# Computing the Lang-Trotter Constant

Neil Calkin, Lauren Huckaba, Kevin James,
Jason Joyner, Josh Schwartz, Ethan Smith

July 9, 2008

**Abstract**

In this paper, we compute constants $C_{E,r}$ found in the Lang-Trotter conjecture for many elliptic curves $E$ and integers $r$. These computations are simplified when $E$ belongs to a special class of curves called Serre curves. This is due to the fact that the image of the Galois representation for $E$ is as large as possible for a Serre curve.

## 1 Introduction

First, we recall some facts about elliptic curves. Recall that an elliptic curve $E$ over a field $K$ is a nonsingular plane curve of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

The discriminant for such a curve is given by $\Delta = -16(4A^3 + 27B^2)$. In this paper, we consider elliptic curves over $\mathbb{Q}$ and their reductions modulo primes $q$. A minimal model for $E$ is an equation of the form (1) with smallest discriminant. When reducing modulo $q$, we always work with a minimal model. In the the cases where $q$ is not 2 or 3, we may assume that our minimal model can be reduced to the form

$$E : y^2 = x^3 + Ax + B. \tag{2}$$

If the reduction of $E$ modulo $q$ is nonsingular, then $E$ is said to have good reduction at $q$. Otherwise, $E$ is said to have bad reduction at $q$. There are two cases of bad reduction.

(i) $E$ has additive reduction if its reduction modulo $q$ has a cusp, or a root of multiplicity 3 modulo $q$.

(ii) $E$ has multiplicative reduction if its reduction modulo $q$ has a node, or a root of multiplicity 2 modulo $q$.

**Definition 1.** *An elliptic curve is **semistable** if and only if the curve has good reduction all primes $p$ or multiplcative reduction at all primes $p$.*

We want establish a simple way to determine whether a given elliptic curve is semistable For a given elliptic curve $E$, define $f_p$ as follows:

$$f_p = \begin{cases} 0, \text{ if } E \text{ has good reduction at } p, \\ 1, \text{ if } E \text{ has multiplicative reduction at } p, \\ 2+\delta_p, \text{ if } E \text{ has additive reduction at } p. \end{cases}$$

The value of $\delta_p$ is equal to 0 for fields of characteristic $\neq 2, 3$. We use Tate's algorithm [3] to determine the values of $f_p$.

**Definition 2.** *The* ***conductor*** $N_E$ *of an elliptic curve E is defined as:*

$$N_E = \prod_p p^{f_p}$$

The following theorem simply follows from the definitions of semistability and the conductor of an elliptic curve:

**Theorem 1.** *An elliptic curve E is semistable if and only if the conductor* $N_E$ *is square-free.*

**Conjecture 1** (Lang and Trotter)**.** *Let $E$ be an elliptic curve, $q$ a prime, and $r \in \mathbb{Z}$,*

$$\#\{q \le X : a_q(E) = r\} \sim C_{E,r} \frac{\sqrt{X}}{\log X},$$

*where $C_{E,r}$ is some explicit constant defined in terms of Galois representations and the error term is defined as $a_q(E) = q + 1 - \#E(\mathbb{F}_q)$.*

We now describe the constant $C_{E,r}$. The absolute Galois group acts on the N-torsion points of $E$ as follows:

$$\begin{array}{rcl} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \times E[N] & \longrightarrow & E[N] \\ (\sigma, (x, y)) & \longmapsto & (\sigma x, \sigma y) \end{array}$$

This action induces the representation

$$\phi_{N,E} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

For any subgroup $G$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, let $G_r$ denote the subset of elements with trace $r$. By [9] (see also [4]), there is an integer $m_E$ such that for all primes $q \nmid m_E$, $\phi_{q,E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ $= \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$.

Then Lang and Trotter [6] define

$$C_{E,r} := \frac{2}{\pi} \cdot \frac{m_E \cdot \#(\phi_{m_E,E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))_r)}{\#(\phi_{m_E,E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})))} \prod_{\substack{p \nmid m_E \\ p \nmid r}} \frac{p(p^2-p-1)}{(p+1)(p-1)^2} \prod_{\substack{p \nmid m_E \\ p | r}} \frac{p^2}{p^2-1}. \tag{3}$$

We calculate the constant $C_{E,r}$ for a range of $r$ and for a number of elliptic curves $E$ that are Serre curves.

**Lemma 1.** *The size of* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *is* $\displaystyle\prod_{p|N}(p^2-1)(p^2-p)(p^{4(\mathrm{ord}_p(N)-1)})$.

*Proof.* To compute the size of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, for $N$ prime, we look at an element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. By definition, the columns of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ are linearly independent. There are $N$ choices for $a$ and $N$ choices for $c$. However, linear independence implies that the zero vector cannot be included in the set of vectors $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$. So, there are $N^2-1$ choices for $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$. The vector $\left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right)$ cannot be a multiple of $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$. Similarly, there are $N^2$ choices for $\left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right)$ and since there are $N$ choices for both $a$ and $c$, there are $N$ possible multiples of the vector $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$. Therefore, there are $N^2-N$ choices for $\left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right)$, giving $(N^2-1)(N^2-N)$ elements in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

When $N$ is not prime, then $N$ is the product of prime powers, $p_1^{n_1}, ..., p_k^{n_k}$ and the size of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is $\displaystyle\prod_{p|N}(p^2-1)(p^2-p)(p^{4(\mathrm{ord}_p(N)-1)})$. Then $N$ can be factored as the product, $M_1...M_k$, where $M_i = p_i^{n_i}$. A matrix in $\mathrm{GL}_2(\mathbb{Z}/M_i\mathbb{Z})$ has the form $\left(\begin{smallmatrix} a_0+a_1p_i & b_0+b_1p_i \\ c_0+c_1p_i & d_0+d_1p_i \end{smallmatrix}\right)$, where $a_0, b_0, c_0, d_0 \in \mathbb{Z}/p_i\mathbb{Z}$ and $0 \leq a_1, b_1, c_1, d_1 < p_i^{n_i-1}$. Recall that there are $(p_i^2-1)(p_i^2-p_i)$ choices for $a_0, b_0, c_0$, and $d_0$. Similarly, there are $p_i^{n_i-1}$ choices for each $a_1, b_1, c_1$, and $d_1$, i.e. $p_i^{(n_i-1)^4}$ combinations of $a_1, b_1, c_1$, and $d_1$. So, there are $(p_i^2-1)(p_i^2-p_i)p_i^{(n_i-1)^4}$ choices for $\left(\begin{smallmatrix} a_0+a_1p_i & b_0+b_1p_i \\ c_0+c_1p_i & d_0+d_1p_i \end{smallmatrix}\right)$. Then, $\#\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) = \#\mathrm{GL}_2(\mathbb{Z}/M_1\mathbb{Z})\cdots\#\mathrm{GL}_2(\mathbb{Z}/M_k\mathbb{Z})$. □

## 2 Acknowledgements

We are grateful to
Dr. Nigel Boston for his insight and interest in the topic.
Richard Crandall for pointing us to the prime zeta function.
Jobby Jacobs for his help with submitting jobs to Clemson Condor.
Eric Manley for pointing us to Pari/GP and allowing us to view his code.
Aaron Rosen for his unlimited support with programming in C and the Linux environment.
Dr. Matt Saltzman for his evaluation of our programming techniques.
Dr. Paul Savas for his sessions on high throughput and parallel computing.
Dr. Dan Warner for his advice concerning high throughput computations.

