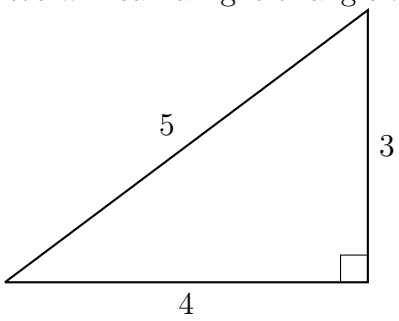
ON TUNNELL'S SOLUTION TO THE CONGRUENT NUMBER PROBLEM

JACK YOSHIKAWA

Abstract. This is a self contained expository paper on the proof of Tunnell's theorem. The goal is to sketch the proof of Tunnell's theorem and give an introduction to the relevant areas of mathematics.

1. Introduction

We will call a right triangle *rational* if all of its sides are rational numbers.



For example, the above right triangle is a rational right triangle because all of the sides are integers.

A natural question to ask is, "What numbers appear as areas of these triangles?" For instance, 6 appears as an area of the above triangle since $\frac{3*4}{2} = 6$. However, if we are given a number like 5, it's quite difficult to find one. We will call numbers that appear as areas of rational right triangles *congruent*.

This question (in its modern form) has been contemplated since at least 1000 C.E., and in other forms since ancient times. For instance, it was known to the tenth-century Persian mathematician Al-Khazin; for more discussion, see [3].

However, only in the 1980s was there a partial resolution by Tunnell to this problem. However, this resolution is dependent on the B. S. D conjecture, which is so hard that a solution is worth one million dollars. This resolution is called Tunnell's theorem. Its statement is deceptively simple.

Theorem 1.1 (Tunnell's theorem)**.** *If*

$$2x^2 + y^2 + 8z^2 = n$$

has twice as many solutions as

$$2x^2 + y^2 + 32z^2 = n$$

with n odd and square-free, then the number n is congruent; if not, then n is not congruent. If n is even and square-free and

$$8x^2 + 2y^2 + 16z^2 = n$$

has twice as many solutions as

$$8x^2 + 2y^2 + 64z^2 = n$$

then n is congruent; if not then n is not congruent.

This paper will be devoted to the exposition of the proof of this theorem. In the first section, we will transform this into a problem about elliptic curves. In the second section, we will cover the basics of elliptic curve theory. In the third section, we will discuss the theory of L-functions. In the fourth section, we will discuss modular forms. Finally, in the last section, we will sketch a proof of Tunnell's theorem.

For a little warm-up, let us prove a small result on congruent numbers: if a number n is congruent, then there is a rational x such that $x^2 \pm n$ is also a square.

2. Transformations

We will try to find a correspondence between rational right triangles of area n and points on a certain elliptic curve.

Theorem 2.1 (congruent numbers to elliptic curves)**.** *Right triangles of area n are in a one-to-one correspondence with solutions to the equation*

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

Proof. We know that integral solutions to the equation

$$X^2 + Y^2 = Z^2$$

are mapped to solutions to the equation

$$(u)^2 + v^2 = 1$$

by setting $u = \frac{X}{Z}, v = \frac{Y}{Z}$. We know that solutions to this equation are parameterized by

$$\left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right)$$

with t an arbitrary rational number. For an arbitrary x, y on the circle, we see that $t = \frac{x}{1-y}$. We thus get:

$$\frac{n}{Z^2} = \frac{X}{Z}\frac{Y}{Z}\frac{1}{2} = uv\frac{1}{2} = \frac{t^2-1}{t^2+1}\frac{2t}{2(t^2+1)} = \frac{t^3-t}{(t^2+1)^2}.$$

Now we set $x = -nt$ and $y = \frac{n^2(t^2+1)}{Z}$. We get that the above equation is:

$$(nt)^3 - n^2(nt) = \frac{n^4(t^2+1)^2}{Z^2}.$$

Now expanding out gets us:

$$n^3(t^3-t) = n^3\frac{(t^3-t)}{(t^2+1)^2}(t^2+1)^2.$$

Thus we can go from any right triangle to a point on this elliptic curve; however, we also want to go in reverse.

We set

$$X = \frac{x^2-n^2}{y} \quad Y = \frac{2nx}{y} \quad Z = \frac{x^2+n^2}{y}.$$

We see that $X^2 + Y^2 = Z^2$ as

$$(\frac{x^2 - n^2}{y})^2 + (\frac{2nx}{y})^2 \ = \ (\frac{x^2 + n^2}{y})^2 \frac{x^4 + n^4 - 2nx + 4nx}{y^2} = \frac{(x^4 + 2nx + n^4)}{y^2}.$$

Now it is clear that

$$\frac{1}{2}XY = \frac{x^2 - n^2}{y}\frac{(2nx)}{y} = \frac{2n(x^3 - n^2x)}{y^2} = \frac{1}{2}2n = n.$$

Thus $\frac{1}{2}XY = n$. To find the point (x, y) given by the (a, b, c) such that $a^2 + b^2 = c^2$ and $\frac{1}{2}ab = n$, we make the substitution $t = \frac{\frac{b}{c}}{1-\frac{a}{c}}$; thus we get that $x = \frac{n(a+c)}{b}, y = \frac{2n^2(a+c)}{b^2}$; this gives us a bijection between the solutions to

$$x^3 - n^2x = y^2.(??)$$

with $y \neq 0$ and solutions to the equation, $a^2 + b^2 = c^2$ and $\frac{1}{2}ab = n$.

