The Congruent Number Problem

Andreas Hatziiliou
MATH 470 - Honours Research Project
Under supervision of: Prof. Henri Darmon, Prof. Dmitry Jakobson
McGill University

August 2020

Abstract

This paper aims to give an in-depth review of the foundations behind the theorem of Tunnell regarding the congruent number problem. We discuss the works of Waldspurger, Shimura and Gross-Zagier in the theory of elliptic curves and modular forms of half-integer weight.

Contents

1 Preliminaries **3**
- 1.1 Elliptic Curves . . . 3
- 1.2 The Weierstrass $\wp$ function and a certain correspondence . . . 4
- 1.3 Modular forms . . . 6
- 1.4 Modular forms on congruence subgroups . . . 9

2 Other notions **10**

3 Congruent numbers **11**
- 3.1 First equivalent form of the statement . . . 12
- 3.2 Second equivalent form - relating the problem to some elliptic curve 13

4 Elliptic Curves and their Hasse-Weil L function **14**
- 4.1 Congruence Zeta-function . . . 14
- 4.2 The BSD conjecture . . . 16
- 4.3 Coates-Wiles Theorem . . . 16

5 Modular forms of Half-Integer Weight **17**
- 5.1 Transformation formula for the theta function . . . 17
- 5.2 Hecke operators on $M_k(N,\chi), S_k(N,\chi)$ . . . 18
- 5.3 Defining modular forms of half integral weight . . . 19
- 5.4 Hecke Operators for half-integral forms . . . 21

6 The theorems of Shimura, Waldspurger and Tunnell **22**
- 6.1 The Shimura map . . . 23
- 6.2 Waldspurger's theorem . . . 24
- 6.3 Tunnell's work and the CNP . . . 24

1 Preliminaries

We introduce some common definitions and notations which will reoccur during the entirety of the paper.

1.1 Elliptic Curves

Let K denote a field. In the following sections, we will assume $\text{char}(K) \neq 2$. Let K' be some extension of K, $f(x) \in K[x]$ a cubic polynomial with distinct roots. Then the solutions to $y^2 = f(x)$ where (x, y) are in K' are called the $K' - points$ of the elliptic curve defined by $y^2 = f(x)$.

Definition 1.1. Formally, we define an elliptic curve to be a smooth, projective, algebraic plane curve of genus one, which has a specified point $\mathcal{O}$. The exact meaning of these terms will become clear shortly.

Definition 1.2. Let $F(x, y)$ be a polynomial in two variables of degree n, we define the *homogeneous polynomial* $\tilde{F}(x, y, z)$ corresponding to F to be the polynomial which results in multiplying each monomial of F by some power of z^i for $0 \leqslant i < n$ in order to bring the total degree of latter monomials to n. Formally,

$$\tilde{F}(x, y, z) = z^n F\left(\frac{x}{z}, \frac{y}{z}\right)$$

This definition can be generalized to a polynomial in n variables, but we restrict our attention to simply two. Furthermore, it motivates the following definitions.

Definition 1.3. Let $x, y, z \in K$ and consider the equivalence relation $(x, y, z) \cong (x', y', z')$ if and only if $\exists \lambda \in K : (x, y, z) = \lambda(x', y', z')$. We define the *projective plane* $\mathbb{P}^2_K$ to be the set of all such equivalence classes of nontrivial triples. Once again, we can generalize this definition to higher dimensions, as well as possibly modifying the equivalence relation.

One can notice that that there is a trivial embedding of $K^n \to \mathbb{P}^{n+1}_k$ which takes $(x_1, x_2, ..., x_n) \mapsto (x_1, x_2, ..., x_n, 1)$. And so for some polynomial $F(x, y)$ with coefficients in K, if we want to study the solution set to $F(x, y) = 0$, it is equivalent to looking at $\tilde{F}(x, y, z) = 0$. The latter is comprised of points of form $(x, y, 1)$ where $\tilde{F}(x, y, 1) = F(x, y) = 0$, as well as the points which lie on the line at infinity. The solution set to $\tilde{F}(x, y, z) = 0$ is called the projective completion of $F(x, y) = 0$. This alternate way of approaching things is of interest because it allows us to define a group structure on elliptic curves when considering them as objects living in $\mathbb{P}^2_K$.

Definition 1.4. Let $L = \{n\omega_1 + m\omega_2 | n, m \in \mathbb{Z}\}$ be some lattice of $\mathbb{C}$, we define the fundamental parallelogram of ω_1, ω_2 to be

$$\Pi = \{a\omega_1 + b\omega_2 | 0 \leqslant a, b \leqslant 1\}$$

Definition 1.5. For some lattice L, we say that a meromorphic function f is *elliptic* relative to L if $f(z+l) = f(z)$ for $l = \omega_1, \omega_2$. Any such function is determined uniquely by the values it takes on inside the fundamental parallelogram. Moreover, it becomes intuitive to think of elliptic functions as functions on the torus which results from "gluing" the opposite sides of the fundamental parallelogram together. This construction will be useful when we trying to define the group operation of an elliptic curve.

1.2 The Weierstrass $\wp$ function and a certain correspondence

Building from the previous heuristic, we now can see that elliptic functions can be considered as functions on the torus $\mathbb{C}/L$ obtained by modding out by some lattice L. We will build up to a certain correspondence between $\mathbb{C}/L$ and a certain elliptic curve, which will allow us to define the group operation for all elliptic curves.

Definition 1.6. Given some lattice $L = \{m\omega_1 + n\omega_2\}$ of $\mathbb{C}$, we define the "Weierstrass $\wp$ function" to be

$$\wp(z) = \wp(z; L) := \frac{1}{z^2} \sum_{\substack{l \in L \\ l \neq 0}} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right)$$

This function is doubly periodic and it is well defined since the sum converges on any compact subset of $\mathbb{C} \backslash L$

Proposition 1.7. *We let $\mathscr{E}_L$ denote the field of elliptic functions. We have that $\mathscr{E}_L = \mathbb{C}(\wp, \wp')$. Moreover, the space of even elliptic functions $\mathscr{E}_L^+ = \mathbb{C}(\wp)$*

We now use the two following facts in order to construct our desired correspondence. 1) the function $(\wp')^2$ is an even elliptic function and it is a cubic polynomial in $\wp$ since it has a triple pole at 0 and three simple zeros. 2) $(\wp')^2$ has double zeroes at $\omega_1/2, \omega_2/2$ and $(\omega_1 + \omega_2)/2$. 3) for any positive integer N, the even elliptic function $\wp(Nz)$ is a rational function in $\wp$.

