# The Nagao Conjecture

Leo Goldmakher, Steven Miller

January 20, 2002

**Abstract**

After covering the necessary background material, we describe the Nagao Conjecture:

$$\lim_{X\to\infty} \frac{1}{X} \sum_{p\leq X} -A_{\mathcal{E}}(p)\log p = \mathrm{rank}\left(\mathcal{E}\left(\mathbb{Q}(T)\right)\right) \ .$$

In particular we discuss the Silverman-Rosen Theorem and other current results. In the second part of the paper, we describe the results of our computational work on the subject.

# 1 The Theory

## 1.1 Introduction

Let $E$ be an elliptic curve (we can assume $E$ is in the Weierstrass normal form, after the necessary transformations) over $\mathbb{Q}$ (by which we mean $E$ has rational coefficients, and we consider the rational solutions).

We now define some parameters which will be used. Suppose $E$ is our curve, in the form $y^2 = f(x) = x^3 + ax + b$. For any prime $p$ we define

$$N_p(E) = \#\{(x, y) : x, y \in \mathbb{Z}/p\mathbb{Z} \text{ and } y^2 \equiv f(x) \bmod p\} \tag{1}$$

We further define

$$a_p(E) = p + 1 - N_p(E) \tag{2}$$

At first, Nagao examined

$$s(N, E) = -\frac{1}{N} \sum_{p \leq N} a_p(E) \cdot \log p\,,$$

but unfortunately, from the numerical evidence it was impossible to conclude whether or not $s(N, E)$ converges as $N \to \infty$.

So Nagao turned to studying one-parameter families instead. We make parallel definitions to equations 1 and 2, except this time for the family of curves $\mathcal{E} : y^2 = f_t(x) = x^3 + A(t)x + B(t)$.

We first let $E_t$ be $\mathcal{E}$ evaluated at $t$. Then we define

$$a_t(p) = a_p(E_t)\,. \tag{3}$$

In fact, there is a simple formula for $a_t(p)$, which we now derive. Recall the definition of the Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \neq 0,\ a \text{ is a perfect square in } \mathbb{Z}/p\mathbb{Z} \\ 0 & a = 0 \\ -1 & a \text{ is not a perfect square in } \mathbb{Z}/p\mathbb{Z} \end{cases}$$

We claim that for each $x$ in $\mathbb{Z}/p\mathbb{Z}$, the number of $y$ in $\mathbb{Z}/p\mathbb{Z}$ s.t. $y^2 \equiv f_t(x) \bmod p$ is

$$1 + \left(\frac{f_t(x)}{p}\right)$$

The proof of this claim is trivial; simply consider the three cases $f_t(x)$ is a non-zero perfect square in $\mathbb{Z}/p\mathbb{Z}$, $f_t(x) \equiv 0 \bmod p$, and $f_t(x)$ is not a perfect sqare in $\mathbb{Z}/p\mathbb{Z}$, and verify. For example, suppose for some $x$ we have $f_t(x)$ is a non-zero perfect square mod$p$. Then there are two distinct values of $y$ in $\mathbb{Z}/p\mathbb{Z}$ s.t. $y^2 \equiv f_t(x) \bmod p$. And $1 + \left(\frac{f_t(x)}{p}\right) = 2$.

Thus $\widetilde{N_p}(E_t)$, the number of rational solutions not counting the rational point at infinity, can be calculated as

$$\widetilde{N_p}(E_t) = \sum_{x \bmod p} \left[1 + \left(\frac{f_t(x)}{p}\right)\right], \tag{4}$$

whence we have

$$a_t(p) = -\sum_{x \bmod p} \left(\frac{f_t(x)}{p}\right). \tag{5}$$

Now, two more definitions:

$$A_{\mathcal{E}}(p) = \frac{1}{p} \sum_{t \bmod p} a_t(p) \tag{6}$$

and

$$S(N, \mathcal{E}) = -\frac{1}{N} \sum_{p \leq N} A_{\mathcal{E}}(p) \log p \tag{7}$$

To give the reader a firmer grasp of how one actually calculates $A_{\mathcal{E}}(p)$, we now explicitly derive a formula for it for one specific family.