□

To show the usefulness of this, let's find the point on $x^3 - 36x = y^2$ given by the $3, 4, 5$ right triangle. As $x = \frac{6(3+5)}{4}, y = \frac{2(6)^2(3+5)}{(4)^2}$, we see that the point $(12, 18)$ should be a solution to the elliptic curve $x^3 - 36x = y^2$; we see that $12^3 = 1728$ and $12 * 36 = 432$; we see that $1728 - 432 = 1296 = 36^2$; thus this is a point on our curve. Moreover, $\frac{12^2-36}{36} = 3$, $\frac{2*6*12}{36} = 4$, and $\frac{12^2+36}{36} = 5$. However, just by exchanging $3, 4$, we instead get a different solution $(18, 72)$, which, when reversed, does indeed give the solution $4, 3, 5$.

3. Elliptic Curves

The curve $x^3 - n^2x = y^2$ is something called an elliptic curve.

Definition 1. An elliptic curve is the set of solutions to the equation $y^2 = f(x)$ and a special "point at infinity," with $f(x)$ a polynomial of the form $x^3 + ax + b$ such that $-16(4a^3 + 27b^2) \neq 0$.

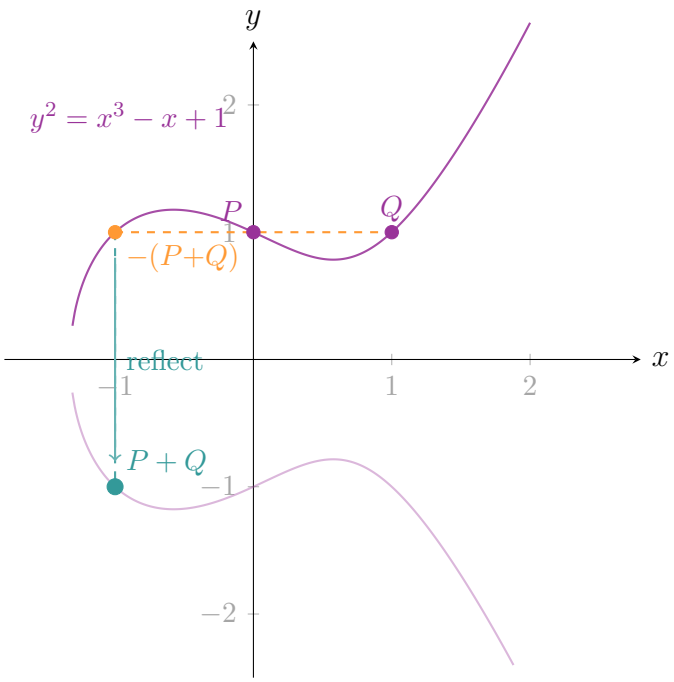
Note we do not mean just over $\mathbb{Q}$.

Example 3.1. *the elliptic curve* $x^3 - x - 1 \equiv y^2 \mod 7$ *is the reduction of an elliptic curve over* $\mathbb{Q}$ *to* $\mathbb{F}_7$*; it is the set of points* $\{\infty, (3, 3), (3, 4), (5, 0)\}$

We know that an elliptic curve has a way to add points. Geometrically, adding two points basically means drawing a line through them to find the third intersection point, and flipping the y coordinate. If the two points are the same, we instead take the tangent line to the point on the curve and find its other intersection point.

If there is not a third intersection point, we say that the addition results in the "point at infinity," which is also the identity element for the group of rational points. This operation forms a group law; for a proof, see, for example, [4].

Below is an example calculation of elliptic curve addition.



While this is a nice picture, it's not really very helpful for actual computation. The actual formula for the addition of two points $(x_1, y_1), (x_2, y_2)$ is $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ on the elliptic curve E with the equation $y^2 = x^3 + ax + b$. The formula for x_3 is $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_3 - x_1) - y_1$, with λ being $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ if they are distinct. If $(x_1, y_1) = (x_2, y_2)$ we set $\lambda = \frac{3x_1^2 + a}{y_1}$. If this requires division by zero, we say that they sum to the identity.

One interesting property that will be useful later is that the group law is defined over $\mathbb{F}_p$; this is fairly clear, since reducing the group law modulo p keeps all of the operations the same. Indeed, if we denote $\overline{x}$ to be the reduction of a point (x, y) on our elliptic curve to a point over $\mathbb{F}_p$, we see that $\overline{p_1 + p_2} = \overline{p_1} + \overline{p_2}$.

This group law makes the set of points over a field K on an elliptic curve E an abelian group, which we denote $E(K)$.

Definition 2 (rank and torsion of an elliptic curve)**.** Since $E(K)$ is an abelian group, we know that it is of the form $T \oplus \mathbb{Z}^r$ with T a finite group, which we call *torsion*. We will also call r the *rank*, though when we say rank, we only mean over $\mathbb{Q}$.

Our goal in the rest of this section is to prove the implication that if n is a congruent number, E_n has rank greater than zero, and vice versa.

As torsion will be the most important concept in the following sections, we will note some important facts about it.

Lemma 1. *The 2-torsion of an elliptic curve is the set of points with y-coordinate equal to zero.*

Proof. As $\frac{3x_1^2 + a}{y_1}$ is undefined when $y_1 = 0$, it goes to the point at infinity. If not, then the addition has a well-defined x- and y-coordinate, so it does not vanish. □

This gives us a set of torsion points for the elliptic curve $x^3 - n^2 x = y^2$, namely $\infty, (n, 0), (0, 0), (-n, 0)$, which are the trivial right triangles for the congruent number problem.

Now we are ready to prove that $rank(E_n) > 0$ is equivalent to n congruent. By the above note, this is equivalent to proving that the points $\infty, (n, 0), (0, 0), (-n, 0)$ are the only

torsion points, since if another point existed, this would imply a nontrivial right triangle and a non-torsion point, so the curve would have rank greater than 0.

By the above discussion of the reduction over $\mathbb{F}_{p^n}$, we see that $x \mapsto \overline{x}$ for $x \in E(\mathbb{Q})$ is a homomorphism, which can be used to find the torsion of an elliptic curve.