## 3 The Definition of a Serre Curve

Roughly speaking, a Serre curve is an elliptic curve whose torsion subgroup has as much Galois symmetry as possible. Serre has shown that the image of $\phi_{M_W,E}$ is always contained in a subgroup of index 2 called the Serre subgroup and denoted by $H_{M_W}$. The curve $E$ is said to be a Serre curve when $\phi_{M_W,E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = H_{M_W}$.

**Definition 3.** *The* ***Serre number*** *for some elliptic curve E is:*

$$M_{\Delta_{sf}}(E) = \begin{cases} 2|\Delta_{sf}|, & \textit{if } \Delta_{sf} \equiv 1 \pmod 4 \\ 4|\Delta_{sf}|, & \textit{otherwise} \end{cases}$$

*where $\Delta_{sf}$ is the square-free part of the discriminant of $E$.*

The definition of a Serre curve is as follows.

**Definition 4.** *An elliptic curve $E$ is a* ***Serre curve*** *if for every $m \in \mathbb{Z}^+$, we have:*

$$[\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \phi_{m,E}(G_\mathbb{Q})] = \begin{cases} 2, & if\ M_{\Delta_{sf}} | m \\ 1, & otherwise \end{cases}$$

**Definition 5.** *The integer $N$ is said to be* ***exceptional*** *for $E$ if $\phi_{N,E}$ is not surjective.*

**Theorem 2.** *[7, p. 131] Let $E$ be a semistable elliptic curve, and $N$ a prime number. Then the image of $\phi_{N,E}$ is $GL_2(\mathbb{Z}/N\mathbb{Z})$ if $N \geq 11$. Equivalently, there are no exceptional primes $N \geq 11$ for a semistable elliptic curve $E$.*

In [5, Lemma 5], we find the following sufficient conditions for an elliptic curve to be Serre.

**Lemma 2.** *If $E$ over $\mathbb{Q}$ is an elliptic curve such that:*

*(i) $E$ has no exceptional primes.*

*(ii) $E$ is not exceptional at $4$ or $9$.*

*(iii) The index $[\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) : \phi_{8,E}(G_\mathbb{Q})] \neq 2$.*

*(iv) There exists a prime $p > 3$ which divides the Serre number $M_{\Delta_{sf}}(E)$.*

*Then, $E$ is a Serre curve.*

We see that checking an elliptic curve for semistability is a matter of calculating the conductor. It is easy to apply Lemma 2 to semistable curves because we need only check that primes less than 11 are not exceptional.

To identify Serre curves, we use [8, Theorem 3.2] by Reverter and Vila, as well as the Antwerp tables [1] to choose curves to which we can apply Lemma 2. From this theorem we see that for many elliptic curves $E/\mathbb{Q}$ without complex multiplication and with conductor $N_E \leq 200$, $E$ has no exceptional primes. For these curves, we need only check conditions $2-4$ of Lemma 2.

# 4 Examples of Serre Curves

**Proposition 1.** *The following elliptic curves in table A.1 are Serre curves.*

*(i) $E_1 : y^2 = x^3 - 4x + 4$*

*(ii) $E_2 : y^2 = x^3 + 32x + 212$*

*Proof.* First, we consider the curve $E_1$. According to part $(i)$ of the theorem by Reverter and Vila [8] the fact that $E_1$ has conductor $88 \leq 200$ and does not have complex multiplication implies that $\rho_{E,p}(G_{\mathbb{Q}})$ is $\mathrm{GL}_2(\mathbb{F}_p)$ for all prime numbers $p > 13$. Therefore, $E_1$ has no exceptional primes greater than 13. Part $(iii)$ of the theorem states that the image of $\rho_{E,11}(G_{\mathbb{Q}})$ is $\mathrm{GL}_2(\mathbb{F}_{11})$ with the exception of five curves, not including $E_1$. Parts $(iv)$, $(v)$, and $(vi)$ show that the primes 7, 5, and 3 are not exceptional. We now check that $E_1$ is not exceptional at 8 and 9. Since we have checked whether $2^3 = 8$ is exceptional, we are not required to check if $2^2 = 4$ is exceptional because if $E$ is not exceptional at $p^n$, then $E$ is not exceptional at $p^{n-1}$, for $p$ prime. Recall then, that the integer $N$ is exceptional for $E$ if $\phi_{N,E}$ is not surjective. Therefore, in order to verify that $E_1$ is a Serre curve, we compute $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ as well as $\mathrm{Gal}(\mathbb{Q}(E[8])/\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}(E[9])/\mathbb{Q})$. Then we compare the size of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with its corresponding Galois group. However, the 8th and 9th division polynomials, whose roots give $x$-coordinates for $E[8]$ and $E[9]$ respectively, are the minimal polynomials $\mathbb{Q}(E[8])/\mathbb{Q}$, and $\mathbb{Q}(E[9])/\mathbb{Q}$. Therefore,

We use the Galois group function in Magma [2] to compute the size of $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ for $n = 8, 9$.

Now we consider the curve $E_2$. $E_2$ does not have complex multiplication and has conductor $N_E = 140$, according to the Antwerp tables [1]. Similar to $E_1$, [8, Theorem 3.2] gives $\rho_{E,p}(G_{\mathbb{Q}})$ is $\mathrm{GL}_2(\mathbb{F}_p)$, for all prime numbers $p > 13$, meaning $E_2$ has no exceptional primes greater than 13. In the same manner as $E_1$, we use parts $(iii)$-$(vi)$ of the theorem to confirm that $E_2$ has no exceptional primes.