Thus, from 1 and 2, we get

$$\begin{aligned}(\wp'(z))^2 &= C(\wp(z)-\wp(\omega_1/2))(\wp(z)-\wp(\omega_2/2))(\wp(z)-\wp((\omega_1+\omega_2)/2)\\ &= C(\wp(z)-e_1)(\wp(z)-e_2))(\wp(z)-e_3)\end{aligned}$$

We let e_i replace the roots. Comparing coefficients in the Laurent expansion at the origin, it is readily shown that the constant $C = 4$. Thus, $\wp$ satisfies

$$\wp'(z)^2 = f(\wp(z)) \qquad \text{where} \qquad f(x) = 4(x-e_1)(x-e_2)(x-e_3)$$

This differential equation can be transformed into a slightly nicer form:

$$\wp'(z)^2 = f(\wp(z)) \qquad \text{where} \qquad f(x) = 4x^3 - g_2(L)x - g_3(L)$$

where $g_2(L), g_3(L)$ are constants which depend on our lattice L.

This differential equation leads us to an analytic map from $\mathbb{C}/L \to \mathbb{P}^2_{\mathbb{C}}$ given by

$$\begin{aligned}&z \mapsto (\wp(z), \wp'(z), 1) \quad \text{for} \quad z \neq 0\\ &0 \mapsto (0,1,0)\end{aligned}$$

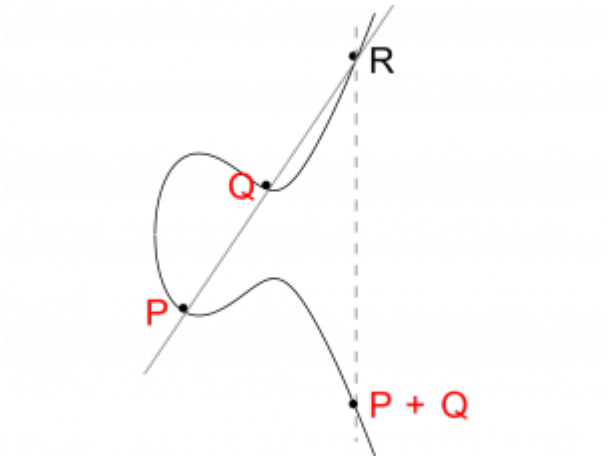
We can see that this map takes any nonzero $z \in \mathbb{C}/L$ to a point (x, y) which satisfies $y^2 = f(x)$. Since $f(x)$ is a cubic polynomial with distinct roots, this maps actually sends z to a point on the elliptic curve defined by $y^2 = f(x)$.

Proposition 1.8. *Every elliptic curve E defined over $\mathbb{C}$ can be written in the form*

$$y^2 = 4x^3 - g_2(L)x - g_3(L)$$

for some lattice L and constants g_2, g_3 depending on L.

Now, given this analytic map, we have a natural way of defining "addition" of two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, on an elliptic curve E. We use the standard notion of addition of points in $\mathbb{C}/L$ to define the group law on the curve. More precisely, we use the inverse map to send points of the curve back to the z-plane, find z_1, z_2 such that $P_1 = (\wp(z_1), \wp'(z_1))$ and $P_2 = (\wp(z_2), \wp'(z_2))$ then set $P_1 + P_2 = (\wp(z_1+z_2), \wp'(z_1+z_2))$. The specified point a curve, denoted $\mathcal{O}$, is taken to be the point $(0, 1, 0)$ at infinity, and acts as the identity. Moreover, there is a nice geometric interpretation of addition on an elliptic curve. To add two points P and Q we draw the line joining them, find the third point of intersection of that line with the curve, and then take the symmetric point on the other side of the x-axis.



Addition of two points on an elliptic curve.

1.3 Modular forms

Let R be a commutative ring.

Definition 1.9. Let $M_n(R)$ denote the set of matrices with entries in R. The general linear group $GL_n(R) := \{M \in M_n(R) : det(M) \in R^*\}$

Definition 1.10. The special linear group $SL_n(R) \leqslant GL_n(R)$ such that $SL_n(R) := \{g \in GL_n(R) : det(g) = 1\}$

In this paper we will often refer to $\tilde{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ also known as the Reimann Sphere or complex projective line $\mathbb{P}^1_{\mathbb{C}}$. We will work with $SL_2(\mathbb{Z})$ and its subgroups for reasons which will become apparent soon.

Definition 1.11. For some $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$, some $z \in \mathbb{C}$ we define the 'fractional linear transformation'

$$gz \mapsto \frac{az + b}{cz + d}$$

and moreover g send the point at infinity to $\lim_{z\to\infty} gz = \frac{a}{c}$. This type of transformation defines a group action on $\tilde{\mathbb{C}}$.

It is readily shown that the two only matrices in $SL_2(\mathbb{R})$ which act trivially on $\tilde{\mathbb{C}}$ are $\pm I$. Thus, by quotient out by $\{\pm I\}$ we obtain a group which acts faithfully on $\mathbb{C}$. This group acts by transformations on the upper half plane $\mathbb{H}$.

To see this, take $g \in SL_(\mathbb{R}), z \in \mathbb{H}$. Then, Im(z) $>0 \implies$ Im(gz) > 0 since

$$Im(gz) = Im\frac{az+b}{cz+d} = Im\frac{(az+b)(c\bar{z}+d)}{|cz+d|^2} = \frac{Im(adz+bc\bar{z})}{|cz+d|^2}$$
$$= \frac{det(g)Im(z)}{|cz+d|^2} = \frac{Im(z)}{|cz+d|^2} > 0$$

Definition 1.12. This construction leads us to define to be the "Modular Group", a group of central importance in number theory. The full modular group is defined as $\Gamma = SL_2(\mathbb{Z})$, and is the group of all rational fractional linear transformations. Moreover we denote $\bar{\Gamma} = \Gamma/\{\pm I\}$, which acts faithfully on $\mathbb{H}$.

We now introduce a few important subgroups of the modular group which will be useful for the coming sections

Definition 1.13. Let $N \in \mathbb{N}$. We introduce a normal subgroup of $SL_2(\mathbb{Z})$ called the "principal congruence subgroup of level N" to be

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

We can see this subgroup to be normal as it is the kernel of the map $\phi : \Gamma \to SL_2(\mathbb{Z})$ sending $g \mapsto g \mod N$. We call a subgroup of Γ a congruence subgroup of level N if it contains $\Gamma(N)$. Remark that any congruence subgroup of level N will also contain level M when M is a multiple of N.

In the context of this paper, we will often work with the following two congruence subgroups of Γ:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \middle| c \equiv 0 \mod N \right\}$$

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \middle| a \equiv 0 \mod N \right\}$$

We now consider the group action of $\Gamma \circlearrowright \mathbb{H}$ in order to define its fundamental domain.

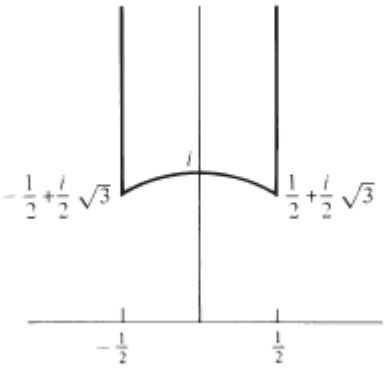
Proposition 1.14. *The group* $\Gamma =< T, S >$. *Where*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

The first acts on z by translating it to $z+1$. *The second sends z to* $\frac{-1}{z}$, *the*

negative reciprocal map.

