An Algorithm for Calculating Central Values of a Certain Twisted L-Function

Author:
Jerrik Feliciano

Advisors:
Dr. Pavel Guerzhoy
Dr. Michelle Manes

April 18, 2014
Acknowledgements

There are many people who I would like to thank who have had a hand in this thesis. First, a special thanks to Dr. Manes who accepted to be my second advisor on such late notice. Secondly, I’d like to give a big mahalo to Dr. Guerzhoy who has gone far beyond what I would have expected from an advisor. After every mentoring session with Dr. Guerzhoy I left with a new sense of inspiration and drive. It had been a while since I had a desire to research math topics on my own. I was so inspired by the many different topics of mathematics that it almost hindered the writing process of my thesis. There were several times when I came to that "ah-ha!" moment while conversing with Dr. Guerzhoy, which left me wanting to explore more. Some meetings would go on for hours; sometimes we would just talk about the lives of mathematicians and even that added to my drive to do the research for this paper. I would also like to extend a warm thanks to Miss Sue Hasegawa for all her patience and assistance pertaining to my graduation process. Last, but certainly not least, I would like to thank my family, friends, and Ms. Naomi Castro, for all their support and especially for their encouragement to graduate. God knows I wanted to give up, but they wouldn’t let me, and for that I thank them.
Abstract

This paper is motivated by a question Diophantus had on congruent numbers, as well as an algorithm created by Don Zagier. We will try to create an algorithm similar to one that Zagier writes in his paper, "From Quadratic Functions to Modular Functions." The algorithm will be a different method of calculating $a(n)$'s from Tunnell's Theorem in, "A Classical Diophantine Problem and Modular Forms of Weight $3/2$."

CONTENTS

Acknowledgements 1
Abstract 2
1. Introduction 4
2. The Question Under Investigation and Generalities on Elliptic Curves 4
3. Modular Forms and Their $L$-Functions 6
4. Putting It All Together 8
5. The GP code to verify Conjecture 1 10
References 17
1. Introduction

In this paper some interesting topics related to congruent numbers and an elliptic curve will be mentioned. One such topic is the BSD conjecture. In 1965 Bryan Birch and Peter Swinnerton-Dryer presented a conjecture, known today as the Birch and Swinnerton-Dryer Conjecture or BSD Conjecture. It is an open problem in number theory and is one of the seven Millennium Prize Problems. The BSD Conjecture is an if and only if statement. It has only been proven in one direction, and has only been proven in both directions for very specific cases. This paper will explore a possible consequence of the BSD conjecture, if the conjecture were to ever be proven.

Elliptic curves is another topic that is the basis of many papers and books. The usefulness of elliptic curves is evident in the proof of Fermat’s Last Theorem, proven by Andrew Wiles.

These two aforementioned topics, along with a paper written by Don Zagier, brings us to our question under investigation.

2. The Question Under Investigation and Generalities on Elliptic Curves

Let $F$ be a field. We refer to an elliptic curve over $F$ as the set of pairs $(x, y) \in F$ which satisfies the equation

$$y^2 + a_1 xy + a_3 y = x^3 - a_2 x^2 - a_4 x - a_6,$$

where $a_i \in F$. A specific example of an elliptic curve, $E$, which we discuss in this paper, is the curve

$$y^2 = x^3 - x$$ (1)

which is considered as an elliptic curve over the field of rational numbers. As a generalization, we consider a family of elliptic curves enumerated by integers $D$ (also over rationals) $E_D$

$$y^2 = x^3 - D^2 x$$ (2)

The question that may arise is whether the elliptic curve has infinitely or finitely many rational points. In other words, are there infinitely or finitely many pairs of rational numbers $(x, y)$ that satisfies the equation of the elliptic curve? For
example, a tricky argument, that Fermat proves is that the elliptic curve \( E \) has only three rational points, namely, equation (1) has no rational solutions besides the obvious three \((0, 0)\) and \((\pm 1, 0)\). Similarly, equation (2) has three solutions \((0, 0)\) and \((\pm D, 0)\), however, (2) may have more rational solutions depending on \(D\). Furthermore, one can prove (cf. [1, Chapter 1, Proposition 17]) that equation (2) has infinitely many rational solutions \((x, y)\) if it has at least one besides the three aforementioned obvious solutions. The Birch and Swinnerton-Dyer conjecture predicts that equation (2) has infinitely many solutions if and only if the central value of the \(L\)-function associated with the elliptic curve \(E_D\) is zero. This conjecture is, in fact, stated for any elliptic curve defined over rationals. The \(L\)-function of an elliptic curve is, in general, a specific complex-analytic function which may be constructed out of the equation of the curve (cf. [1, Chapter 2]). Another way to construct this function is to make use of the celebrated result by Andrew Wiles. He proved that this \(L\)-function is always the \(L\)-function associated to a certain modular form of weight two. This fact was actually known for quite awhile in the specific case of elliptic curves \(E_D\), and the weight two modular forms in question may be constructed explicitly as we will recall in section 4. Also, Tunnell in [2] proved a celebrated result which we quote here in a slightly modified and simplified form.