Again, we use the Galois group function in Magma [2] to compute the size of $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ for $n = 8, 9$. □

**Proposition 2.** *Curves $4 - 22$ of table A.1 are Serre curves.*

*Proof.* The Antwerp tables [1] give the conductor $N_E$ for each of these elliptic curves. One can verify that the conductor for each of these curves is square-free. Recall from Theorem 1 that these curves are semistable. Then we can apply Theorem 2 to prove that an elliptic curve $E$ has no exceptional primes greater than or equal to 11. Therefore, we need only compute the sizes of $\mathrm{GL}_2\mathbb{Z}/N\mathbb{Z}$ and $\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q})$, for $N = 2, 3, 5, 7, 8, 9$. □

# 5 The Serre Subgroup $H_{M_W}$

In this section, we give a more explicit characterization of the Serre subgroup $H_{M_W}$. Serre [9] has shown that for each elliptic curve $E$, there is an index two subgroup $H_E \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ so that $\phi_E(G_{\mathbb{Q}}) \subseteq H_E$. The image of the projection of $H_E$ onto $\mathrm{GL}_2(\mathbb{Z}/M_W\mathbb{Z})$ is a subgroup of $H_{M_W}$, while the image of the projection $\pi_N(H_E)$ onto $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is the entire group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for $(M_W, N) = 1$.

As a result, we need to characterize the subgroup $H_{M_W}$ in order to understand the $\phi_{N,E}$ map.

To describe $H_{M_W}$, we must first recall the definition of the Kronecker symbol, a generalization of the Legendre symbol.

Let $p$ be an odd prime and $a$ an integer. The Legendre symbol is defined by:

$$\left(\frac{a}{p}\right) := \begin{cases} -1, & \text{if } x^2 \equiv a \pmod{p} \text{ has no solutions} \\ 0, & \text{if } a \equiv 0 \pmod{p} \\ 1, & \text{if } x^2 \equiv a \pmod{p} \text{ has two solutions.} \end{cases}$$

The Kronecker symbol is an extension of the preceeding definition, where we write $\left(\frac{a}{b}\right)$ for every $a, b \in \mathbb{Z}$ as follows,

(i) If $b = 0$, then

$$\left(\frac{a}{0}\right) := \begin{cases} 1, & \text{if } a = \pm 1 \\ 0, & \text{otherwise.} \end{cases}$$

(ii) For $b \neq 0$, write $b = up_1 \cdots p_k$, where $p_i$ is prime and not necessarily distinct and $u \in \{\pm 1\}$. Then the Kronecker symbol is defined as

$$\left(\frac{a}{b}\right) = \left(\frac{a}{u}\right) \prod \left(\frac{a}{p}\right),$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol defined above for $p > 2$, and define

$$\left(\frac{a}{2}\right) = \begin{cases} 0, & \text{if } a \text{ is even} \\ (-1)^{\left(a^2-1\right)/8}, & \text{if } a \text{ is odd} \end{cases}$$

and

$$\left(\frac{a}{-1}\right) = \begin{cases} 1, & \text{if } a \geq 0 \\ -1, & \text{if } a < 0. \end{cases}$$

From Jones' paper [5, p. 13], we see that there exists a map

$$\epsilon : \mathrm{GL}_2(\mathbb{Z}/2m\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \xrightarrow{\sim} S_3 \xrightarrow{\mathrm{sgn}} \{\pm 1\},$$

where $S_3$ is the group of permutations on 3 letters and sgn is the signature character mapping even permutations to 1 and odd permutations to -1.

For an elliptic curve $E$, Jones defines the subgroup

$$H_{M_W} := \ker\left(\left(\frac{W}{\det(\cdot)}\right)\epsilon(\cdot)\right) \subset \mathrm{GL}_2(\mathbb{Z}/M_W\mathbb{Z}), \tag{4}$$

where $W = \Delta_{sf}(E)$ is the square-free part of the discriminant of an elliptic curve $E$ and $M_W$ is the Serre number of $E$, as defined in Section 3 [5, p. 13]. $H_{M_W}$ is known as the "Serre subgroup of $E$."

# 6 Computing the Rational Constant

Recall the constant

$$C_{E,r} = \frac{2}{\pi} \cdot \frac{m_E \cdot \#(\phi_{m_E,E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))_r)}{\#(\phi_{m_E,E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})))} \prod_{\substack{p \nmid m_E \\ p \nmid r}} \frac{p(p^2-p-1)}{(p+1)(p-1)^2} \prod_{\substack{p \nmid m_E \\ p \mid r}} \frac{p^2}{p^2-1}. \tag{5}$$

For the case $r = 0$, we break $C_{E,0}$ into two parts:
an infinite product:

$$C_0 = \prod_p \left( \frac{p^2}{p^2-1} \right), \tag{6}$$

and a finite product:

$$C = m_e \cdot \prod_{p \mid m_E} \left( \frac{p^2-1}{p^2} \right) \cdot \frac{\#(\phi_{m_E,E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))_0)}{\#(\phi_{m_E,E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})))}. \tag{7}$$

We see that

$$C_0 = \prod_p \left( \frac{p^2}{p^2-1} \right) = \prod_p \left( \frac{1}{1-\frac{1}{p^2}} \right) = \zeta(2) = \frac{\pi^2}{6}.$$

So, when $r = 0$, $C_{E,r}$ reduces to

$$C_{E,r} = \frac{\pi^2}{6} \cdot C.$$

When $r \neq 0$, we break $C_{E,r}$ into three parts. Define the products $C_1, C_2$, and $C_3$ by

$$C_1 = \prod_p \frac{p(p^2-p-1)}{(p^2-1)(p-1)}, \tag{8}$$

$$C_2 = \frac{2}{\pi} \cdot m_E \prod_{p \mid m_E} \frac{(p+1)(p-1)^2}{p(p^2-p-1)} \prod_{\substack{p \nmid m_E \\ p \mid r}} \frac{\left(\frac{p^2}{p^2-1}\right)}{\left(\frac{p(p^2-p-1)}{(p+1)(p-1)^2}\right)}, \tag{9}$$

$$C_3 = \frac{\#(\phi_{m_E,E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))_r)}{\#(\phi_{m_E,E}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})))}. \tag{10}$$

Observe that $C_{E,r} = C_1 \cdot C_2 \cdot C_3$.