The fundamental domain of Γ is $F := \{z \in \mathbb{H} : |Re(z)| \leqslant \frac{1}{2} and |z| \geqslant 1\}$



Fundamental domain of $SL_2(\mathbb{Z})$

We now briefly discuss an alternative and more convenient way of working with modular forms. Consider the map from $\bar{\mathbb{H}} = \mathbb{H} \cup \{\infty\}$ to the punctured unit disc given by

$$z \mapsto q = e^{2\pi i z}$$

where we map the point at infinity in $\mathbb{H}$ to the origin. We then get Laurent expansions for our complex functions which resemble

$$f(z) = \sum_{n \in \mathbb{Z}} a_n q^n$$

This allows us to talk about meromorphicity and holomorphicity at ∞ by stating that:

- f is meromorphic at ∞ if the q-expansion has only finitely many nonzero a_n with $n < 0$
- f is holomorphic at ∞ if the q-expansion has no nonzero a_n with $n < 0$
- f is said to vanish at ∞ if it is holomorphic on $\mathbb{H}$ and $a_0 = 0$.

Definition 1.15. Let $k \in Z$, let $f(z)$ be meromorphic on $\mathbb{H}$ with q-expansion $\sum_{n \in \mathbb{Z}} a_n q^n$. Suppose $f(z)$ satisfies

$$f(\gamma z) = (cz + d)^k f(z) \quad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

1. If $f(z)$ is meromorphic at infinity then we call f a "modular function" of weight k for Γ.

2. If $f(z)$ is holomorphic on $\mathbb{H}$, then we call f a "modular form" of weight k for Γ.

3. Finally if f additionally has $a_0 = 0$, then we call f a "cusp form" of weight k for Γ

We denote the space of all modular forms of weight k for Γ by $M_k(\Gamma)$. The space of cusp forms is denoted $S_k(\Gamma)$.

Definition 1.16. Let $k > 2$ be an even integer, for $z \in \mathbb{H}$ we define the *Eisenstein series*

$$G_k(z) = \sum_{m,n \in \mathbb{Z}} \frac{1}{(mz+n)^k}$$

Proposition 1.17. $G_k(z) \in M_k(\Gamma)$

Definition 1.18. We define the normalized Eisenstein series to be

$$E_k(z) = \frac{1}{2\zeta(k)} G_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

Where the B_k are the Bernoulli numbers and $\sigma_{k-1}(n) \sum_{d|n} d^{k-1}$.

Definition 1.19. The *j-invariant* is a modular form of weight zero defined as

$$j(z) = \frac{1728 g_2(z)^3}{\Delta(z)} = \frac{1728 E_4(z)^3}{E_4(z)^3 - E_6(z)^2}$$

Proposition 1.20. *The j function gives us a bijection between* $\Gamma/\bar{\mathbb{H}}$ *and the Reimann Sphere*

Proof. temp. □

1.4 Modular forms on congruence subgroups

We now want to make the previous definition more precise. To start off by introducing some notation. Let $GL_2^+(\mathbb{Q})$ be the subgroup of $GL_2(\mathbb{Q})$ consisting of matrices of positive determinant. Let $f(z)$ be a function on $\bar{\mathbb{H}} = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$, let $k \in \mathbb{Z}$ and $\gamma \in GL_2^+(\mathbb{Q})$. We denote

$$f(z)|[\gamma]_k := (\det \gamma)^{k/2} (cz+d)^{-k} f(\gamma z) \qquad \text{for} \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Given this notation, it is clear that any modular function of weight k for Γ satisfies $f|[\gamma]_k = f$ for any $\gamma \in \Gamma$. This now allows us to define modular functions, forms and cusp forms for the congruence subgroups $\Gamma' \supset \Gamma(N)$.

If $f(z)$ is a meromorphic function on $\mathbb{H}$, $\Gamma' \subset \Gamma$ a congruence subgroup of level N, $k \in \mathbb{Z}$. If

$$f|[\gamma]_k = f \quad \text{for all} \quad \gamma \in \Gamma'$$

and for any $\gamma_0 \in \Gamma$ $f(z)$ has a q-expansion $\sum a_n q_N^n$ with only finitely many non-zero a_n with $n < 0$, we call f a modular function of weight k for Γ'. We define similarly as before, a modular form of weight k on Γ', to be an f which is holomorphic on $\mathbb{H}$ and has no non-zero a_n for $n < 0$. Again, cusp forms have the additional requirement of vanishing at ∞. We denote the space of all modular forms of weight k for Γ' by $M_k(\Gamma')$. The space of cusp forms is denoted $S_k(\Gamma')$.

Definition 1.21. Let χ be a Dirichlet character mod N, we define

$$M_k(N,\chi) = \left\{ f \in M_k(\Gamma_1(N)) : f|[\gamma]_k = \chi(d)f \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \right\}$$

Proposition 1.22. *$M_k(\Gamma_1(N)) = \oplus M_k(N,\chi)$ where the sum is over all Dirichlet characters modulo N.*

The spaces $M_k(N,\chi)$ include many important examples of modular forms. Moreover, we introduce the notation $S_k(N,\chi)$to denote the subspace of cusp forms $S_k(N,\chi) = M_k(N,\chi) \cap S_k(\Gamma_1(N))$.

2 Other notions

Definition 2.1. Let $d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ be an odd integer, c be any integer. We define the *Jacobi Symbol* $(\frac{c}{d})$

$$\left(\frac{c}{d}\right) = \left(\frac{c}{p_1}\right)^{\alpha_1} \left(\frac{c}{p_2}\right)^{\alpha_2} \cdots \left(\frac{c}{p_k}\right)^{\alpha_k}$$

Where $(\frac{c}{p})$ denotes the usual Legendre symbol defined by:

$$\left(\frac{c}{p}\right) = \begin{cases} 0 & \text{if } c \equiv 0 \pmod{p} \\ 1 & \text{if } c \not\equiv 0 \pmod{p} \text{ c is a quadratic residue modulo p} \\ -1 & \text{if } c \not\equiv 0 \pmod{p} \text{ c isn't a quadratic residue modulo p} \end{cases}$$

Whereby quadratic residue modulo p, we mean that $\exists x$, an integer, such that $x^2 = c \mod p$

Definition 2.2. Let n be a positive integer. We call define χ, a *character modulo n* to be complex valued function on $\mathbb{Z}$ such that

$$\chi(a) = \begin{cases} 0 & \text{if gcd(a,n)} \neq 1 \\ \chi_0(\text{a mod n}) & \text{if gcd(a,n)=1} \end{cases}$$

Where $\chi_0 : \mathbb{Z}/n\mathbb{Z} \to T$ is some homomorphism and $T := \{z \in \mathbb{C} : |z| = 1\}$. We call the *conductor* of χ the smallest integer c such that $\chi(a)$ depends only on (a mod c) when gcd(a,n) = 1. A character modulo n is called *primitive* if its conductor is n.