Theorem 3.1. $\text{tors}(E_n(\mathbb{Q})) = \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$

Proof. We hope that the reader is comfortable with assuming the following: there exists some N such that for some $p_1, p_2, p_3 \ldots \in \mathbb{P}^n$, if $p_i \neq p_j$ then $\overline{p}_i \neq \overline{p_j} \in \mathbb{F}_{p^n}$. This implies that there is some N such that if $q > N$ then the p torsion should inject into $\text{tor}(E(\mathbb{F}_q))$, since elliptic curves have finite torsion. By Lagrange's theorem, this is an injective map. Thus $\text{tors}(E_q(\mathbb{Q}))|\#E_q(\mathbb{F}_p)$ for infinitely many p.

We now note that if $p \equiv 3 \mod 4$, either $-n$ or n is a square, as if n is a square, then $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \mod p$; if not, this is not one. So we see that $a^{\frac{p-1}{2}} - 1$ has at most $\frac{p-1}{2}$ solutions, and as 0 is already a solution, either x or $-x$ is a square, as if they were both squares, then $a^2 = -b^2$ implies that $-1 = (b\overline{a})^2$, which is impossible, as

$$(-1)^{\frac{p-1}{2}} = (-1)^{2n+1} = (-1) \mod p$$

, so -1 is nonsquare. So we see that either x or $-x$ is a square.

For each $x \in \mathbb{F}_p, x \not\equiv n, 0, -n \mod p$, we consider the pair $(x, -x)$; applying $x^3 - n^2x$ to each pair, we see that $x^3 - n^2x$ takes value $(x^3 - n^2x, -(x^3 - n^2x))$; as one of $x, -x$ is a square, we see that for all pairs exactly one element is of the form y^2. Since $y^2 = (-y)^2 \mod p$, for all of these $\frac{p-3}{2}$ pairs, we have 2 solutions to this equation; thus there are $\frac{p-3}{2}$ possible values of x; however, for each x we see that both $y, -y$ are solutions, so we get $p-3$ solutions. Adding the three solutions where $x^3 - n^2x = 0$, we see that there are p solutions in total; however, there is a single point at infinity that we must add, getting us a full count of $p+1$ solutions when $p \equiv 3 \mod 4$.

Thus, the torsion of $E_n(\mathbb{Q})$ must inject into the torsion of $E_n(\mathbb{F}_q)$, as the torsion of $E_n(\mathbb{F}_q)$ is of cardinality $q+1$; thus $\text{tors}(E_n(\mathbb{Q}))|\,\text{tors}(E_n(\mathbb{F}_q))$. Thus, if the cardinality of the torsion is not equal to any divisor of 4, then by Dirichlet's theorem we know that there is at least one prime p not equal to $-1 \mod d$ and equal to $3 \mod 4$. So $\text{tors}(E_n(\mathbb{F}_q)) \nmid p+1$, which is a contradiction.

We also see that we have the 4 points that we know are torsion points for every prime: $(-n, 0), (n, 0), (0, 0)$ and the point at infinity, since these all have $y = 0$. Thus $E_n(\mathbb{Q})$ has torsion isomorphic to $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$, given by $(-n, 0), (n, 0), (0, 0)$, which are all of the points with $y = 0$. Thus, if there is a rational right triangle of area n, then the elliptic curve $E_n(\mathbb{Q})$ has infinitely many rational points. □

Now you may think that this is a useless result, as the rank seems incomputable; however, we know a lot about the rank of elliptic curves over $\mathbb{Q}$.

4. L-Functions

Now that we see that there is a correspondence between points on certain elliptic curves and congruent numbers, it is natural to ask if there is some way to determine if an elliptic curve has infinitely many rational solutions. Fortunately, there is a conjecture on this subject; it's called the BSD conjecture [2]. In our case, what matters is that there is a function attached to an elliptic curve E, which we denote $L(E, s)$; this is defined as the product over certain

local factors at every prime. $L(E,s)$ can be extended to the entire complex plane. The B.S.D. conjecture relates the value of $L(E,1)$ to the rank of the elliptic curve:

Conjecture 4.1 (Birch and Swinnerton-Dyer)**.** *Let $E(\mathbb{Q})$ be an elliptic curve over $\mathbb{Q}$, let $L(E,s)$ be the L-function of the curve, and let r be the rank of $E(\mathbb{Q})$. Then $\operatorname{ord}_{s=1} L(E,s) = r$. In particular, the rank of the elliptic curve is nonzero if the L-function vanishes at zero.*

Remark. This is not the full conjecture; it actually includes a prediction of the leading Taylor coefficient, but this less strong statement will suffice for our purposes.

To motivate the definition of $L(E,s)$, we will define the following function for a set of polynomial equations V. Given a set of polynomial equations V, we denote the set of solutions in $\mathbb{F}_{p^n}$ as $V(\mathbb{F}_{p^n})$.

Definition 3 ($\zeta(V,s)$)**.** We define the local zeta function at prime p to be:

$$Z_p(V,x) = \exp\left(\sum_{n>0} \frac{|V(\mathbb{F}_{p^n})|x^n}{n}\right).$$

We also define

$$\zeta(V,s) = \prod_{\text{p prime}} Z(V,p^{-s}).$$

For the elliptic curve case, it turns out that $Z_p(E,x)$ is easy to compute for any elliptic curve; in fact, it is of the form

$$\frac{(1-a_pt+qt^2)}{(1-t)(1-qt)}.$$

Due to this, we can actually compute a_p.