**Theorem 1.** Let the integers \(a(n)\) be defined by

\[
H = \sum_{n=1}^{\infty} a(n)q^n = q \prod_{n=1}^{\infty} (1 - q^{8n})(1 - q^{16n}) \left(1 + 2 \sum_{n=1}^{\infty} q^{2n^2}\right).
\]

For an odd integer \(D\), if \(a(D) \neq 0\), then the elliptic curve \(E_D\) has only finitely many rational points.

Note that the statement of the Theorem 1 is conjecturally “if and only if”. The conjectural part of Theorem 1 depends on the Birch and Swinnerton - Dyer conjecture, which is only proven for the elliptic curves \(E_D\) in one direction. The proof of the theorem relies on the fact that, up to a non-zero factor, the squares \(a(D)^2\) equal to the central critical values of the \(L\)-function associated with \(E_D\).

The purpose of this paper is to provide a different algorithm to calculate quantities similar to \(a(n)\) in Tunnell’s theorem.
3. Modular Forms and Their $L$-Functions

Let $\mathbb{H}$ be the upper half of the complex plane, denoted as $\mathbb{H} = \{z \in \mathbb{C} : \text{Im}(z) > 0\}$.

**Definition 1.** The modular group, $SL_2(\mathbb{Z})$, is defined by

$$SL_2(\mathbb{Z}) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \}.$$  

**Definition 2.** A function, $f$, is referred to as a modular form on $SL_2(\mathbb{Z})$ of weight $k$ if:

1. $f$ is analytic in the upper half plane,
2. $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$, whenever $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$,
3. and the Fourier series of $f$ has the form,

$$f(z) = \sum_{n=0}^{\infty} c(n) e^{2\pi inz}.$$  

Also we will call a modular form a cusp form if $c(0) = 0$.

And we will use the standard notation

$$q = e^{2\pi iz}$$

throughout this text. This notation makes the Fourier series of a modular form a power series in $q$.

**Example 1.** In MM century Ramanujan observed that the series

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=0}^{\infty} \tau(n)q^n$$

is the Fourier expansion of a modular form of weight $k = 12$.

We will also need a certain Dirichlet character. We call an integer $D$ a discriminant if either $D \equiv 1 \mod 4$ or $D \equiv 0 \mod 4$. Define a function $\chi_D$ on integers
relatively prime to $D$ by

$$
\chi_D(n) = \begin{cases} 
1 & \text{if there exists an integer } x \in \mathbb{Z} \text{ such that } x^2 \equiv n \pmod{|D|} \\
-1 & \text{if for every integer } x \in \mathbb{Z} \text{ we have that } x^2 \not\equiv n \pmod{|D|}.
\end{cases}
$$

We also let $\chi_D(n) = 0$ if $\gcd(D, n) > 1$.

For a modular form of weight $k$,

$$
f = \sum_{n=0}^{\infty} c(n)q^n,
$$

and a Dirichlet character $\chi_D$, as defined above, we associate the following twisted $L$-function

$$
L(f, D, s) = \sum_{n=0}^{\infty} c(n)\chi_D(n)n^{-s}.
$$

We will regard $s$ as a complex variable. A growth estimate for the Fourier coefficients of a modular form $|c(n)| < Cn^{k-1}$, for some constant $C$, allows us to conclude that the series converges in the right half-plane $\Re(s) > k$. It is also known that this function can be analytically continued to a holomorphic function on the whole complex plane. We do not pursue this topic further since it provides no clue on the calculation of certain specific values of the function $L(f, D, k/2)$ which is our primary goal in this paper. Another method of calculating these values can be read in a paper by Zagier [3]. We will explain the method below.