One can see that Serre curves simplify the computation of $C_3$ because counting the elements in $\phi_{m_E,E}(G_{\mathbb{Q}})$ is equivalent to counting the elements in $H_{M_W}$. Recall the definition of $H_{M_W}$ from equation 4. We can verify that $H_{M_W}$ is the kernel of a homomorphism, so it forms a normal subgroup of $\mathrm{GL}_2(\mathbb{Z}/M_W\mathbb{Z})$. When we mod out $\mathrm{GL}_2(\mathbb{Z}/M_W\mathbb{Z})$ by $H_{M_W}$, we obtain a group of order 2. This implies that that $H_{M_W}$ is one-half the size of $\mathrm{GL}_2(\mathbb{Z}/M_W\mathbb{Z})$. Therefore,

$$H_{M_W} = \frac{1}{2}\prod_{p|M_W}((p^2-1)(p-1)p^{4(\mathrm{ord}_{M_W}(p)-1)}). \tag{11}$$

# 7 Computing the Number of Trace $r$ Elements in $H_{M_W}$

In this section, we discuss the computation of the number of trace $r$ elements in $H_{M_W}$.

In order to calculate the rational factor in the constant, we need the cardinality of the set of trace $r$ elements in the Serre subgroup. We can find this for any $r$ using the followng procedure.

Recall that $W$ is equal to the square-free discriminant of the curve $\Delta_{sf}$. Consider $W$ as a product of distinct primes $p_i$:

$$W = \pm p_1 \dots p_k$$

For the square-free dicriminant $W$, we recall that the Serre number $M_W$ is equal to either $4|W|$ or $2|W|$, depending on $W$'s reduction modulo 4.

Our notation is such that the group $E_q$ is a subgroup of $\prod\limits_{p \text{ prime}} \mathrm{GL}_2\mathbb{Z}_p$ such that $E_q$ is the kernel of the map that takes an element from $\prod\limits_{p \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_p)$ to the set $\{\pm 1\}$ by a composition of the projection homomorphism and the Kronecker symbol.

$$\prod_{p \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_p) \xrightarrow{\pi_q} \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}) \xrightarrow{\left(\frac{\det(\cdot)}{W}\right)} \{\pm 1\}$$

We can think of $E_q$ as the subgroup of ‘even’ elements of $\prod\limits_{p \text{ prime}} \mathrm{GL}_2\mathbb{Z}_p$ and the coset $O_q = -E_q$ as the set of ‘odd’ elements. We define the group $H_E$ as the group whose projection onto $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ yields the image of $\phi_{N,E}$,

$$H_E = \begin{cases} [(E_2 \times E_q) \cup (O_2 \times O_q)] \times \prod_{\ell \nmid 2q} \mathrm{GL}_2(\mathbb{Z}_\ell), & M_W = 2|W| \\ [(E_4 \times E_q) \cup (O_4 \times O_q)] \times \prod_{\ell \nmid 4q} \mathrm{GL}_2(\mathbb{Z}_\ell), & M_W = 4|W|, \end{cases}$$

where $q = |W|$. For a Serre curve, we notice that the projection of $H_E$ onto $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ gives the image of $\phi_{E,N}$.

When we project $H_E$ from a direct product of $\mathrm{GL}_2(\mathbb{Z}_p)$ into $\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$, we define the subgroup $E(q)$ to be the image of this projection from $E_q$. For a prime $p = q$ we can see that this subgroup is equal to the kernel of the homomorphism

$$E(p) = \ker\left(\left(\frac{\det(\cdot)}{p}\right)\right)$$

and the set $O(p)$ is its respective coset. There are two special cases of the subgroup for which we must consider. First, $E(2)$ is the kernel of the composite map that takes $\mathrm{GL}_2(\mathbb{Z}/2q\mathbb{Z})$ to $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$ which is then mapped to $\{\pm 1\}$ by the sign of the permutation

$$\epsilon : \mathrm{GL}_2(\mathbb{Z}/2q\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow \{\pm 1\}.$$

and the subgroup $O(2)$ is its respective coset. Second, $E(4)$ is the kernel of the homomorphism

$$E(4) = \ker\left(\left(\frac{-1}{\det(\cdot)}\right)\epsilon(\cdot)\right)$$

and the subgroup $O(4)$ is its respective coset.

We generalize Lang and Trotter's Serre number to the one defined by Jones and we can show that Lang and Trotter's characterization of the Serre subgroup is equivalent to Jones' description of $H_{M_W}$ [6] [5], i.e.

$$H_{M_W} = \ker\left(\left(\frac{W}{\det(\cdot)}\right)\epsilon(\cdot)\right) = \begin{cases} [(E(2) \times E(q)) \cup (O(2) \times O(q))], & M_W = 2|W| \\ [(E(4) \times E(q)) \cup (O(4) \times O(q))], & M_W = 4|W| \end{cases}.$$

*Proof.*
Case 1: For $W \equiv 1 \pmod 4$
Since we are working in $\mathrm{GL}_2(\mathbb{Z}/M_W\mathbb{Z})$, we can always that the determinant of its elements is positive by reducing $\pmod{M_W}$. Using the properties of the Kronecker symbol we know that for $W \equiv 1 \pmod 4$ the following properties hold:

$$\left(\frac{W}{\det(\cdot)}\right) = \left(\frac{\det(\cdot)}{W}\right), \quad \left(\frac{\det(\cdot)}{W}\right) = \left(\frac{\det(\cdot)}{|W|}\right).$$

Jones defines the Serre subgroup $H_{M_W}$ as the kernel of the following homomorphism [5],

$$H_{M_W} = \ker\left(\left(\frac{W}{\det(\cdot)}\right)\epsilon(\cdot)\right).$$

Notice that the preceeding identity implies that

$$H_{M_W} = \ker\left(\left(\frac{\det(\cdot)}{W}\right)\epsilon(\cdot)\right).$$

Observe that Kronecker symbol can be broken up into a product of Legendre symbols,

$$\left(\frac{\det(\cdot)}{W}\right) = \prod_{p|W}\left(\frac{\det(\cdot)}{p}\right).$$

We now provide a proof by induction on the prime factors of $W$.
For $W = \pm p$,

$$H_{M_W} = \ker\left(\left(\frac{\det(\cdot)}{p}\right)\epsilon(\cdot)\right)$$

This implies that either $\left(\frac{\det(\cdot)}{p}\right) = 1$ and $\epsilon(\cdot) = 1$, or $\left(\frac{\det(\cdot)}{p}\right) = -1$ and $\epsilon(\cdot) = -1$.
Recall that $E(2)$ is the kernel of $\epsilon(\cdot)$ and $E(p)$ is the kernel of $\left(\frac{\det(\cdot)}{p}\right)$, and the sets $O(2)$ and $O(p)$ to be the respective cosets. We can express the Serre subgroup as the union of direct products [6],

$$H_{M_W} = (E(2) \times E(p)) \cup (O(2) \times O(p)).$$

Similarly, the coset of $H_{M_W}$ is representable as

$$-H_{M_W} = (E(2) \times O(p)) \cup (O(2) \times E(p)).$$

Assume that this is possible for $W'$. We now want to show this for $W = pW'$.