Theorem 4.1.

$$a_p = p+1-|E(\mathbb{F}_p)|$$

Proof. We know that

$$\frac{(1-a_pt+qt^2)}{(1-t)(1-qt)} = \exp(\ln(1-\alpha t)+\ln(1-\overline{\alpha}t)-\ln(1-t)-\ln(1-qt)).$$

Recalling the Taylor expansion for

$$\ln(1-x)$$

, we see that this series is equivalent to

$$\sum \frac{(p^n+1-(\alpha^n+\overline{\alpha}^n))}{n}x^n.$$

Evaluating this expression at $n=1$, we see that $-(\alpha+\overline{\alpha})+p+1 = |E(\mathbb{F}_p)|$. As $\alpha+\overline{\alpha}=a$, we get that

$$a_p = p+1-|E(\mathbb{F}_p)|$$

□

We thus see that the number of solutions to an elliptic curve E over $\mathbb{F}_p$ determines the zeta function $Z_p(E,s)$; moreover, the zeta function has a trivial bottom part, which would be nice to discard. Luckily, using our previous definitions, we see that $\zeta(E,s) = \frac{\zeta(s)\zeta(s-1)}{L(E,s)}$ with $\zeta(s)$ being the Riemann zeta function. This allows us to throw away the trivial part of the solution count.

We will now compute the L-function for E_n.

We know that for our curve, if we multiply y by $n\sqrt{n}$, getting us

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

, setting $x = nx$ gets us $n^3y^2 = n^3x^3 - n^3x$; thus $y^2 = x^3 - x$. The multiplication of y by $\sqrt{n}$ is called a quadratic twist. It is clear that if $\sqrt{n}$ exists modulo p, the solution count of the curve $y^2 = x^3 - n^2x$ is the same as $y^2 = x^3 - x$. For the case where n^2 does not exist modulo p, we see that our elliptic curve is equal to:

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

or

$$y^2 = n(x^3 - x).$$

If there was exactly one value of y for every x, then there would be $p+1$ solutions; however, if x is a square $\mod p$, it contributes an extra 1 to the count, as there are two possible values of y, and if x is not a square, it removes one possible value of x. Let's call this function $\frac{a}{p}$; summing over all $x^3 - n^2x$, we see that $a_p = -\sum_{\mathbb{F}_p}(\frac{n(x^3-x)}{p})$.

Definition 4. we call a function from $\chi : (\frac{\mathbb{Z}}{n\mathbb{Z}})^\times \to \mathbb{C}^*$ a character if $\chi(ab) = \chi(a)\chi(b)$.

Theorem 4.2. *The function given by $(\frac{a}{p}) = 1$ if $a \equiv n^2 \mod p$ for some $n \in \mathbb{F}_p$, and $(\frac{a}{p}) = -1$ if $a \not\equiv n^2 \mod p$ for some $n \in \mathbb{F}_p$, or 0 if $n = 0$, is equal to $a^{\frac{p-1}{2}} \mod p$ and is a character.*

Proof. We first will prove that $\chi(a) \equiv a^{\frac{p-1}{2}} \mod p$. $b^{\frac{p-1}{2}}$ is equal to one on any square, as if $a = b^2$, then $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \mod p$ by Fermat's little theorem. As there are $\frac{p-1}{2}$ squares $\mod p$, we see that $x^{\frac{p-1}{2}} - 1 \equiv 0$ has at least $\frac{p-1}{2}$ solutions mod p, as an equation of degree d must have at most d solutions mod p by Lagrange's theorem. We see that if $a \in \mathbb{F}_p$ is nonsquare, then $\chi(a) \neq 1$, as if it were, then $x^{\frac{p-1}{2}} - 1 \equiv 0$ would have more than $\frac{p-1}{2}$ solutions, which contradicts Lagrange's theorem. As $(x^{\frac{p-1}{2}})^2 \equiv x^{p-1} \equiv 1 \mod p$ if $x \in \mathbb{F}_p^\times$, we see that $\chi(a)^2$ must equal one for all a in $\mathbb{F}_p^\times$; thus $\chi(a) \equiv \pm 1$. As $\chi(a)$ cannot equal one when a is nonsquare, $\chi(a) \equiv -1$. We thus see that $\chi(a) \equiv a^{\frac{p-1}{2}} \mod p$. Thus $\chi(ab) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \times b^{\frac{p-1}{2}} \equiv \chi(a)\chi(b) \mod p$, so $\chi(a)$ is clearly multiplicative and thus a character. We denote $\chi(a) = (\frac{a}{p})$ for the rest of this paper. For more information, see [1]. □

By the discussion before the definitions, we get that $a_{p,n} = -\sum_{x\in\mathbb{F}_p}(\frac{n(x^3-x)}{p}) = (\frac{n}{p})a_{p,1}$.

Remark. The astute reader may notice that this curve is not always an elliptic curve; sometimes it gains a "kink" at some prime numbers; at these points we say that the local factor is one.

Now we compute the local factor for the elliptic curve $x^3 - x = y^2$.

Theorem 4.3. *For any point on the curve $E : x^3 - x = y^2$ not equal to $(0, 0)$, there exists a point on the curve $E' : u^2 = v^4 + 4$; and for any point on the curve $u^2 = v^2 + 4$, there is a point on the curve $x^3 - x = y^2$ not equal to the point at infinity or $(0, 0)$.*

Proof. Given a point on the curve $u^2 = v^4 + 4$, we consider the point

$$(\frac{1}{2}(u+v^2), \frac{1}{2}v(u+v^2))$$

as

$$\frac{1}{2}(u+v^2) + \frac{1}{2^3}(u+v^2)^3 = (\frac{1}{2}v(u+v^2))^2,$$

expanding, which gets us:

$$\frac{1}{2}(u+v^2)(\frac{1}{2^2}(u+v^2)^2 - 1) = (\frac{1}{2}v(u+v^2))^2.$$

As:

$$\frac{1}{2^2}(u+v^2)^2 - 1 = (u^2 + v^4 - 4 + 2uv^2)\frac{1}{4} = (2v^4 + 2uv^2)\frac{1}{4}$$

Thus the full summation is:

$$\frac{u^2}{4}(v^2+u)(v^2+u)$$

which is the left-hand side as desired.