## 1.2 A nice family

Let $\mathcal{E}$ denote the family $\mathcal{E} : y^2 = f_t(x) = x^3 - t^2 x + t^4$. This family has many nice properties. For example, one can almost immediately see two points on this curve: $(t, t^2)$ and $(t^2, t^3)$.

As we now demonstrate, another nice property is that this family has $A_{\mathcal{E}}(p) = -2$ for all primes $p$.

From equations 5 and 6 we have

$$-pA_{\mathcal{E}}(p) = \sum_{x(p)} \sum_{t(p)} \left(\frac{f_t(x)}{p}\right)$$

$$
\begin{aligned}
& = \sum_{x(p)} \sum_{t(p)} \left( \frac{t^4 - t^2 x + x^3}{p} \right) \\
(8) \qquad & = \sum_{x(p)} \left( \frac{x^3}{p} \right) + \sum_{x(p)} \sum_{t=1}^{p-1} \left( \frac{t^4 - t^2 x + x^3}{p} \right) \\
(9) \qquad & = \sum_{x(p)} \left( \frac{x}{p} \right) + \sum_{x(p)} \sum_{t=1}^{p-1} \left( \frac{t^4 - t^3 x + t^3 x^3}{p} \right) \\
(10) \qquad & = 0 + \sum_{x(p)} \sum_{t=1}^{p-1} \left( \frac{t^2}{p} \right) \left( \frac{t^2 + (x^3 - x)t}{p} \right) \\
(11) \qquad & = \sum_{x(p)} \sum_{t=1}^{p-1} \left( \frac{t^2 + (x^3 - x)t}{p} \right)
\end{aligned}
$$

Note that in equation 8 we split the sum over $t$ into two sums: one for $t = 0$, and the other for $t \neq 0$. From equation 8 to 9 we make two changes. First, observe that $\left(\frac{x^3}{p}\right) = \left(\frac{x}{p}\right)$. Secondly, for any fixed non-zero $t \in \mathbb{Z}/p\mathbb{Z}$ we have

$$\{tx : x \in \mathbb{Z}/p\mathbb{Z}\} = \{x \in \mathbb{Z}/p\mathbb{Z}\}$$

Thus to get from equation 8 to equation 9 we map $x$ to $tx$, in the sum over all non-zero $t$.

To get from equation 9 to equation 10, we again make two changes. It is well-known (and follows easily from the classical theorem that $\mathbb{Z}/p\mathbb{Z}$ is cyclic) that $\sum_{x(p)} \left(\frac{x}{p}\right) = 0$. We also make use of the fact (trivially verified) that the Legendre symbol is multiplicative, i.e. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

It is a well-known result that

$$\sum_{t(p)} \left( \frac{at^2 + bt + c}{p} \right) = \begin{cases} p - 1 & \text{if } p \text{ divides } (b^2 - 4ac) \\ -1 & \text{if } p \text{ does not divide } (b^2 - 4ac) \end{cases}$$

In our case, the discriminant is $(x^3 - x)^2$. By factoring, we see that if $p$ divides $(x^3 - x)^2$ iff $x \equiv 0, \pm 1 \bmod p$.

Thus continuing where we left off in equation 11, we have

$$-pA_{\mathcal{E}}(p) \;=\; \sum_{x(p)} \sum_{t=1}^{p-1} \left( \frac{t^2 + (x^3 - x)t}{p} \right)$$

$$
\begin{aligned}
&= \sum_{x(p)} \sum_{t(p)} \left( \frac{t^2 + (x^3 - x)t}{p} \right) \\
&= \sum_{x=0,\pm 1} (p-1) + \sum_{x \neq 0,\pm 1} (-1) \\
&= 3(p-1) + (p-3)(-1) \\
&= 2p
\end{aligned}
$$

Thus, we have proved that $\forall p$, $A_{\mathcal{E}}(p) = -2$, where $\mathcal{E}$ is the family $y^2 = x^3 - t^2 x + t^4$.