$$H_{M_W} = \ker\left(\left(\frac{\det(\cdot)}{W}\right)\epsilon(\cdot)\right)$$

$$\left(\frac{\det(\cdot)}{W}\right) = \left(\frac{\det(\cdot)}{p}\right)\left(\frac{\det(\cdot)}{W'}\right)$$

This implies that either $\left(\frac{\det(\cdot)}{p}\right) = 1$ and $\left(\frac{\det(\cdot)}{W'}\right)\epsilon(\cdot) = 1$, or $\left(\frac{\det(\cdot)}{p}\right) = -1$ and $\left(\frac{\det(\cdot)}{W'}\right)\epsilon(\cdot) = -1$.
Observe that $E_{W'} = H_{M_{W'}}$ and $O_{W'} = -H_{M_{W'}}$ and that $(p, W') = 1$, which implies that $H_{M_W}$ has the form

$$H_{M_W} = (E(p) \times E(W')) \cup (O(p) \times O(W')).$$

The case for $W \equiv 1 \pmod 4$ is proved by induction.

Case 2: For $W \not\equiv 1 \pmod 4$
We cannot use the same properties as for $W \equiv 1 \pmod 4$, but we can use the following properties:

$$\left(\frac{W}{\det(\cdot)}\right) = \left(\frac{-1}{\det(\cdot)}\right)\left(\frac{\det(\cdot)}{W}\right), \qquad \left(\frac{\det(\cdot)}{W}\right) = \left(\frac{\det(\cdot)}{|W|}\right).$$

Using the preceeding identity, we obtain

$$H_{M_W} = \ker\left(\left(\frac{-1}{\det(\cdot)}\right)\left(\frac{\det(\cdot)}{W}\right)\epsilon(\cdot)\right).$$

Again we can break up the Kronecker symbol into a product of Legendre symbols,

$$\left(\frac{\det(\cdot)}{W}\right) = \prod_{p|W}\left(\frac{\det(\cdot)}{p}\right).$$

We now provide a proof by induction on the prime factors of $W$.
For $W = \pm p$,

$$H_{M_W} = \ker\left(\left(\frac{-1}{\det(\cdot)}\right)\left(\frac{\det(\cdot)}{p}\right)\epsilon(\cdot)\right)$$

This implies that either $\left(\frac{\det(\cdot)}{p}\right) = 1$ and $\left(\frac{-1}{\det(\cdot)}\right)\epsilon(\cdot) = 1$, or $\left(\frac{\det(\cdot)}{p}\right) = -1$ and $\left(\frac{-1}{\det(\cdot)}\right)\epsilon(\cdot) = -1$.

Recall that the kernel of $\left(\frac{-1}{\det(\cdot)}\right)\epsilon(\cdot)$ is the subgroup $E(4)$, and we again define $E(p)$ to be the kernel of $\left(\frac{\det(\cdot)}{p}\right)$, and the sets $O(4)$ and $O(p)$ to be the respective cosets. We can express the Serre subgroup as the union of direct products [6],

$$H_{M_W} = (E(4) \times E(p)) \cup (O(4) \times O(p)).$$

Similarly, the coset of $H_{M_W}$ is representable as

$$-H_{M_W} = (E(4) \times O(p)) \cup (O(4) \times E(p)).$$

Again, we assume that this is possible for $W'$. We now want to show this for $W = pW'$.

$$H_{M_W} = \ker\left(\left(\frac{\det(\cdot)}{W}\right)\left(\frac{-1}{\det(\cdot)}\right)\epsilon(\cdot)\right)$$
$$\left(\frac{\det(\cdot)}{W}\right) = \left(\frac{\det(\cdot)}{p}\right)\left(\frac{\det(\cdot)}{W'}\right)$$

This implies that either $\left(\frac{\det(\cdot)}{p}\right) = 1$ and $\left(\frac{\det(\cdot)}{W'}\right)\left(\frac{-1}{\det(\cdot)}\right)\epsilon(\cdot) = 1$, or $\left(\frac{\det(\cdot)}{p}\right) = -1$ and $\left(\frac{\det(\cdot)}{W'}\right)\left(\frac{-1}{\det(\cdot)}\right)\epsilon(\cdot) = -1$.

Observe that $E(W') = H_{M_{W'}}$ and $O(W') = -H_{M_{W'}}$ and that $(p, W') = 1$, which implies that $H_{M_W}$ has the form

$$H_{M_W} = (E(p) \times E(W')) \cup (O(p) \times O(W')).$$

Hence, the case for $W \not\equiv 1 \pmod 4$ is proved by induction.

□

We introduce the notation $(E_q)_r$, which means the subset of $E_q$ of elements of trace $r$. Similarly, we define $E(q)_r$.

Using the Chinese remainder theorem, we see that the following identities hold for $(s,t) = 1$:

$$(E_{st})_r = ((E_s)_r \times (E_t)_r) \cup ((O_s)_r \times (O_t)_r)$$
$$(O_{st})_r = ((E_s)_r \times (O_t)_r) \cup ((O_s)_r \times (E_t)_r)$$
$$E(st)_r = (E(s)_r \times E(t)_r) \cup (O(s)_r \times O(t)_r)$$
$$O(st)_r = (E(s)_r \times O(t)_r) \cup (O(s)_r \times E(t)_r)$$

We can see from these identites that the Serre subgroup can be expressed as union of direct products of subgroups of even $E(p)$ and odd $O(p)$ trace $r$ elements.