We also see that

$$(2x - \frac{y^2}{x^2})^2 = (\frac{y}{x})^4 + 4 \tag{1}$$

$$4x^2 - \frac{4xy^2}{x^2} + \frac{y^4}{x^4} = \frac{y^4}{x^4} + 4 \tag{2}$$

$$\frac{4x(x^3 - y^2)}{x^2} + \frac{y^4}{x^4} = \frac{y^4}{x^4} + 4 \tag{3}$$

$$4 + \frac{y^4}{x^4} = \frac{y^4}{x^4} + 4 \tag{4}$$

Thus, we see that there is a correspondence between nonzero solutions to the elliptic curve with $x \neq 0$ and solutions to the equation $u^2 = v^4 + 4$, which we denote E'. □

If $x = 0$, then there is a single solution to the equation $y^2 = x^3 - n^2x$, namely $y = 0$; thus the number of solutions to E' is equal to the number of solutions to E minus one. However, we actually include the "point at infinity," adding an extra one to our count. Thus $\#(E(\mathbb{F}_p)) = \#(E'(\mathbb{F}_p)) + 2$. We can use this to re-prove our formula for $|E_n(\mathbb{F}_p)|$ when p is equal to 3 modulo 4. Since $p - 1 \neq m^2 \mod p$, we see that $\chi(p-1) = -1$; thus $\chi((p-1)x) = \chi(p-1)\chi(x)$; thus either $\chi(x)$ or $\chi((p-1)x)$ is one, and the other is -1; thus all numbers are of the form $\pm m^2 \mod p$; thus, every square is a 4th power. Thus, we now count solutions to the equation $u^2 + 4 = v^2$: there are clearly $p-1$ solutions to this equation, given by $(u-v)(u+v) = (u)(u+2v)$, as we may set u, v to be arbitrary. We set u as a free parameter not equal to zero and v equal to $\overline{2}(4\overline{u} - u)$, which is well-defined for $u \neq 0$; thus there are $p-1$ solutions to this equation when $p \equiv 3 \mod 4$, so we see that $a_p = 0$.

Theorem 4.4. *If $p \equiv 1 \mod 4$, then $p = \pi\overline{\pi}$ with π a prime in $\mathbb{Z}[i]$ such that $\pi \equiv 1 \mod 2 + 2i$; then $a_p = \pi + \overline{\pi}$.*

Proof. When $p \equiv 1 \mod 4$, we see that the number of solutions to E is equal to

$$2 + \sum_{r+s=4} (N(u^2 = r)N(v^4 = -s)),$$

with $N(a^n = b)$ being the number of solutions to the equation $a^n = b$. Via some character theory, we know that $N(u^2 = r) = \lambda^2 + 1$ with λ being a character of order 4; moreover, $N(u^4 = r) = \lambda(r) + \lambda^2(r) + \overline{\lambda(r)} + 1$. We thus see that $(\lambda^2(a)+1)(\lambda(r)+\lambda^2(r)+\overline{\lambda(r)}+1) = \lambda(r)+\lambda^2(r)+\overline{\lambda(r)}+1+\lambda(r)\lambda^2(a)+\lambda^2(r)\lambda^2(a)+\overline{\lambda(r)}\lambda(a)+\lambda^2(a)$. We know that the sum of any nontrivial Dirichlet character over all $x \mod p$ is equal to zero, so this full sum collapses into

$$p + 2 + \sum_{a+s=4} \lambda^2(a)\lambda^2(-s) + \sum_{a+s=4} \lambda^2(a)\lambda(-s) + \sum_{a+s=4} \lambda^2(a)\overline{\lambda}(-s).$$

Since $-s^2 \equiv (is)^2 \mod p$ with $p \equiv 1 \mod 4$, we see that the first sum is just $\sum_{a+s=4} \lambda^2(a)\lambda^2(s)$; moreover, since all $a, s = 4x, 4y$, this is equivalent to

$$\sum_{x+y=1} \lambda^2(y)\lambda^2(x)\lambda(4)^4 = \sum_{x+y=1} \lambda^2(y)\lambda^2(1-y).$$

The sum above is called a *Jacobi sum*, which is a sum of the form $J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$.

By [1], Chapter 8, Section 3, Theorem 1, the above sum is -1. We thus get that

$$p + 1 + \sum_{a+s=4} \lambda^2(a)\lambda(-s) + \sum_{a+s=4} \lambda^2(a)\overline{\lambda}(-s),$$

so

$$a_p = \sum_{a+s=4} \lambda^2(a)\lambda(-s) + \sum_{a+s=4} \lambda^2(a)\overline{\lambda}(-s).$$

Using the same trick as before, we see that $a_p = \overline{\lambda(-4)}J(\lambda, \lambda^2) + \lambda(-4)J(\overline{\lambda}, \lambda^2)$ by Ireland and Rosen, Proposition 9.94, and since 4 is a square modulo all primes, we see that if $p = \pi\overline{\pi}$ with π a prime in $\mathbb{Z}[i]$, we choose π uniquely such that $\pi \equiv 1 \mod 2+2i$; then $a_p = \pi + \overline{\pi}$. $\square$

This implies that $1 - a_p p^s + p^{1-2s} = (1 - \pi p^s)(1 - \overline{\pi} p^s)$, given that $p \equiv 1 \mod 4$. Thus, every Euler factor can be broken up into $\frac{1}{1-a_p p^s (E_1)+p^{1-2s}} = \prod_{\mathfrak{p}|p, \mathfrak{p}\in\mathbb{Z}[i]} \frac{1}{1-\alpha_{\mathfrak{p}} N(\mathfrak{p})^{-s}}$, with $\alpha_{\mathfrak{p}}$ being equal to the unique generator of $\mathfrak{p}$ such that $\alpha \equiv 1 \mod 2 + 2i$. We thus see that $a + bi = \alpha_p$, with $a^2 + b^2 = p$, with a odd, as $\overline{a + bi} \equiv 1 \mod 2 + 2i$.