Let $D > 0$ be a positive integer such that $D \equiv 1 \pmod{4}$, and $D$ is not a perfect square. For a rational number $x$ we consider the set $R_D(x)$ of all quadratic functions $Q = Q(X) = AX^2 + BX + C$ which satisfy the following conditions.

- The three quantities $A, B, C$ are integers.
- $A < 0$.
- $B^2 - 4AC = D$.
- $Q(x) > 0$

It is not difficult to prove that the set $R_D(x)$ is finite for every rational number $x$. Consider the sum

$$
\Phi_D(x) = \sum_{Q \in R_D(x)} Q(x)^5.
$$

A consequence of Zagier’s paper is as follows.
Theorem 2. Let $D > 0$ be a positive integer such that $D \equiv 1 \mod 4$, and $D$ is not a perfect square.

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

The function on rational numbers

$$\Psi_{\gamma, D}(x) = \Phi_D(x) - \Phi_D\left(\frac{ax + b}{cx + d}\right)$$

is identically zero if and only if the special value of $L$-function $L(\Delta, D, 6) = 0$.

It is important to our further discussion that $L(\Delta, D, 6)$ is exactly the central value, i.e.

$$6 = \frac{k}{2},$$

of the $L$-function associated to the cusp modular form $\Delta$ of weight $k = 12$. It is also important that the power of 5 in the definition of $\Phi(x)$, is introduced in Zagier’s paper [3] as

$$5 = \frac{k}{2} - 1.$$

4. PUTTING IT ALL TOGETHER

In Section 2, we recalled the Birch and Swinnerton-Dyer conjecture which reduces the question whether a rational elliptic curve has finitely or infinitely many rational points to the (zero or non-zero) value of the $L$-function associated with the elliptic curve. In Section 3, we discussed a method of the calculation of central values of $L$-function associated with a certain modular form (cusp form $\Delta$ of weight $k = 12$). These two subjects are far from being disjoint. A celebrated result of Wiles (formerly Shimura - Taniyama conjecture) states that “every rational elliptic curve is modular,” this statement can be reformulated to the following: The $L$-function of a rational elliptic curve coincides with the $L$-function of a certain weight 2 cusp modular form. This was actually well-known in the case of elliptic curves $E$ and $E_D$ that we discuss in this paper. We can and will be more specific below. The function on the upper half-plane

$$g = q \prod_{n=1}^{\infty} (1 - q^{4n})^2(1 - q^{8n})^2$$

is quite similar to $\Delta$. Although it is not a modular form in the sense of our definition in Section 2, it is quite close to it. Namely, it satisfies the modular transformation
law
\[ g^{(az + b)/(cz + d)} = (cz + d)^k g(z) \]
with the weight \( k = 2 \) for every \( \left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in SL_2(\mathbb{Z}) \) such that \( c \equiv 0 \mod 32 \). These matrices form a subgroup \( \Gamma_0(32) \subset SL_2(\mathbb{Z}) \), and \( g \) is referred to as a cusp modular form of weight 2 on \( \Gamma_0(32) \). In the case under consideration, Wile’s result may be rewritten as the equality of \( L \)-functions
\[ L(E_D,s) = L(g,D,s), \]
and our investigation comes down to investigating the central values \( L(g,D,1) \), which are quite similar to the values \( L(\Delta,D,6) \) discussed above (here ”central” corresponds to half of the weight).

Thus, now we will try to produce an analog of the procedure describe in Section 3. Specifically, for a rational number \( x \) and a positive integer \( D \equiv 1 \mod 4 \) we define \( R_{D,32}(x) \) as the set of all quadratic functions \( Q = Q(X) = AX^2 + BX + C \) which satisfy the following conditions.