The cardinality of set of trace $r$ elements in the Serre subgroup can then be expressed as

$$|(H_{M_W})_r| = \begin{cases} |E(2)_r||E(q)_r| + |O(2)_r||O(q)_r|, & M = 2|W| \\ |E(4)_r||E(q)_r| + |O(4)_r||O(q)_r|, & M = 4|W| \end{cases}.$$

Observe that each $|E(q)_r|$ and $|O(q)_r|$ can be broken into a sum of products of its prime counterparts $|E(p)_r|$ and $|O(p)_r|$ for each $p|q$ by the previous identities.
The values of $|E(p)_r|$ and $|O(p)_r|$ for each prime $p$ and trace $r$ are given by the following table [6]:

| | $r \equiv 0 \mod p$ | $r \not\equiv 0 \mod p$ |
|---|---|---|
| $\left(\frac{-1}{p}\right) W > 0$ | $\lvert E(p)_r\rvert = \left(\frac{1}{2}\right) p(p^2 - 2p + 1)$<br>$\lvert O(p)_r\rvert = \left(\frac{1}{2}\right) p(p^2 - 1)$ | $\lvert E(p)_r\rvert = \left(\frac{1}{2}\right) p(p^2 - p)$<br>$\lvert O(p)_r\rvert = \left(\frac{1}{2}\right) p(p^2 - p - 2)$ |
| $\left(\frac{-1}{p}\right) W < 0$ | $\lvert E(p)_r\rvert = \left(\frac{1}{2}\right) p(p^2 - 1)$<br>$\lvert O(p)_r\rvert = \left(\frac{1}{2}\right) p(p^2 - 2p + 1)$ | $\lvert E(p)_r\rvert = \left(\frac{1}{2}\right) p(p^2 - p - 2)$<br>$\lvert O(p)_r\rvert = \left(\frac{1}{2}\right) p(p^2 - p)$ |

For the values of $|E(4)_r|$ and $|O(4)_r|$, we refer to the following table:

| | $r \equiv 0 \mod 4$ | $r \equiv 1 \mod 4$ | $r \equiv 2 \mod 4$ | $r \equiv 3 \mod 4$ |
|---|---|---|---|---|
| $\lvert E(4)_r\rvert$ | 12 | 8 | 20 | 8 |
| $\lvert O(4)_r\rvert$ | 20 | 8 | 12 | 8 |

The values in this table were found by inspection of the 96 elements of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$.

For the values of $|E(2)_r|$ and $|O(2)_r|$, we refer to the following table:

| | $r \equiv 0 \mod 2$ | $r \equiv 1 \mod 2$ |
|---|---|---|
| $\lvert E(2)_r\rvert$ | 1 | 2 |
| $\lvert O(2)_r\rvert$ | 3 | 0 |

The values in this table were found by inspection of the 6 elements of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$.
For a demonstation on how we use these tables to calculate the values of the trace $r$ elements in the Serre subgroup, consider the following example:

**Example 1.**

$$W = 15 = (5) \cdot (3)$$

$$M_W = 4|W| = 60$$

*We now use the table and the identities to construct the number of elements in $H_{M_W}$ with trace 0:*

$$\begin{aligned}
|E(5)_0| &= (1/2)5(5^2 - 2(5) + 1) \\
|O(5)_0| &= (1/2)5(5^2 - 1) \\
|E(3)_0| &= (1/2)3(3^2 - 1) \\
|O(3)_0| &= (1/2)3(3^2 - 2(3) + 1) \\
|E(4)_0| &= 20 \\
|O(4)_0| &= 12
\end{aligned}$$

$$|(H_{M_W})_0| = |E(4)_0|(|E(3)_0||E(5)_0|+|O(3)_0||O(5)_0|)+|O(4)_0|(|E(3)_0||O(5)_0|+|O(3)_0||E(5)_0|)$$

*Substituting in the correct values for* 3 *and* 5*, we obtain:*

$$|(H_{M_W})_0| = 29280$$

For example, when we consider the case where $W = \pm p$, where $p$ is an odd prime, we write out the explicit values of the trace $r$ elements as functions of $p$:

| For $W \equiv 1 \pmod 4$ | | | |
|---|---|---|---|
| | | $2 \mid r$ | $2 \nmid r$ |
| $W > 0$ | $p \mid r$ | $p(2p^2 - 3p + 1)$ | $p(p^2 - p)$ |
| | $p \nmid r$ | $p(2p^2 - 2p - 1)$ | $p(p^2 - p - 2)$ |
| $W < 0$ | $p \mid r$ | $p(2p^2 - p - 1)$ | $p(p^2 - 2p + 1)$ |
| | $p \nmid r$ | $p(2p^2 - 2p - 3)$ | $p(p^2 - p)$ |

| For $W \equiv 3 \pmod 4$ | | | | |
|---|---|---|---|---|
| | | $r \equiv 0 \mod 4$ | $r \equiv 2 \mod 4$ | $2 \nmid r$ |
| $W > 0$ | $p \mid r$ | $4p(4p^2 - 3p - 1)$ | $4p(4p^2 - 5p + 1)$ | $4p(2p^2 - 2p)$ |
| | $p \nmid r$ | $4p(4p^2 - 4p - 5)$ | $4p(4p^2 - 4p - 3)$ | $4p(2p^2 - 2p - 2)$ |
| $W < 0$ | $p \mid r$ | $4p(4p^2 - 5p + 1)$ | $4p(4p^2 - 3p - 1)$ | $4p(2p^2 - 2p)$ |
| | $p \nmid r$ | $4p(4p^2 - 4p - 3)$ | $4p(4p^2 - 4p - 5)$ | $4p(2p^2 - 2p - 2)$ |

# 8 Calculation of the Irrational Constant

The Lang-Trotter conjecture deals with an infinite product:

$$C_1 = \prod_p \frac{p^3 - p^2 - p}{(p^2-1)(p-1)}$$

To evaluate this product, we must consider a more general form $C_s$ and take limits as $s \longrightarrow 1^+$ at the appropriate time.

$$C_s = \prod_p \frac{p^{3s} - p^{2s} - p^s}{(p^{2s}-1)(p^s-1)}$$

We recall that the Riemann zeta function has the Euler product expansion $\zeta(s) = \prod_p (1 - 1/p^s)^{-1}$. We factor out a $\zeta(s)\zeta(2s)$ and rewrite to obtain:

$$C_s = \zeta(s)\zeta(2s)\prod_p p^{-2s}(p^{2s} - p^s + 1) = \zeta(s)\zeta(2s)\prod_p p^{-2s}(p^s - \alpha)(p^s - \bar{\alpha}) = \prod_p \left(1 - \frac{\alpha}{p^s}\right)\left(1 - \frac{\bar{\alpha}}{p^s}\right)$$

where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\bar{\alpha} = \frac{1-\sqrt{5}}{2}$.
This implies that we can now focus on the product

$$S(s) = \prod_{p \text{ prime}} \left(1 - \frac{\alpha}{p^s}\right)^{-1}$$

for $\alpha \in \mathbb{C}$. Multiplying by $\frac{\zeta(s)^\alpha}{\zeta(s)^\alpha}$, we obtain the identity:

$$S(s) = \zeta(s)^\alpha \prod_p \frac{(1 - \frac{1}{p^s})^\alpha}{(1 - \frac{\alpha}{p^s})}$$

$$\begin{aligned} S(s) &= \zeta(s)^\alpha \exp \sum_p \left(\alpha \log\left(1 - \frac{1}{p^s}\right) - \log\left(1 - \frac{\alpha}{p^s}\right)\right) \\ &= \zeta(s)^\alpha \exp\left(\sum_p \sum_{k\geq 2} \frac{\alpha^k}{kp^{sk}} - \frac{\alpha}{kp^{sk}}\right) \end{aligned}$$