## 1.3 The Nagao Conjecture

We finally arrive at the Nagao Conjecture:

$$\lim_{N\to\infty} S(N, \mathcal{E}) = \mathbb{Q}(T) - \text{rank of } \mathcal{E} \tag{12}$$

The conjecture is very strongly supported numerically (see below), and in fact has shown to be true in special cases. Nagao himself proved his conjecture for five families:
(i) $\mathcal{E}_1 : y^2 = f(x) + T$, where $f(x) \in \mathbb{Z}[x]$ is a monic cubic with no double roots
(ii) $\mathcal{E}_2 : y^2 = f(x) + T^2$, where $f(x) \in \mathbb{Z}[x]$ is a monic cubic with no double roots
(iii) $\mathcal{E}_3 : y^2 = x^3 - 3T^4 x - T^2(1 + T^8)$
(iv) $\mathcal{E}_4 : y^2 = x^3 - k^2(T^3 - T)^2 x$, where $k \in \mathbb{Z}, k \neq 0$
(v) $\mathcal{E}_5 : y^2 = x^3 - k^2(T^4 + 1)^2 x$, where $k \in \mathbb{Z}, k \neq 0$
Then, assuming that the Sato-Tate conjecture holds, he proved one more special case.

To prove these results, Nagao uses clever manipulations to find $\lim_{N\to\infty} S(N, \mathcal{E})$, and Shioda's Theorem (with some basic Galois theory) to find the $\mathbb{Q}(T)$-rank of his elliptic curves. Although I do not understand Shioda's Theorem in its full generality, in a simplified form it can be stated as follows:

**Theorem 1.1 (Shioda's Theorem)** *Let $b_1$, $b_2$, $b_3$ be distinct rational numbers. Then the $\mathbb{Q}(T)$-rank of the elliptic curve*

$$\mathcal{E} : y^2 = (x - b_1)(x - b_2)(x - b_3) + T^2$$

*is 2, and $\mathcal{E}$ is generated by $P_1 = (b_1, T)$ and $P_2 = (b_2, T)$.*

## 1.4 Silverman/Rosen Theorem

In his original paper, Nagao stated that there should be a connection between his conjecture and Tate's conjecture. And this is exactly what Silverman and Rosen proved - that Tate's conjecture in fact implies Nagao's conjecture. We first state Tate's conjecture:

**Conjecture 1.2 (Tate's Conjecture)** *Let $L_2(\mathcal{E}/K, s)$ be the Hasse-Weil L-function of $\mathcal{E}/K$ attached to $H^2_{\acute{e}t}(\mathcal{E}/\bar{K}, \mathbb{Q}_\ell)$, and let $NS(\mathcal{E}/K)$ be the Néron-Severi group of $\mathcal{E}/K$. Then $L_2(\mathcal{E}/K, s)$ has a meromorphic continuation to $\mathbb{C}$ and has a pole at $s = 2$ of order*

$$-ord_{s=2} L_2(\mathcal{E}/K, s) = rank\ NS(\mathcal{E}/K)\,.$$

This statement of the conjecture is purely for the reader's enjoyment - the writer does not understand it. Those readers with a similar background to that of the author may prefer to look at the conjecture as talking about a function similar to the zeta-function; and the conjecture is that there is a meromorphic continuation of this function, with a pole at $s = 2$ of a certain order.

The main result of Silverman's and Rosen's paper [S-R] is their proof that if Tate's conjecture holds, and also if the $\zeta$-like function $L_2(\mathcal{E}/K, s)$ does not vanish on the line $\mathrm{Re}(s) = 2$, then the Nagao conjecture must hold. (This will bring to mind the Prime Number Theorem, which is proven using the fact that the zeta function does not vanish on the line $\mathrm{Re}(s) = 1$, the line on the edge of the critical strip. In our case, the line $\mathrm{Re}(s) = 2$ is the edge of the critical strip for the function $L_2(\mathcal{E}/K, s)$.)

An application of this result, which they state in their paper, is that the Nagao conjecture holds for rational surfaces. A rational surface is a family $\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$ which satisfies one of the two properties:
(i) $0 < \max\{3 \deg A, 2 \deg B\} < 12$, or
(ii) $3 \deg A = 2 \deg B = 12$, and $\mathrm{ord}_{T=0} T^{12} \Delta(T^{-1}) = 0$

Since, as Silverman and Rosen humorously put it, it "seems to be 'well-known,' but lacking a suitable reference" [S-R] that Tate's conjecture holds for rational surfaces, their theorem implies that Nagao's conjecture must also hold on rational surfaces.