- The three quantities \( A, B, \) and \( C \) are integers.
- \( A < 0. \)
- \( B^2 - 4AC = D. \)
- \( Q(x) > 0 \)
- \( A \equiv 0 \mod 32. \)

*Note that we added an extra condition \( A \equiv 0 \mod 32. \)

We now want to define the analog of the sums \( \Phi_D(x) \). Since the weight of our modular form \( g \) is two, the exponent which was one less than half of the weight becomes zero instead of 5, and the sum degenerates into a sum of ones:
\[ \Phi_{D,32}(x) = \sum_{Q \in R_{D,32}(x)} 1, \]
which is simply the number of elements in the set \( R_{D,32}(x) \). However, numerical experiments showed that this definition is not quite right. So, we will slightly modify \( \Phi_{D,32}(x) \). Note that for a quadratic form \( Q = AX^2 + BX + C \in R_{D,32}(x) \)
we have that \( B^2 - 4AC = D \equiv 1 \mod 4 \), and thus \( B \) is always odd. We let
\[
\omega(Q) = \begin{cases} 
1 & \text{if } Q = AX^2 + BX + C \text{ and } B \equiv 1 \mod 4 \\
-1 & \text{if } Q = AX^2 + BX + C \text{ and } B \not\equiv 1 \mod 4 
\end{cases}
\]
and define
\[
\Phi_{D,32}(x) = \sum_{Q \in \mathcal{R}_{D,32}(x)} \omega(Q).
\]

In order to define an analog of the function \( \Psi_{\gamma,D}(x) \), we will pick \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(32) \subseteq (\mathbb{Z}) \).

We can now formulate an analog of Theorem 2 as a conjecture which is the subject to our numerical verification.

**Conjecture 1.** Let \( D > 0 \) be a positive integer such that \( D \equiv 1 \mod 4 \), and \( D \) is not a perfect square.

Let \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(32) \). The function on rational numbers
\[
\Psi_{\gamma,D,32}(x) = \Phi_{D,32}(x) - \Phi_{D,32}\left(\frac{ax + b}{cx + d}\right)
\]
is identically zero if and only if the central special value of \( L \)-function \( L(g,D,1) = 0 \).

5. The GP code to verify Conjecture 1

In this section we describe a GP-code which implements our numerical experiments.

\[
\text{\texttt{ps}} \ 500 \\
\text{lim}=500; \\
\text{et}=q*\texttt{eta}(q^8)*\texttt{eta}(q^{16}); \\
\text{th2}= 1+2*\texttt{sum}(n=1, \text{lim}, \ q^{-2*2^n}); \\
\text{H}=0(q^{-\text{lim}})+\text{th2}+\text{et};
\]
The first 500 terms of the series from Theorem 1

\[ H = \sum_{n=1}^{\infty} a(n)q^n = q \prod_{n=1}^{\infty} (1 - q^{8n})(1 - q^{16n}) \left( 1 + 2 \sum_{n=1}^{\infty} q^{2n^2} \right). \]

is calculated here. In particular, we have that

\[ H = q + 2q^3 + q^9 - 2q^{11} - 4q^{17} - 2q^{19} - 3q^{25} + 4q^{33} - 4q^{35} + \ldots \]

N=32;

{ for(delta=2,500, 
  if((delta%4==1)&&!issquare(delta),
    print1(delta," ... ",polcoeff(H,delta));
  )
}

t=0;
x=t;

For every \( D \) (called “\( \text{delta} \)” in the code) satisfying the conditions of Conjecture 1 we are going to calculate \( \Psi_{\gamma,D,32}(0) \). We put \( x = 0 \) here quite arbitrarily. By the nature of our conjecture, almost any other value would work as well as this one.

count=0;
a_bound=floor(-delta*v^2/4/N);
for(a=a_bound,-1, b_bound_l=floor(-2*a*N*x-sqrt(delta));
  b_bound_u=1+floor(-2*a*N*x+sqrt(delta));
  for(b=b_bound_l,b_bound_u,
    c=(b^2-delta)/(4*N*a);if(denominator(c)==1,
      if(a*N*x^2+b*x+c>0,count=count+kronecker(-1,b); ))));
constant=count;

The quantity \( \Phi_{\gamma,D,32}(0) \) is calculated in variable “\( \text{count} \)” and stored in the variable “\( \text{constant} \)”.

g=[-21,-1;64,3];
x=(g[1,1]*t+g[1,2])/(g[2,1]*t+g[2,2]);

The matrix \( \gamma = \left( \begin{array}{cc} -21 & -1 \\ 64 & 3 \end{array} \right) \in \Gamma_0(32) \) is taken quite arbitrarily. Any other \( \gamma \in \Gamma_0(32) \) would also work.
count=0;

a_bound=floor(-delta*v^2/4/N);
for(a=a_bound,-1, b_bound_l=floor(-2*a*N*x-sqrt(delta));
b_bound_u=1+floor(-2*a*N*x+sqrt(delta));
for(b=b_bound_l,b_bound_u,
c=(b^2-delta)/(4*N*a);if(denominator(c)==1,
if(a*N*x^2+b*x+c>0,count=count+kronecker(-1,b); ))));

This is the same calculation as above, and the variable “count” now contains the value of \( \Phi_{\gamma,D,32}(x) \) with \( x = \gamma(0) = -\frac{1}{3} \).