(the term in $k = 1$ vanishing). Thus, the inner sum is absolutely convergent even for $s = 1$.
Since $\alpha + \bar{\alpha} = 1$ it follows that

$$\begin{aligned} \lim_{s\to 1^+} \frac{S(s)\bar{S}(s)}{\zeta(s)} &= \exp\left(\sum_p \sum_{k\geq 2} \frac{\alpha^k - \alpha}{kp^k}\right) \exp\left(\sum_p \sum_{k\geq 2} \frac{\bar{\alpha}^k - \bar{\alpha}}{kp^k}\right) \\ &= \exp\left(\sum_{k\geq 2} \frac{\alpha^k - \alpha}{k} \sum_p \frac{1}{p^k}\right) \exp\left(\sum_{k\geq 2} \frac{\bar{\alpha}^k - \bar{\alpha}}{k} \sum_p \frac{1}{p^k}\right) \end{aligned}$$

For a fixed $k$, we can now compute $\sum_p 1/p^k$ to high accuracy via the identity

$$\sum_p \frac{1}{p^k} = \sum_l \left(\frac{\mu(l)}{l}\right) \log(\zeta(kl))$$

For large $k$,

$$\sum_p \frac{1}{p^k} \simeq \frac{1}{2^k}$$

# 9 Error Analysis

$$g_\alpha = \sum_{k\geq 2}^{\infty} \frac{\alpha^k - \alpha}{k} \sum_{n\geq 1}^{\infty} \left(\frac{\mu(n)}{n}\right) \log \zeta(kn)$$

We will first find the truncation error of the series when the series is evaluated for terms up to $K-1$. To do this, consider the following:

$$\{\text{Error}\} = \sum_{k\geq K}^{\infty} \frac{\alpha^k - \alpha}{k} \sum_{n\geq 1}^{\infty} \left(\frac{\mu(n)}{n}\right) \log\zeta(kn)$$

For large $K$,

$$\sum_{n\geq 1}^{\infty} \left(\frac{\mu(n)}{n}\right) \log\zeta(kn) \sim 2^{-k}$$

Using this identity, we can say that:

$$\{\text{Error}\} \sim \sum_{k\geq K}^{\infty} \frac{\alpha^k - \alpha}{k} 2^{-k}$$

This series can be split into two sums:

$$\{\text{Error}\} \sim \sum_{k\geq K}^{\infty} \left(\frac{\alpha}{2}\right)^k \frac{1}{k} - \alpha \sum_{k\geq K}^{\infty} \left(\frac{1}{2}\right)^k \frac{1}{k}$$

Recall the Taylor series for $-\log(1-x)$:

$$-\log(1-x) = \sum_{i=1}^{\infty} \frac{x^k}{k}$$

Since these two series can be identified as Taylor series, we can use the integral form for the remainder of a Talyor polynomial to find a bound on the error:

$$R_n = \int_0^{\alpha/2} \frac{f^{(K+1)}(t)}{K!} \left(\frac{\alpha}{2} - t\right)^K dt$$

We can find the $K+1$-th derivative and substitute it into the integral:

$$R_n = \int_0^{\alpha/2} (1-t)^{-K-1} \left(\frac{\alpha}{2} - t\right)^K dt$$

This function is concave up on the interval, so we can approximate the integral with a trapezoid. For the integrand $g$:

$$R_n \leq \frac{g(0) + g(\alpha/2)}{2} \left(\frac{\alpha}{2}\right) = \frac{(\alpha/2)^K + 0}{2} \left(\frac{\alpha}{2}\right) = \frac{1}{2} \left(\frac{\alpha}{2}\right)^{K+1}$$

Similarly, for the other series found in the error term:

$$R_n' \leq \left(\frac{1}{2}\right)^{K+2}$$

From these bounds on the truncated terms in the Taylor polynomial, we can use these to find a bound on the error of the truncation.

$$\{\text{Error}\} \sim \sum_{k\geq K}^{\infty} \left(\frac{\alpha}{2}\right)^k \frac{1}{k} - \alpha \sum_{k\geq K}^{\infty} \left(\frac{1}{2}\right)^k \frac{1}{k} \leq \frac{1}{2}\left(\frac{\alpha}{2}\right)^{K+1} - \frac{\alpha}{2}\left(\frac{1}{2}\right)^{K+1}$$

Therefore, for a partial sum of $K$ terms, the truncation error is bounded by:

$$\{\text{Error}\}_K \leq \frac{1}{2}\left(\frac{\alpha}{2}\right)^{K+1} - \frac{\alpha}{2}\left(\frac{1}{2}\right)^{K+1}$$

The round-off error can be measured by observing that we lose one significant digit per computated addition, and the constant was calculated using about $\log_2(K)$ additions.
We observe that for $K = 2^{14}$:

$$\frac{1}{2}\left(\frac{\alpha}{2}\right)^{2^{14}+1} - \frac{\alpha}{2}\left(\frac{1}{2}\right)^{2^{14}+1} \sim 10^{-1508}$$

which implies that the partial sum should be accurate for about 1508 digits. Combined with the round-off error:

$$1508 - \log_2(2^{14}) = 1494$$

The value obtained for $g_\alpha$ calculated using this method for $K = 2^{14}$ is accurate to about 1494 digits. $g_{\bar{\alpha}}$ has the same number of significant digits. This error propagates to the constant $C_1$ as follows:

$$e^{(g_\alpha+\epsilon)} \simeq e^{g_\alpha}(1+\epsilon)$$

$$e^{g_\alpha}(1+\epsilon_\alpha)e^{g_{\bar{\alpha}}}(1+\epsilon_{\bar{\alpha}}) \simeq e^{g_\alpha}e^{g_{\bar{\alpha}}}(1+\epsilon_\alpha+\epsilon_{\bar{\alpha}})$$

since $\epsilon_\alpha\epsilon_{\bar{\alpha}}$ is insignificant.

$$C_1 + \epsilon_{C_1} = \frac{\zeta(2)}{e^{g_\alpha}e^{g_{\bar{\alpha}}}(1+\epsilon_\alpha+\epsilon_{\bar{\alpha}})} \simeq \frac{\zeta(2)}{e^{g_\alpha}e^{g_{\bar{\alpha}}}}(1-\epsilon_\alpha-\epsilon_{\bar{\alpha}})$$

since $(1+\epsilon)^{-1} \simeq (1-\epsilon)$ for small $\epsilon$. Therefore, the error in the constant $C_1$ is on the order of:

$$\{\text{Error}\}_{C_1} \sim C_1(\epsilon_\alpha+\epsilon_{\bar{\alpha}})$$

The value of $\epsilon_\alpha+\epsilon_{\bar{\alpha}}$ is about $2\times 10^{-1494}$.
We have computed $C_1 = 0.61513265731817180255072...$, so the error of the constant is: $\sim 1.230\times 10^{-1494} < 10^{-1493}$ This implies the evaluation of the the constant $C_1$ is accurate to at least 1493 digits.

