptic curves will be limited to the discussion of one-parameter families. A one-parameter family is one where the coefficients of the curve are replaced by polynomial functions of t. Families of particular interest are those of the form $y^2 = x^3 + A(t)x + B(t), t \in \mathbb{Z}$.

Theorem 3.2 (Silverman-Rosen Theorem) *Let $\mathbf{E}$ be the above family of elliptic curves with $A(t)$ and $B(t)$ integer polynomials of degree at most 3 and 5. To each t corresponds an elliptic curve E_t.*

$$a_{\mathbf{E}_t}(p) = -\sum_{x=0}^{p-1} \left(\frac{x^3 + A(t)x + B(t)}{p}\right) \tag{3.1}$$

Now, we write

$$A_{\mathbf{E}}(p) = \frac{1}{p}\sum_{t=0}^{p-1} a_{E_t}(p) \tag{3.2}$$

Then

$$\lim_{X\to\infty}\sum_{p\leq X} -A_{\mathbf{E}}(p)\log p = rank\left(\mathbf{E}\left(\mathbb{Q}(T)\right)\right) \tag{3.3}$$

This result is related to the rank of a family rather than an individual curve and a sum of a_p's rather than an individual a_p. However, we can use it to get a crude estimate of bias in individual a_p's. From the $\log p$ term in the infinite sum, we expect any bias to diminish with p. It turns out that we expect the bias to be around $\frac{r}{sqrtp}$ for each a_p. This bias will then vanish in the limit of the Sato-Tate Conjecture. However, the rest of this paper aims to explore its influence on the distribution of a_p in finite cases.

4 Experimental Findings

4.1 Beginnings

The first thing that I did was modify a program in the C programming language that used functions from the software package Pari. The program was very simple and tested to see if there was any bias in θ_p by taking the sum $\sum_{i=1}^{800000} a_{p_i}$ where p_i is the ith prime. I chose to do this since it required less calculation and the range was easier to work with. I played around calculating this for a few different curves of rank 2 and rank 0. The results hinted at a bias, but showed nothing definite. For some curves, the sum would vary noticeably even with more summands. I also had the program display a small smattering (ten) of the partial sums along the way.

5 Bibliography

N. Katz, Exponentional Sums over Finite Fields and Differential Equations over the Complex Numbers: Some Interactions, Bulletin of the AMS 23 (2) 269-309.

A. Knapp, Elliptic Curves, Princeton Univ. Press, Princeton, N.J., 1992.

S. Miller, Constructing One-Parameter Families with Forced Rank, Bounding the Average Rank of One-Parameter Families, 2001.

J. Silverman and J. Tate, Rational Points on Elliptic Curves, Springer, New York, 1992.