Thus we see that $\prod_{\mathfrak{p}|P}(\frac{1}{1-\alpha_{\mathfrak{p}} N(\mathfrak{p})^s}) = \frac{1}{1-a_p p^s + p^{1-2s}}$, as either $p = a^2 + b^2$ or p does not split. In this case, only $p|p$, and $N(p) = p^2$, and $\alpha_p = -p$, as $-p$ is equal to $-(2 + 2i)(1 - i)^{\frac{p+1}{2}} + 1$. In the split case, we see that $p \equiv 1 \mod 4$ and that $p = (a + bi)(a - bi)$; we see that $N(a + bi) = p, N(a - bi) = p$, so we see that our product is $\frac{1}{1-(a+bi)p^{-s}} \frac{1}{1-(a-bi)p^{-s}} = \frac{1}{1-(a+bi+a-bi)p^{-s}+p^{-2s}(a^2+b^2)} = \frac{1}{1-2ap^{-s}+p^{-2s}}$. Thus we get our desired result.

Now, as $(\frac{a}{N(p)})^2 = 1$, we can simply add that in as a factor and get that this full product is: $L(E_n, s) = \prod_{\mathfrak{p}\in\mathbb{Z}[i]} \frac{1}{1-(\frac{n}{N(\mathfrak{p})})\alpha(\mathfrak{p})N(\mathfrak{p})^{-s}}$, as all prime ideals in $\mathbb{Z}[i]$ divide primes in $\mathbb{Z}$; we see that the above product is indeed valid. Now, for an ideal of $\mathbb{Z}[i]$, we will see that $\alpha(I) = \overline{I} \mod 2 + 2i$, and as $\frac{\mathbb{Z}[i]}{(2+2i)\mathbb{Z}[i]}$ is clearly a group, we see that $\alpha(I)$ is clearly multiplicative, as $\overline{ab} = \overline{a}\overline{b}$.

Since α_n is clearly dependent only on what n is modulo $2 + 2i$, adding the character $(\frac{n}{N(x)})\psi(x) = \chi'_n(x)$ does not really change much besides what modulus we are working with. Given a number, the product of these two characters depends only on the norm of x modulo n. For more discussion of the character theory, see [2] and [1].

Combining the two turns out to depend only on $x \mod n(2 + 2i)$ if n is even, or $x \mod (2n)$ otherwise. We denote this period n'. We denote $N = 4|n'|^2$; now we will prove

that the L-function has a functional equation. Before proving this theorem, we will do some complex analysis.

Definition 5 (Mellin transform)**.** We call

$$\mathcal{M}(f(x))(s) = \int_0^\infty x^{s-1} f(x) dx$$

the "Mellin transform" of $f(x)$.

We know that

$$\mathcal{M}(f(mx))(s) = m^{-s} \int_0^\infty x^{s-1} f(x) dx.$$

The proof of this is as follows:

Proof. We know that

$$\mathcal{M}(f(mx))(s) = \int_0^\infty x^{s-1} f(xm) dx = \frac{1}{m} \int_0^\infty m(\frac{xm}{m})^{s-1} f(xm) dx = \frac{1}{m^s} \int_0^\infty x^{s-1} f(x) dx.$$

Thus $\mathcal{M}(f(mx))(s) = \frac{1}{m^s} \mathcal{M}(f(x))(s)$. □

Also $\mathcal{M}(e^{-x}, s) = \Gamma(s)$, which is the generalization of $(n-1)!$ to non-integer arguments. We also need the formula:

Definition 6 (Fourier transform for $\mathbb{R}^2$)**.** we denote

$$\mathcal{F}(y) = \int_{\mathbb{R}^2} f(x) e^{-2\pi i x \cdot y} dx$$

which is a Fourier transform for $\mathbb{R}^2$.

which has the following properties:

$$\mathcal{F}(e^{-\pi |x|^2}) = e^{-\pi |x|^2} \tag{5}$$

$$\mathcal{F}(g(ax))(s) = a^{-2} \mathcal{F}(g(x))(\frac{s}{b}) \tag{6}$$

$$\mathcal{F}(f(x+a))(s) = e^{2\pi i a \cdot s} \mathcal{F}(f(x))(s) \tag{7}$$

$$\mathcal{F}(f(x) e^{2\pi i x \cdot a}) = \mathcal{F}(f(x))(s-a) \tag{8}$$

$$\mathcal{F}(a \cdot \frac{\partial}{\partial x} f(x))(s) = 2\pi i w \cdot s \mathcal{F}(f(x))(s) \tag{9}$$

Here $w \cdot \frac{\partial}{\partial x}$, with $w = c_0 x + c_1 y$, is just $c_2 \frac{\partial f}{\partial x} + c_1 \frac{\partial f}{\partial y}$; the proof of (1) is difficult, and we refer the reader to [2]. (2)–(4) are simply consequences of the linearity of the dot product and multivariate substitution; (5) is just integration by parts, due to linearity in one variable. We also need the following proposition.

Proposition 4.1 (Poisson summation)**.** Poisson summation:

$$\sum_{m \in \mathbb{Z}^2} f(m) = \sum_{m \in \mathbb{Z}^2} \mathcal{F}(f)(m)$$

The main use of the above propositions is to motivate the following theorem. The idea of the proof is to expand the function $\sum_{m\in\mathbb{Z}^2} f(m)$ as a Fourier series.