S=constant-count;

print(" ... ",S);

});
{}

Finally, we calculate

\[ S = \Psi_{\gamma,D,32}(0) = \Phi_{D,32}(x) - \Phi_{D,32}(-1/3), \]

and print it.

The printout looks as follows:

5 ... 0 ... 0
13 ... 0 ... 0
17 ... -4 ... -1
21 ... 0 ... 0
29 ... 0 ... 0
33 ... 4 ... 1
37 ... 0 ... 0
41 ... 0 ... 0
45 ... 0 ... 0
53 ... 0 ... 0
57 ... 4 ... 1
61 ... 0 ... 0
65 ... 0 ... 0
69 ... 0 ... 0
73 ... 4 ... 1
77 ... 0 ... 0
85 ... 0 ... 0
89 ... -4 ... -1
93 ... 0 ... 0
97 ... -4 ... -1
101 ... 0 ... 0
105 ... -8 ... -2
109 ... 0 ... 0
113 ... 8 ... 2
117 ... 0 ... 0
125 ... 0 ... 0
129 ... -4 ... -1
133 ... 0 ... 0
137 ... 0 ... 0
141 ... 0 ... 0
145 ... 0 ... 0
149 ... 0 ... 0
153 ... 4 ... 1
157 ... 0 ... 0
161 ... 0 ... 0
165 ... 0 ... 0
173 ... 0 ... 0
177 ... 4 ... 1
181 ... 0 ... 0
185 ... 8 ... 2
189 ... 0 ... 0
193 ... -4 ... -1
+197 ... 0 ... 0
201 ... -4 ... -1
205 ... 0 ... 0
209 ... 4 ... 1
213 ... 0 ... 0
217 ... -8 ... -2
221 ... 0 ... 0
229 ... 0 ... 0
233 ... -4 ... -1
237 ... 0 ... 0
241 ... 4 ... 1
245 ... 0 ... 0
249 ... -4 ... -1
253 ... 0 ... 0
257 ... 0 ... 0
261 ... 0 ... 0
265 ... 0 ... 0
269 ... 0 ... 0
273 ... -8 ... -2
277 ... 0 ... 0
281 ... 4 ... 1
285 ... 0 ... 0
293 ... 0 ... 0
297 ... 0 ... 0
301 ... 0 ... 0
305 ... -8 ... -2
309 ... 0 ... 0
313 ... 0 ... 0
317 ... 0 ... 0
321 ... 4 ... 1
325 ... 0 ... 0
329 ... 8 ... 2
333 ... 0 ... 0
<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>337</td>
<td>8</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>341</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>345</td>
<td>8</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>349</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>353</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>357</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>365</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>369</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>373</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>377</td>
<td>-8</td>
<td>-2</td>
<td></td>
</tr>
<tr>
<td>381</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>385</td>
<td>8</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>389</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>393</td>
<td>-4</td>
<td>-1</td>
<td></td>
</tr>
<tr>
<td>397</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>401</td>
<td>-4</td>
<td>-1</td>
<td></td>
</tr>
<tr>
<td>405</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>409</td>
<td>-8</td>
<td>-2</td>
<td></td>
</tr>
<tr>
<td>413</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>417</td>
<td>12</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>421</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>425</td>
<td>4</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>429</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>433</td>
<td>-12</td>
<td>-3</td>
<td></td>
</tr>
<tr>
<td>437</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>445</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>449</td>
<td>-4</td>
<td>-1</td>
<td></td>
</tr>
<tr>
<td>453</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>457</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>461</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>465</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>469</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
We observe the results of computer calculations, and find that
\[ a(D) = 4 \Psi_{\gamma,D,32}(0) \]

for all \( D \equiv 1 \mod 4 \) which are not perfect squares within the range of our calculations (i.e. for \( D < 500 \)).

We believe that this may serve as convincing numerical evidence towards Conjecture 1.
References