Definition 2.3. For a primitive character χ modulo n, we define the *Gauss sum* $g(\chi)$

$$g(\chi) = \sum_{k=1}^{n} \chi(k) e^{\frac{2\pi i k}{r}}$$

Definition 2.4. Let A, B be subgroups of G. We call A and B "commensurable" given that $[A : A \cap B] < \infty$ and $[B : A \cap B] < \infty$.

Definition 2.5. The Gamma function is given by

$$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt$$

$$\Gamma(s+1) = s\Gamma(s)$$

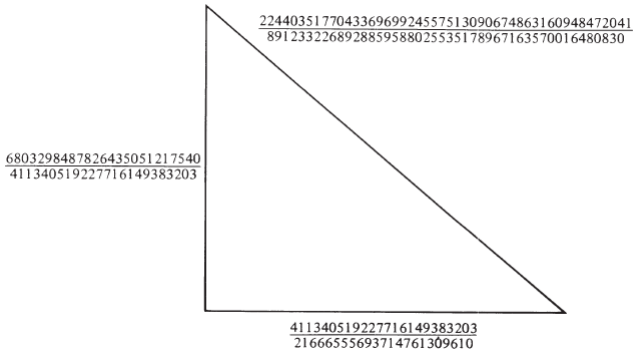
Definition 2.6. The zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\text{primes p}} \frac{1}{1 - p^{-s}}$$

3 Congruent numbers

In layman's terms, a congruent number is a number n which is the area of some possible right angle triangle with rational side-lengths. Right angle triangles and Pythagorean triples have been of interest since the times of ancient Greece. The question of whether or not a given integer n is or is not a congruent number was first rigorously discussed by Arab Scholars in the tenth century. This age old question is now of interest more than ever, and with the advancements made in the theory of elliptic curves in the last decade, the CNP has seen significant progress - even a partial solution which we will discuss further in the coming sections.

Definition 3.1. A number n is called congruent if it is a square-free integer such that $\exists X, Y, Z \in \mathbb{Q}$ such that the equations $X^2 + Y^2 + Z^2 = n$ and $\frac{XY}{2} = n$ have simultaneous solutions. Note that we may assume n to be square-free, because for any $r \in \mathbb{Q}$ such that r is the area of a right triangle with sides $X, Y, Z \in \mathbb{Q}$, there exists some $s \in \mathbb{Q}$ such that $s^2 r$ is a square-free integer. But the triangle with sides sX, sY, sZ has area $s^2 r$.



Triangle of area 157 [D. Zagier]

3.1 First equivalent form of the statement

For the remainder of this paper, when we refer to an integer n as the area of a right angle triangle, we will assume that it square-free.

Proposition 3.2. *Let $X, Y, Z \in \mathbb{Q}^+$ such that $X < Y < Z$ be the sides of a right angle triangle, n be the area of this triangle. Consider the numbers x such that $x+n$ and $x-n$ are each the square of a rational number. Then, considering the correspondence*

$$X, Y, Z \to x = \left(\frac{Z}{2}\right)^2$$

$x \to X = \sqrt{x+n} - \sqrt{x-n}, Y = \sqrt{x+n} + \sqrt{x-n}.Z = 2\sqrt{x}$

Then n is congruent iff $\exists$ such an x for which $x+n$ and $x-n$ are squares of some rational numbers.

Proof. Suppose X, Y, Z satisfy that $X^2 + Y^2 = Z^2$, $\frac{XY}{2} = n$. Then we get

$$(X \pm Y)^2 = Z^2 \pm 4n$$

by adding or subtracting the two equations four times. Then, dividing through by four: $x = \left(\frac{Z}{2}\right)^2$ and $x \pm n = \left(\frac{X+Y}{2}\right)^2$. Conversely, given x with such properties, then the numbers X,Y,Z as defined above satisfy $XY = 2n$ and

$X^2 + Y^2 = 4x = Z^2$. Finally, the correspondence is readily checked to be bijective. □

3.2 Second equivalent form - relating the problem to some elliptic curve

We will now derive yet another equivalent formulation of our problem. From the proposition above, we are given that when X,Y,Z are the rational side lengths of a triangle of area n, then $((X \pm Y)/2)^2 = (Z/2)^2 \pm n$. Thus, multiplying the two equations we obtain: $((X^2 - Y^2)/4)^2 = (Z/2)^4 - n^2$. After introducing new variables $u = Z/2, v = (X^2 - Y^2)/4$ and multiplying by $u^2 \implies u^6 - n^2u^2 = u^2v^2$ has rational solutions. Moreover, after another choice of variables $x = u^2 = (Z/2)^2$ and $y = uv = Z/8 * (X^2 - Y^2)$ we get a rational 2-tuple (x,y) which satisfies

$$y^2 = x^3 - n^2x$$

Now, it is natural to wonder under what conditions a rational point (x,y) on this curve would arise from the sides of a right angle triangle.

Proposition 3.3. *Let (x,y) be a rational point on the curve $y^2 = x^3 - n^2x$. Suppose x satisfies the following: (i) x is the square of some rational number, (ii) the denominator of x is even, (iii) the numerator has no common factor with n. Then, there exists some 'congruent' triangle with area n that corresponds to x under the correspondence of proposition 2.2*

We now state the main result of this paper, a very nice theorem of Tunnell [4] which provides a criterion upon which a given square-free integer is a congruent number. In the following sections, we will build up more theory in order to give a heuristic understanding behind the logic and arguments used in the proof of Tunnell's theorem, which will be discussed in the final chapter.

Theorem 3.4 (Tunnell 1983)**.** *If n is a squarefree and odd (respectively, even) positive integer and n is the area of a right triangle with rational sides, then*

$$\#\{x, y, z \in \mathbb{Z} | n = 2x^2 + y^2 + 32z^2\} = \frac{1}{2}\#\{x, y, z \in \mathbb{Z} | n = 2x^2 + y^2 + 8z^2\}$$

$$\left(resp. \quad \#\{x, y, z \in \mathbb{Z} | \frac{n}{2} = 4x^2 + y^2 + 32z^2\} = \frac{1}{2}\#\{x, y, z \in \mathbb{Z} | \frac{n}{2} = 4x^2 + y^2 + 8z^2\} \right)$$

And if the weak form of BSD holds true for the curves $E_n : y^2 = x^3 - n^2x$, then the converse of this statement also holds true.