For more discussion, see [2]. We now define for $u \in \mathbb{R}^2$

$$\theta_u(t) = \sum_{m\in\mathbb{Z}^2} (m+u)\cdot(1,i)e^{-\pi t(|m+u|^2)}$$

and

$$\theta^u(t) = \sum_{m\in\mathbb{Z}^2} (m)\cdot(1,i)e^{2\pi i m\cdot u}e^{-\pi t(|m+u|^2)}$$

We define $g_u(x) = (x+u)\cdot(1,i)e^{-\pi t(|x+u|^2)}$ with $f(x) = e^{-\pi x\cdot x}$; $g_u(x) = \frac{-1}{2\pi t}((1,i)\cdot\frac{\partial}{\partial x})f(\sqrt{t}(x+u))$; unwrapping the definition gets us: $\mathcal{F}(g(x))(s) = -it^{-2}(1,i)\cdot me^{2\pi iu\cdot s}e^{-\frac{\pi}{t}|s|^2}$ We see that

$$\theta_u(t) = \sum_{m\in\mathbb{Z}^2} (m+u)\cdot(1,i)e^{-\pi t(|m+u|^2)} =$$

$$\sum_{m\in\mathbb{Z}^2} g(m) = \sum_{m\in\mathbb{Z}^2} \mathcal{F}(g)(m) =$$

$$\sum_{m\in\mathbb{Z}^2} -it^{-2}(1,i)\cdot me^{2\pi iu\cdot m}e^{-\frac{\pi}{t}|m|^2} =$$

$$-it^{-2}\sum_{m\in\mathbb{Z}^2} w\cdot me^{2\pi iu\cdot s}e^{-\frac{\pi}{t}|m|^2} = -it^{-2}\theta^u(\frac{1}{t})$$

Moreover,

Theorem 4.5.

$$\mathcal{M}(\theta_u(t))(s) = \pi^s\Gamma(s)\sum\frac{(m+u)\cdot(1,i)}{|m+u|^{2s}}$$

Proof.

$$\mathcal{M}(\theta(t))(s) = \int_0^\infty \sum_{m\in\mathbb{Z}^2}(m+u)\cdot(1,i)e^{-\pi t(|m+u|^2)}t^{s-1}dt = \sum_{m\in\mathbb{Z}^2}\int_0^\infty (m+u)\cdot(1,i)e^{-\pi t(|m+u|^2)}t^{s-1}dt = \sum_{m\in\mathbb{Z}^2}(m+$$

this is the same thing that appeared in the above theorem; thus we get the desired result. □

Now this may seem unmotivated; however, the point of this is to find functions that are related to our L-function that have good symmetries.

Theorem 4.6. *Now we will prove that* $\Lambda(2-s, E_n) = \Lambda(s, E_n)$*, with* $\Lambda(s, E_n) = (\frac{|N|}{2\pi})^{\frac{s}{2}}\Gamma(s)L(E_n, s)$.

Proof. We now write out the $L(E_n, s)$ function as

$$\frac{1}{4}\sum_{a+bi\in\mathbb{Z}[i]}\frac{\chi'(a+bi)(a+bi)}{N(a+bi)^s} = \sum_{0\le a,b<4n}\chi'(a+bi)\sum_{m\in\mathbb{Z}^2}\frac{(a+bi+4nm\cdot w)}{|(a,b)+4nm|^{2s}}$$

with $w = (1,i)$; this is:

$$\frac{(4n)^{1-2s}}{4}\sum_{0\le a,b<4n}\chi'(a+bi)\sum_{m\in\mathbb{Z}^2}\frac{((\frac{a}{4n},\frac{b}{4n})+m)\cdot w}{|((\frac{a}{4n},\frac{b}{4n})+m)\cdot w|^{2s}}$$

We thus get by the previous discussion

$$\pi^{-s}\Gamma(s)L(E_n,s)=\frac{(4n)^{1-2s}}{4}\sum_{0\leq a,b<4n(0,0)\neq(a,b)}\chi'(a+bi)\int_0^\infty t^{s-1}\theta_{\frac{a}{4n},\frac{b}{4n}}(t)dt$$

The function inside the integral is an entire function in s, so we do get a well-defined value at one; we now get the functional equation for the L-function.

We will now hyperfocus on the integral:

$$\int_0^\infty t^{s-1}\theta_{\frac{a}{4n},\frac{b}{4n}}(t)dt$$

By the functional equation given above, this is:

$$-i\int_0^\infty t^{s-3}\theta^{\frac{a}{4n},\frac{b}{4n}}(\frac{1}{t})dt$$

Then, after changing variables, we finally get:

$$\int_0^\infty t^{3-s}\theta^{\frac{a}{4n},\frac{b}{4n}}(t)dt=\pi^{s-2}\Gamma(s-2)\sum_{m\in\mathbb{Z}^2}m\cdot(1,i)\frac{e^{(\frac{2\pi i}{4n}(a,b))\cdot m}}{|m\cdot(1,i)|^{2(2-s)}}$$

Thus, as a full sum, we get that this is equal to

$$S_m=\sum_{0\leq a,b<4n}e^{(\frac{2\pi i}{4n}(a,b))\cdot m}\chi'(a+bi)$$

We refer the reader to [2] for more discussion of this sum; what matters here is that it's $\chi'(m)(\frac{-2}{n})n'$.

$$4\left(\frac{-2}{n}\right)(1+i)2^{s-1}(2+2i)nL(E_n,2-s)$$

combining everything together gets us:

$$(\frac{-2}{n})\pi^{s-2}\Gamma(2-s)(8n^2)^{1-s}L(E_n,2-s)$$

Thus balancing terms gets us that $(\frac{\sqrt{32}n}{2\pi})^{\frac{s}{2}}\Gamma(s)L(E_n,s)=(\frac{\sqrt{32}n}{2\pi})^{\frac{1-s}{2}}\Gamma(1-s)L(E_n,1-s)$ as desired.