# 10 Calculation of the Error Terms $a_q(E)$

Recall, the error term

$$a_q(E) = q + 1 - \#E(\mathbb{F}).$$

After calculating the constants for known Serre curves, we calculate $a_q(E)$ for each curve to observe the asymptotic behavior conjectured by Lang and Trotter. For each calculation, we vary $r$ from -100 to 100 and record

$$\frac{\#\{q < X : a_q(E) = r\}}{\frac{\sqrt{X}}{\log X}}.$$

We check to see if the data appear to be converging to $C_{E,r}$ at $X = 179,424,673$, $X = 573,259,392$, and $X = 1,086,218,491$.
To compute the terms, we use the Pari/GP computer algebra system [10], which has a specific function for such computations. Depending on the size of $q$, this function implements either a sum of Legendre symbols (recommended $q < 457$) or the Mestre-Shanks algorithm (useful for larger $q$).

# References

[1] B. J. Birch and W. Kuyk, editors. *Modular functions of one variable. IV.* Lecture Notes in Mathematics, Vol. 476. Springer-Verlag, Berlin, 1975.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] J. E. Cremona. *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge, second edition, 1997.

[4] Kevin James. Average Frobenius distributions for elliptic curves with 3-torsion. *J. Number Theory*, 109(2):278–298, 2004.

[5] Nathan Jones. Almost all elliptic curves are Serre curves. To appear in *Trans. Amer. Math. Soc.*. Preprint available on-line as arXiv:math/0611096v1 [math.NT].

[6] Serge Lang and Hale Trotter. *Frobenius distributions in* $\mathrm{GL}_2$*-extensions.* Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in $\mathrm{GL}_2$-extensions of the rational numbers.

[7] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[8] Amadeu Reverter and Núria Vila. Images of mod $p$ Galois representations associated to elliptic curves. *Canad. Math. Bull.*, 44(3):313–322, 2001.

[9] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[10] The PARI Group, Bordeaux. *PARI/GP, version* `2.1.7`, 2005. available from `http://pari.math.u-bordeaux.fr/`.

# A Appendix

## A.1 Table of Serre Curves

In the following table, each curve is in the form

$$E : y^2 = x^3 + Ax + B$$

and we use the following notation:

- $\Delta_{sf}$ is the square free part of the discriminant
- $M_{\Delta_{sf}}$ is the Serre number as defined by Jones [5, p. 13]
- $N$ is the conductor of $E$

| $A$ | $B$ | $\Delta_{sf}$ | $M_{\Delta_{sf}}$ | $N$ |
|---:|---:|---:|---:|---:|
| 6 | -2 | -3 | 6 | 5184 |
| -4 | 4 | -11 | 22 | 16 |
| 32 | 212 | 35 | 140 | 140 |
| 32 | 16 | -11 | 22 | 77 |
| -16 | 16 | 37 | 74 | 37 |
| -1971 | 64206 | -593 | 2372 | 593 |
| -3024 | 70416 | -19 | 38 | 57 |
| -1539 | 33534 | -29 | 116 | 58 |
| -2619 | 54486 | -61 | 244 | 61 |
| -15984 | -778032 | -67 | 134 | 67 |
| -2619 | 47574 | 79 | 316 | 79 |
| 1269 | -10746 | -83 | 166 | 83 |
| 1296 | 11664 | -91 | 182 | 91 |
| -1323 | 28134 | -89 | 356 | 89 |
| -1728 | -15984 | 101 | 202 | 101 |
| -10611 | -421362 | -109 | 436 | 109 |
| -10395 | 31158 | -57 | 228 | 114 |
| 3213 | 1998 | -61 | 244 | 122 |
| 864 | -22896 | -123 | 246 | 123 |
| 864 | 23760 | -131 | 262 | 131 |
| -4563 | -121554 | -139 | 278 | 139 |
| -1728 | -7344 | 141 | 282 | 141 |

## A.2 Irrational Constant to 1497 digits

The following is the first 1497 digits of the irrational constant $C_1$:

.6151326573 1817180255 0725664929 1924616780 1694045261 2777657497
0417137754 9363232728 8665159438 7019482560 5683292134 4487523490
9443054903 2861278864 2253427305 7811388828 3278554499 8368417981
7773333532 5517905266 0096208354 5685190641 8746757760 1330439071
5958784234 7191508537 0461632051 4833584473 9834454169 1397668436
2554288109 6111873990 8932045465 9513426971 6408031796 4050480479
3069354324 2137846053 2405104623 7835141036 4216245597 5855110892
7369688274 0130080179 9177798856 1918105047 8419738048 6241890023
3543598671 8894134152 1595784508 3476232304 1554376423 3659562835
7683634224 3755876233 1110566365 3444037845 7993200373 0003108773
7539978354 3304848332 0269075097 1880853418 6553312086 8801927623
2962571989 9403602645 7732803456 2597037562 1316140512 8450158164
6456186163 5336741652 5484465777 6001963817 0231859609 7788784521
6087904638 8273252166 5143157813 3376502412 5390779805 2758122660
7251855404 5330883029 4632588162 8514307855 3051482611 0156025144
2837298559 0950600888 0758151177 0309664301 5722122532 4263865388
5929727109 5885416080 9617695293 8182645368 3308819512 3935743476
8240483500 0703029897 2435666442 7384733290 6310841559 5609990290
0611162667 7878846952 9911520184 9109349129 5727107847 6607579240
9335728804 5445811125 3179804023 5080615706 8540846101 1823134335
4566830845 1847518255 0374546226 3168345527 2016817554 8277372520
1584930757 2660033170 6579655667 9018235057 0829977915 5891114089
3931124171 3638605739 7019088093 4363418995 9076895211 2696524424
0999123168 2313342366 6087798970 4685007221 1769425869 0703975059
0891037261 1678494990 4673236254 7083824470 4047874762 154(5178)