4 Elliptic Curves and their Hasse-Weil L function

4.1 Congruence Zeta-function

In this section, our goal is to define what is called the L-function of an elliptic curve. These objects encode key information about curves, as well as give rise to nice functional equations which allow us to derive many important results. We first start by introducing one of the "building blocks" of the L-function

Definition 4.1. Given some sequence $\{N_r\}_{r\in\mathbb{N}}$, we define the corresponding zeta function by the formal power series

$$Z(T) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\right)$$

Theorem 4.2. *Let E_n be the curve $y^2 = x^3 - n^2x$ defined over $\mathbb{F}_p$ where $p \nmid 2n$. Then*

$$Z(E_n/\mathbb{F}_p; T) = \frac{(1-\alpha T)(1-\bar{\alpha}T)}{(1-T)(1-pT)}$$

where $\alpha = i\sqrt{p}$ if $p \equiv 3$ (mod 4), and if $p \equiv 1$ (mod 4) then $\alpha \in \mathbb{Z}[i]$ of norm p which is congruent to $(\frac{n}{p})$ mod 2+2i.

Now, we remark that the information which we obtain by considering the zeta function of the reduction of the curve E modulo primes p of good reduction is quite important. It is what helps us define the Hasse-Weil L-function.

Definition 4.3. We define the L function of E_n. First, make substitution $T = p^{-s}$

$$\begin{aligned} L(E_n, s) &= \frac{\zeta(s)\zeta(s-1)}{\prod_p Z(E_n/\mathbb{F}_q; p^{-s})} \\ &= \prod_{p\nmid 2n} \frac{1}{1 - 2a_{E_n,p}p^{-s} + p^{1-2s}} \\ &= \prod_{P\nmid 2n} \frac{1}{1 - \alpha_P^{degP}(\mathbb{N}(P))^{-s}} \end{aligned}$$

Where α_P is defined similarly to above and the second product is taken over prime ideals P which divide primes p of good reduction. $\mathbb{N}(P)$ denotes the norm.

Theorem 4.4. *The Hasse-Weil L-function $L(E_n, s)$ for the elliptic curve E_n extends analytically to an entire function on the complex s-plane . In addition,*

let

$$N = \begin{cases} 32n^2 & n \text{ odd} \\ 16n^2 & n \text{ even} \end{cases}$$

Let

$$\Lambda(s) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s)L(E_n, s)$$

Then, $L(E_n, s)$ satisfies the functional equation

$$\Lambda(s) = \pm\Lambda(2-s)$$

where the "root number" ± 1 is equal to 1 if $n \equiv 1, 2, 3$ (mod 8) and -1 if $n \equiv 5, 6, 7$ (mod 8).

Theorem 4.5 (Mordell-Weil)**.** *Let A be an abelian variety defined over a feild K, then the group of K-points $A(K)$ is a finitely generated abelian group.*

The Mordell-Weil theorem is useful to us because elliptic curves can be viewed abelian varieties of dimension 1. Thus when considering curves defined over $\mathbb{Q}$, we get that the group of $\mathbb{Q}$-points of an elliptic curve $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$, where the integer r is called the *rank* of the curve. This rank is greater than 0 if only if the elliptic curve has infinitely many $\mathbb{Q}$-points. It is an open problem weather curves of arbitrarily large rank exist, although many believe this to be the case. In the case of our beloved curves E_n, we have the following propositions:

Proposition 4.6. *ord$(E_n(\mathbb{Q}))$ = 4. And the four points of finite order are $(\pm n, 0), (0, 0), \infty$. These points are of order 2.*

Proposition 4.7. *n is a congruent number if and only if $E_n(\mathbb{Q})$ has nonzero rank.*

Proof. Suppose that n is congruent. from (prop where i talk about the equivalence of n cong and E_n] we know that n being congruent leads to a rational point on E_n whose x coordinate is in $(\mathbb{Q}^+)^2$. The x-coordinates of the three nontrivial points are 0 or $\pm n$. Thus, there must exist some rational point of order $\neq 2$ (since these are not in $(\mathbb{Q}^+)^2$). This forces the point to be of infinite order.

Conversely, suppose some point $P = (x_0, y_0)$ has infinite order. We show that the x coordinate of 2P is the square of some rational number. Well, suppose

P is of order not 2, then the x coordinate of $2P$, is given by the addition formula:

$$x = -2x_0 + \frac{(3x_0^2 - n^2)^2}{(2y_0)^2} = \frac{9x_0^4 - 6x_0^2n^2 + n^4 - 2x_0 * 4(x_0^3 - n^2x_0)}{4(x_0^3 - n^2x_0)}$$
$$= \frac{(x_0^2 + n^2)^2}{4(x_0^3 - n^2x_0)} = \frac{(x_0^2 + n^2)^2}{(2y_0)^2}$$

To show that the denominator must be odd, there are two cases we must consider. Firstly, if x_0 and n are even. Then 2 divides them both which means the numerator and n share a common factor. This cannot be since, if some prime $p|x_0^2 + n^2$ and $p|n \implies p|x \implies p^3|x^3 - n^2x = y^2$ and thus we can factor a p^2 on the top and bottom. We can repeat this process and find that the numerator doesn't share any prime factors with n. The second case x and n are both odd. We write $x = 2r + 1$ and $n = 2s + 1$. We get $(x_0^2 + n^2)^2 = 16(r^2 + r + s^2 + s)^2 + 16(r^2 + r + s^2 + s) + 4$. Thus, 4 divides the numerator, and at least $16|(2y)^2$. Thus the denominator is even. And so by the same correspondence as before, we get that n is congruent. □

4.2 The BSD conjecture

Conjecture: [B. J. Birch and H. P. F. Swinnerton-Dyer] Let E be an elliptic curve defined over $\mathbb{Q}$, then the order of vanishing of $L(E, s)$ at $s = 1$ is equal to the rank of $E(\mathbb{Q})$. In particular this implies $L(E, 1) = 0$ if and only if E has infinitely many rational points

4.3 Coates-Wiles Theorem

Theorem 4.8 (J. Coates and A. Wiles)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ having complex multiplication. If E has infinitely many $\mathbb{Q}$-points, then $L(E, 1) = 0$.*

We know that the E_n have complex multiplication and so by proposition 4.7 we get that if $L(E_n, 1) \neq 0$ then n isn't congruent. Conversely, assuming BSD holds true, then $L(E_n, 1) = 0 \implies n$ congruent. We can now state the first major result in our journey to Tunnell's theorem.

Proposition 4.9. *If $n \equiv 5, 6, 7$ (mod 8), and assuming weak BSD to hold true, then n is congruent.*

Proof. According to theorem 4.4 , if $n \equiv 5, 6, 7 \pmod 8$ then $\Lambda(s) = -\Lambda(2 - s)$. Letting $s = 1$, we get that $\Lambda(1) = -\Lambda(1) \implies \Lambda(1) = 0$. But again from 4.4 we know that $\Lambda(1) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(1)L(E_n, 1) \implies L(E_n, 1) = 0$. Thus, by the same proposition we get that $E_n(\mathbb{Q})$ has nonzero rank $\implies n$ is congruent. □

Now, one might ask what happens if we wish to prove a similar result which doesn't depend on the BSD conjecture, an open problem. Well, without going into too much detain, we have a constructive method from Gross-Zagier which uses something called "Heegner points", which tells us the following: If $n \equiv 5, 6, 7 \pmod 8$, E_n has nonzero rank (moreover we can construct some point of infinite order) given only that it's L-function has a simple zero at $s = 1$. It still remains unknown whether the vanishing of $L(E_n, 1)$ of a higher order tells us anything about n being congruent if we do not assume BSD.