As much as I would like to write up the proof, my lack of knowledge of Cohomology Theory (among other things) precludes any such attempt. However, the knowledgeable reader is encouraged to read the original paper [S-R].

# 2 Computational work

## 2.1 Introduction

There have been many numerical studies of families of elliptic curves. In particular Fermigier's study of ranks of one-parameter families is very extensive. However, to our knowledge, all large-scale studies have been done on "non-generic" families of elliptic curves, where by non-generic we mean curves with constant $A_{\mathcal{E}}(p)$ (constant past the first few primes). Our goal computationally is thus to do a study of families with non-constant $A_{\mathcal{E}}(p)$. Thus far we have dealt with such families, all of whose $A_{\mathcal{E}}(p)$'s are integral (and non-constant). We wish to check the Nagao conjecture for curves which are also not rational surfaces. In addition, we are interested in how quickly the Nagao average $S(N, \mathcal{E})$ (see equation 7) converges to the rank of the family. Also, what causes all the $A_{\mathcal{E}}(p)$ in certain curves to be integral is, to our knowledge, unknown. This forms an interesting theoretical question, which perhaps would be easier to answer after seeing numerical data (e.g. are the $A_{\mathcal{E}}(p)$'s bounded? by what? etc.). If the Nagao conjecture is indeed true, and if the Nagao average converges sufficiently quickly to the rank, then this would be the best computational tool available for calculating the rank of a family.

## 2.2 Computation

We programmed in C, making calls on the PARI package to find the various parameters of the elliptic curves. We created two programs. One was a modified program (originally written by Steven Miller) to calculate numerically the values of the $A_{\mathcal{E}}(p)$'s and the $S(N, \mathcal{E})$. The algorithms used were standard, and fairly efficient. Rather than using any integer $N$ in $S(N, \mathcal{E})$, we used the $N^{\text{th}}$ prime, which was read in from an enormous file of primes. This program ran very smoothly, and was an excellent tool for predicting which curves were interesting - as it ran, output was the $A_{\mathcal{E}}(p_N)$ and $S(p_N, \mathcal{E})$ for each prime $p_N$, so we could observe whether or not the values were integral, what convergence was like, etc. So far, this program seems to be confirming the Nagao conjecture in every case tested, and the Nagao averages converge rather quickly to the rank. One nice aspect of the convergence is that, since the rank is always an integer, it becomes clear very quickly which integer the averages are moving towards.

The other proram was a collaboration between the author, Stephen Lu, and Steven Miller, though again the program was written largely by Steven Miller. The purpose of the second program was to find the rank numerically, given a family of elliptic curves. For the main algorithms, I refer the reader to Stephen Lu's paper, as well as to Jon Hsu's (who wrote a program directly in the PARI programming environment, which, although slow, was great for debugging purposes). Currently, the results outputted by this program are in agreement with those published by Fermigier in his paper. However, the program is currently limited by how big the conductor becomes. The author has had several ideas on how to alleviate this problem; however, none of them have been implemented yet.

The two programs are complementary in a very natural way; once the second program becomes more efficient, we can check the Nagao conjecture directly by running the same curve through the two programs, and seeing whether or not the averages in the first program converge to the rank calculated by the second.

### 2.3 Plans

The most immediate plan is to increase the efficiency of the second program. Once this is accomplished, we can run "interesting" families through both programs, and see what comes out of these tests.

I would like to thank Professor Andrew Wiles for introducing me to this beautiful subject, and Steven Miller for countless hours and extreme patience.

## 3 Bibliography

## References

[1] Stefane Fermigier. *Etude experimentale du rang de familles de courbes elliptiques sur Q*. Experimental Math., Vol5 (1996), No. 2.

[2] J. H. Silverman, J. Tate. *Rational Points on Elliptic Curves*. Springer, New York, 1992.

[3] M. Rosen, J. H. Silverman. *On the rank of an elliptic surface*. Inventones. Math., 133 (1998).

[4] Koh-ichi Nagao. *Q(T)-rank of elliptic curves and certain limits coming from local points.* manuscripta math. 92, 13-32 (1997).