5 Modular forms of Half-Integer Weight

5.1 Transformation formula for the theta function

We first start by discussing the Theta function, one which has nice properties which will be desirable later on when defining forms of half-integral weight.

Definition 5.1. The Theta function is defined as follows

$$\Theta(z) = \sum_{n \in \mathbb{Z}} e^{2\pi i n^2 z} \qquad z \in \mathbb{H}$$

Let $(\frac{c}{d})$ be a quadratic residue symbol. Let $\sqrt{z}$ denote the branch for which $\arg(z) \in (-\pi/2, \pi/2]$. Then we define ϵ_d for d odd by $\epsilon_d = \sqrt{(\frac{-1}{d})}$, i.e

$$\epsilon_d = \begin{cases} 1 & \text{if } d \equiv 1 \mod 4 \\ i & \text{if } d \equiv 1 \mod 4 \end{cases}$$

We can now define the "automorphy factor" $j(\gamma, z)$ depending on $\gamma \in \Gamma_0(4)$, $z \in \mathbb{H}$

$$j(\gamma, z) = \left(\frac{c}{d}\right) \epsilon_d^{-1} \sqrt{cz + d} \quad \text{for} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$$

Theorem 5.2. *Let $\gamma \in \Gamma_0(4)$ and $z \in \mathbb{H}$*

$$\Theta(\gamma z) = j(\gamma, z)\Theta(z)$$

From the theorem above, it is clear that the square of the theta function is a modular form of weight 1 for $\Gamma_0(4)$ and χ the unique non-trivial character mod 4. Intuitively, it should stand out that since this function has a transformation rule which contains a square root of the $(cz + d)$ part, that we should be able to extend our study of modular forms of integer weight to half integer weight by simply considering $\sqrt{cz + d}$ to the k-th power.

5.2 Hecke operators on $M_k(N,\chi), S_k(N,\chi)$

Before we formally define Hecke operators, we motivate them by stating that many very important examples of modular forms turn out to be a sort of eigenvector (called "eigenforms") for the action of all of these operators on various spaces M_k and S_k of forms. If $f \in M_k(N,\chi)$ is such an eigenform, then we can conclude a lot of information about its q-expansion coefficients.

Proposition 5.3. *Suppose that $f = \sum a_m q^m \in M_k(N,\chi)$ is an eigenform for all the operators T_m with corresponding eigenvalues λ_m, i.e. $T_m f = \lambda_m f$. Then $a_m = \lambda_m a_1$ for all $m \in \mathbb{N}$. Additionally, $a_1 \neq 0$ unless $k = 0$ and f is a constant function. If $a_0 \neq 0$ then we obtain the eigenvalues by the formula*

$$\lambda_m = \sum_{d|m} \chi(d) d^{k-1}$$

Proposition 5.4. *Let $H \subset G$ be any subgroup, $a \in G$ any element such that H and $a^{-1}Ha$ are commensurable. Let $H' = H \cap a^{-1}Ha$. Let $[H : H'] = d$ and write $H = \bigcup_{j=1}^{d} H'h_j$. Then $HaH = \bigcup_{j=1}^{d} Hah_j$ is a disjoint union of d right cosets. Conversely, if $HaH = \bigcup_{j=1}^{d} Hah_j$ is a disjoint union of d right cosets, then $H = \bigcup_{j=1}^{d} H'h_j$*

We define Hecke operators on a class of congruence subgroups of Γ which includes $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$. Let $S^+ = m\mathbb{Z}$ for some positive integer m, $S^\times$ be a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$, or alternatively denote the subset of $\mathbb{Z}$ whose image mod N is in $S^\times$.

$$\Delta^n(N, S^\times, S^+) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}) : N|c, a \in S^\times, b \in S^+, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = n \right\}$$

Here are some examples:

$$\Gamma_1(N) = \Delta^1(N, 1, \mathbb{Z}) \quad \Gamma_0(N) = \Delta^1(N, (\mathbb{Z}/N\mathbb{Z})^\times, \mathbb{Z}) \quad \Gamma(N) = \Delta^1(N, 1, N\mathbb{Z})$$

Definition 5.5. Let Γ' be a congruence subgroup of Γ and $\alpha \in GL_2^+(\mathbb{Q})$. Let $\Gamma'' = \Gamma' \cup \alpha^{-1}\Gamma'\alpha$ and $d = [\Gamma' : \Gamma'']$, $\Gamma' = \bigcup_{j=1}^{d} \Gamma''\gamma_j'$. Let $f(z)$ be a function on $\mathbb{H}$ invariant under $[\gamma]_k$ for $\gamma \in \Gamma'$. Then

$$f(z)|[\Gamma'\alpha\Gamma']_k := \sum_{j=1}^{d} f(z)|[\alpha\gamma_j']_k$$

Note that this definition does not depends on the choice of representative α nor

on the choice of the representatives γ'_j of Γ' mod Γ''. If $f \in M_k(\Gamma')$ it follows that $f(z)|[\Gamma'\alpha\Gamma']_k \in M_k(\Gamma')$.

Definition 5.6. Let $\Gamma' = \Delta^1(N, S^\times, S^+)$ and let n be a positive integer. Let $f \in M_k(\Gamma')$. Then, we define a Hecke operator T_n to act by

$$T_n f := n^{k/2-1} \sum f|[[\Gamma'\alpha\Gamma']_k]$$

where the sum is taken over all double cosets of Γ' in $\Delta^n(N, S^\times, S^+)$. By the previous proposition, we have $T_n f \in M_k(\Gamma')$

5.3 Defining modular forms of half integral weight

Similarly to the case of integral weight modular forms, we wish to have something which transforms like $f(\gamma z) = (cz + d)^{k/2} f(z)$ where as per usual $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma' \subset \Gamma$ and now k is an *odd* positive integer. One can see that we quickly run into issues by defining such a functional equation because of the possible choice of square root branches. A more natural construction is to define something analogous to the way Θ^k transforms.

Definition 5.7. When we have a functional equation similar to $f(\gamma z) = J(\gamma, z) f(z)$ where γ is in some matrix group and $z \in \mathbb{H}$. We call $J(\gamma, z)$ the "automorphy factor". It must satisfy

$$J(\alpha\beta, z) = J(\alpha z) J(\beta, z) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$$

For some matrix group G

Two such examples of an automorphy factor are $J(\gamma, z) = (cz + d)^k$ for modular forms of integral weight as well as $J(\gamma, z) = (\frac{c}{d}) \epsilon_d^{-1} \sqrt{cz + d}$ where $\gamma \in \Gamma_0(4)$ which is the automorphy factor for $\Theta(z)$. We now define the automorphy factor for integral forms of half integral weight. Given that the automorphy factor for the Theta function already contains a square root, it is natural to want to define something which transforms like k-th powers of it.

Definition 5.8. For a congruence subgroup $\Gamma' \subset \Gamma_0(4)$ we define modular forms of weight $k/2$ to be holomorphic functions on $\mathbb{H}$ (and at cusps) which transform like the k-th powers of $\Theta(\gamma z)$. Formally

$$j(\gamma, z) = \frac{\Theta(\gamma z)}{\Theta(z)} = \left(\frac{c}{d}\right) \epsilon_d^{-1} \sqrt{cz + d} \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$$

Now, if we want to to define $[\gamma]_{k/2}$similarly as before for matrices in $GL_2^+(\mathbb{Q})$, we encounter an issue because the automorphy factor is only defined for $\gamma \in \Gamma_0(4)$ and so we have no preferred branch of the square root for arbitrary $\gamma \in GL_2^+(\mathbb{Q})$. To get arround this issue, consider the following:

Definition 5.9. Let $\mu_4 = \{\pm 1, \pm i\}$ and consider the degree 4 extension of $GL_2^+(\mathbb{Q})$

$$1 \to \mu_4 \to G \to GL_2^+(\mathbb{Q}) \to 1$$

where the group G is defined as

$$G = \left\{(\alpha, \phi(z)) : \alpha \in GL_2^+(\mathbb{Q}), \phi \text{ holomorphic on } \mathbb{H} \text{ s.t. } \phi^2(z) = t\frac{cz+d}{\sqrt{\det a}}, t = \pm 1\right\}$$

G is a group with operation $(\alpha, \phi(z))(\beta, \psi(z)) = (\alpha\beta, \phi(\beta z)\psi(z))$.

Given the previous definition of the group G, it is natural to consider the projection map $P : G \to GL_2^+(\mathbb{Q})$ given by $(\alpha, \phi(z)) \mapsto \alpha$. Moreover, if we are working with $\Gamma' \subset \Gamma_0(4)$, then we define

$$\tilde{\Gamma'} \cong P(\Gamma') := \{(\gamma, j(\gamma, z) : \gamma \in \Gamma'\}$$

We can also consider $L : \Gamma_0(4) \to G$, the lifting of the map P, which sends

$$\gamma \mapsto \tilde{\gamma} := (\gamma, j(\gamma, z)) \in G$$

Definition 5.10. Let k be an integer. A modular form of weight k for $\Gamma' \subset \Gamma_0(4)$ is a holomorphic function on $\mathbb{H}$ such that

1. $f|[\tilde{\gamma}]_{k/2}$ for all $\tilde{\gamma} \in \tilde{\Gamma'}$
2. f is holomorphic at all cusps of Γ'

Additionally f is a cusp form for Γ', if it satisfies the condition of vanishing at each cusp of Γ'. We denote the two spaces respectively by $M_{k/2}(\tilde{\Gamma'})$ and $S_{k/2}(\tilde{\Gamma'})$.

Moreover, we have another analogous result from the integral case. Letting χ be a character of $(\mathbb{Z}/N\mathbb{Z})^*$ and if $M_{k/2}(\tilde{\Gamma}_0(N), \chi)$ is the subspace of $S_{k/2}(\tilde{\Gamma'}, \chi) = M_{k/2}(\tilde{\Gamma}_1(N))$ consisting of $\gamma \in \Gamma_0(N)$ such that $f|[\tilde{\gamma}]_{k/2} = \chi(d)f$. Then we define $S_{k/2}(\tilde{\Gamma}_0(N), \chi) = S_{k/2}(\tilde{\Gamma}_1(N), \chi) \cap M_{k/2}(\tilde{\Gamma}_0(N), \chi)$, and we get

$$M_{k/2}(\tilde{\Gamma}_0(N)) = \oplus_\chi M_{k/2}(\tilde{\Gamma}_0(N), \chi)$$

Proposition 5.11. *Let $4|N$, $k/2 \in \mathbb{Z}$. Then*

$$M_{k/2}(\tilde{\Gamma}_0(N), \chi) = M_{k/2}(N, \chi_{-1}^{k/2}\chi) \qquad S_{k/2}(\tilde{\Gamma}_0(N), \chi) = S_{k/2}(N, \chi_{-1}^{k/2}\chi$$

5.4 Hecke Operators for half-integral forms

We now extend our theory of Hecke operators for the case of $M_{k/2}$ and discuss a few elegant results. Recall that in the integral case, in the definition of the Hecke operator, we take a sum of the form $\sum f|[\Gamma\alpha\Gamma]_k$ over all double cosets of Γ in Δ^n. Now, if n is squarefree, it turns out that there is only one double coset.

Proposition 5.12. *If n is a positive integer coprime to N which isn't a perfect square, then $f|[\tilde{\Gamma_1}(N)\xi_n\tilde{\Gamma_1}(N)]_{k/2} = 0$*

In the case of half integer weight the only non-trivial Hecke operators are the T_{n^2}. Thus, if we consider modular forms which are eigenfunctions for all of the T_{n^2} we obtain certain formulas relating coefficients whose index differs by a perfect square.

6 The theorems of Shimura, Waldspurger and Tunnell

There exists modular forms of weight 3/2 such that the non-vanishing of the d-th fourier coefficient implies that $E_d(\mathbb{Q})$ is finite. This follows from the following theorems. Firstly, the L-series of the curve E_n is the mellin transform of the image of some (actually several) weight 3/2 form under the Shimura map. Second, the main theorem of Waldspurger shows us that the square of the n-th coefficient of a form of this type is a multiple of $L(E_d, 1)$ where d is n or 2n. Finally, Coates-Wiles gives us our desired result. So, to break things down further, we have:

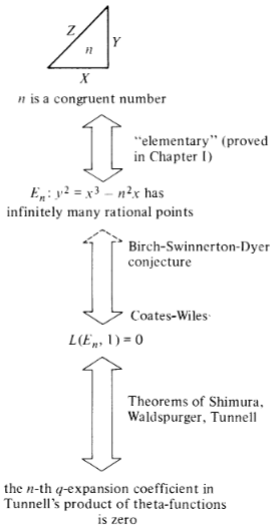
- Shimura proved that if f is a cusp form of weight $k/2$ for k odd greater than 3, and f is an eigenform for T_{p^2} for each prime p (with eigenvalue λ_p), then there exists a form of weight k-1 which is an eigenform with eigenvalue λ_p for T_p for all p. The effect of this map is to square corresponding characters.

- The work of Waldspurger gives us a description of the coefficients of the newform of weight $k-1$ of character χ^2 which is the image of a form of weight $k/2$ under Shimura's map.

- Tunnell describes the basis of the space of cusp forms of weight 3/2 and level 128 which map to forms of weight 2 under Shimura's map

- Tunnell explicitly constructs a modular form of weight 3/2 for $\Gamma_0(128)$ such that the square of the n-th coefficient is a nonzero factor times $L(E_n, 1)$

- Coates-Wiles theorem gives us the conditional two way statement describing when n is in fact a congruent number.



Heuristic "construction" of the argument

6.1 The Shimura map

Theorem 6.1. *Let $k \geqslant 3$ be an odd integer, $N|4$ a positive integer, χ a character mod N and let $f(z) = \sum a_n e^{nz} \in S_{k/2}(N, \chi)$. Let $\lambda = (k-1)/2$. Let d be a positive square-free integer and χ_d the character mod dN defined by*

$$\chi_d(m) = \chi(m) \left(\frac{-1}{m}\right)^{\lambda} \left(\frac{t}{m}\right)$$

Now, define a function $F_d(z)$ by

$$F_d(z) = \sum_{n=1}^{\infty} A_d(n) e^{nz} \text{ where}$$

$$\sum_{n=1}^{\infty} A_d(n) n^{-s} = \left(\sum_{,=1}^{\infty} \chi_d(m) m^{\lambda-1-s}\right) \left(\sum_{m=1}^{\infty} a(tm^2) m^{-s}\right)$$

If f is a common eigen-function for the operators T_{p^2} for all prime factors p of N not dividing the conductor of χ_d. Then, $F_d \in M_{k-1}(N_d, \chi^2)$ for some positive integer N_d. Moreover, if $k \geqslant 5$ then F_d is a cusp form.

As a consequence, this tells us that

6.2 Waldspurger's theorem

We state a less general case of Waldspurger's theorem which suits our needs without getting into all the details of the full theorem.

Theorem 6.2. *Let ϕ be a newform of weight $k-1$ and a characterχ^2 which is the image of a form f of weight $k/2$ under the Shimura map. Assume $16|M$ where M is the level of ϕ. Then there exists a function $A(t)$ from the set of square free integers to $\mathbb{C}$ such that:*

1. $A(t)^2\epsilon(\chi^{-1}\chi_{-1}^{(k-1)/2}\chi_t, 1/2) = 2(2\pi)^{(1-k)/2}\Gamma((k-1)/2)L(\phi\chi^{-1}\chi_{-1}^{(k-1)/2}\chi_t, (k-1)/2)$
2. *For each positive integer N there exists a finite set of explicitly described functions $c(n)$ such that $\sum A(n^{sf})c(n)q^n$ that spans the set of forms of weight $k/2$, level N and character χ which corresponds to ϕ via the Shimura map.*

6.3 Tunnell's work and the CNP

Firstly, it was known to Cohen that the space of forms of weight 3/2 and level 128 for fixed quadratic character is of dimension 3, the same dimension as the space of forms of weight 1/2 and level 128. suggests that we should construct weight 3/2 forms by multiplying forms of weight 1/2 by a weight 1 form g. Consider $\Theta(tz) = \sum q^{tm^2}$, the form of weight 1/2, of level 4t and with character χ_4. From a result of Serre-Stark, we find that $\{\Theta(2z), \Theta(8z), \Theta(32z)\}$ is a basis of forms for the space of 1/2 weight,level 128 and character χ_2. Similarly $\{\Theta(z), \Theta(4z), \Theta(16z)\}$ is a basis for the analogous space with the trivial character. Tunnell now constructs a form g of weight 1, level 128 and character χ_{-2} which allows us to understand the space of 3/2 forms of same level.

Theorem 6.3. *There exists a unique normalized newform g of weight 1, level 128 and character χ_{-2}. Its q-expansion is of the form*

$$g = \sum(-1)^{m+n}q^{(4m+1)^2+16n^2} = \sum(-1)^n q^{(4m+1)^2+8n^2} \qquad (m,n) \in \mathbb{Z}\times\mathbb{Z}$$

Now, one can show that we can rewrite the form g as follows

$$g = (\Theta(z) - \Theta(4z))(\Theta(32z) - \frac{1}{2}\Theta(8z))$$

Theorem 6.4. *The modular forms $g\Theta(2z), g\Theta(4z), g\Theta(8z)$ and $g\Theta(16z)$ correspond to the weight two form ϕ (of level 32, trivial character) under the Shimura map from forms of weight 3/2 to weight 2.*

Theorem 6.5. *Let $g\Theta(2z) = \sum a_n q^n$ and $g\Theta(4z) = \sum b_n q^n$ be modular forms of weight 3/2 and level 128 corresponding to the unique weight 2 normalized newform of level 32 and trivial character. For d square free odd and positive we get*

$$L(E_d, 1) = a(d)^2 \beta \frac{d^{-1/2}}{4}$$

$$L(E_{2d}, 1) = b(d)^2 \beta \frac{(2d)^{-1/2}}{2}$$

where

$$\beta = \int_1^\infty \frac{dx}{(x^3 - x)^{1/2}} \approx 2.62205 \qquad \text{the real period of } E$$

From the two previous results as well as Coates-Wiles theorem, we obtain the main result of the paper. Simply recall that $a(n) = 0$ unless $n \equiv 1, 3 \pmod 8$ and $b(n) = 0$ unless $n \equiv 1, 5 \pmod 8$ and so the L-function vanishes only when $a(n)$ or $b(n)$ are zero. So, if we look the two forms $g\Theta(2z)$ and $g\Theta(4z)$ that we used for the theorem,for n odd their n-th q-expansion coefficient is the same as the n-th coefficient in

$$\Theta(z)(\Theta(32z) - \frac{1}{2}\Theta(8z))\Theta(2z) = \sum_{x,y,z \in \mathbb{Z}} q^{2x^2+y^2+32z^2} - \sum_{x,y,z \in \mathbb{Z}} q^{2x^2+y^2+8z^2}$$

as well as respectively,

$$\Theta(z)(\Theta(32z) - \frac{1}{2}\Theta(8z))\Theta(4z) = \sum_{x,y,z \in \mathbb{Z}} q^{4x^2+y^2+32z^2} - \sum_{x,y,z \in \mathbb{Z}} q^{4x^2+y^2+8z^2}$$

This gives us the original result of Tunnell discussed in 3.4 whenever the forms vanish.

[1] [3] [2] [4] [5]

References

[1] Neal Koblitz. *Introduction To Elliptic Curves And Modular Forms*. Springer-Verlag, 1984. ISBN: 978-1-4684-0255-1.

[2] Goro Shimura. *On modular forms of half-integral weight*. Annals of Math. 97, 1973. ISBN: 440-481.

[3] Joseph H. Silverman. *The Arithmetic Of Elliptic Curves*. Springer-Verlag, 1992. ISBN: 978-0-387-09494-6.

[4] Jerrold B. Tunnell. *A classical Diophantine problem and modular forms of weight 3/2*. Inventiones Math. 72, 1983. ISBN: 323-334.

[5] Benedict Gross Don Zagier. *Heegner points and derivatives of L-series*. Inventiones Math. 84, 1986. ISBN: 225-320.