□

Now going back to the proof once again, one interesting thing is that we can combine the θ_u together to get a function whose Mellin transform is $\pi^{-s}\Gamma(s)L(E_n,s)$; we see that

$$\pi^{-s}\Gamma(s)L(E_n,s)=\frac{(n')}{4}\int_0^\infty\sum_{a+bi\in\mathbb{Z}[i]/n'(0,0)\neq(a,b)}\chi'(a+bi)t^{s-1}\theta_{\frac{a}{4n},\frac{b}{4n}}(N't)dt$$

If we denote the inner sum to be $F(t)$, expanding and switching orders of summation, we see that $F(\frac{1}{N't})=\sum_{a+bi\in\mathbb{Z}[i]/n'(0,0)\neq(a,b)}\chi'(a+bi)\theta_{\frac{a}{4n},\frac{b}{4n}}(\frac{1}{t})$; using the functional equation for $\theta_u(t)$ along with some rewriting gets us:

$$-\frac{it^2n'}{4}\sum_{m\in\mathbb{Z}^2}m\cdot(1,i)e^{-\pi t|m|^2}\sum_{a+bi}\chi'(m_1+m_2i)\chi'(a+bi)e^{\mathrm{Re}\,(\frac{(a+bi)}{n'})}=-\frac{it^2(n')^2}{4}(\frac{-2}{n})\sum_{m\in\mathbb{Z}^2}\tilde{\chi}(m\cdot(1,i))e^{|m|^2}$$

with n odd; for the even case with $n=2n_0$, the same thing is true, and the factor is just equal to $F(E_n,\frac{1}{n_0})=t^2(\frac{-1}{n_0})|n'|^2F(E_n,t)$; thus, at the end of the day, we see that this function

satisfies a very peculiar transformation property, and we can compute the value of $L(E_n, s)$ at $s = 1$.

We shall analyze this function and more functions like this in the next chapter.

5. Modular Forms

It turns out that the function that we have computed is in fact something called a modular form. To define a modular form, we need a lot of difficult machinery. First, we consider the set of 2×2 matrices over $\mathbb{Z}$; we define

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, ad - bc = 1 \right\}$$

Definition 7 (congruence subgroup)**.** One important subgroup of $\mathrm{SL}_2(\mathbb{Z})$ is the subgroup (which we denote $\Gamma(N)$) which is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), a \equiv d \equiv 1 \mod N, b \equiv c \equiv 0 \mod N \right\} \tag{10}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), a \equiv d \equiv 1 \mod N, c \equiv 0 \mod N \right\} \tag{11}$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), c \equiv 0 \mod N \right\} \tag{12}$$

We say a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup if it contains $\Gamma(N)$ for some $N \in \mathbb{N}$.

A congruence subgroup H is said to have weight N if $\Gamma(N) \subseteq H$ but $\Gamma(k) \nsubseteq H$ for all $k < N$.

Definition 8. A modular form of weight k and level N is a function such that for $\gamma \in \mathrm{GL}_2(z)$, $f(z)|[\gamma]_k = \det(\gamma)^{\frac{k}{2}}(cz + d)^{-k} f(\gamma z)$, by $\gamma z = \frac{az+b}{cz+d}$, with γ having all coefficients in $\mathbb{Z}$. A modular form is a series of the form: $f(z) = \sum_{n=1}^{\infty} a_n q_N^n$ with $q = e^{\frac{2\pi i z}{N}}$ such that $f(z)|_\gamma = f(z)$ for $\gamma \in \Gamma_1(N)$ and $f(z)|_{\gamma_0} = \sum_{n=1}^{\infty} a_n q_N^n$

for all $\gamma_0 \in \mathrm{SL}_2(\mathbb{Z})$. This also clearly forms a space. We also define a modular form of weight k and level N with character χ to be one that satisfies the transformation property $f(z)|_\gamma = \chi(d) f(z)$ for $\gamma \in \Gamma_0(N)$. Modular forms allow us to basically prove the functional equation again with much less difficulty. Given a modular form m of level N and character χ with a q-expansion given by

$$\sum_{n=1}^{\infty} c_n q^n,$$

by the same logic we used to compute the inverse Mellin transform of a Dirichlet series, the Mellin transform of m, shifted to the imaginary axis, is equal to $D(s) = \Gamma(s)(-2\pi i)^{-s} \sum_{n=1}^{\infty} \frac{a_n}{n^s}$. It turns out that it can be written as the sum of two functions f, g satisfying $f|_{\alpha_N} = Ci^{-k} f(z)$ with $C = 1$ for f and -1 for g, and with $\alpha_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. Given that a function satisfies this transformation property, we see that $f(\frac{1}{Nz}) = CN^{-\frac{k}{2}}(-iNz)^k f(z)$. Thus,

$$\mathcal{D}(s) = \int_0^{i\sqrt{N}} f(x) x^{s-1} ds + \int_{i\sqrt{N}}^{i\infty} f(x) x^{s-1} ds.$$

Applying the transformation, changing variables, and rearranging gets us that

$$\mathcal{D}(s) = \int_{i\sqrt{N}}^{\infty} (f(z)z^s + i^k C N^{-\frac{k}{2}} f(z)(\frac{-1}{Nz})^{s-k})\frac{1}{z}dz.$$

Replacing k by $k-s$ gets us:

$$\mathcal{D}(k-s) = \int_{i\sqrt{N}}^{\infty} (f(z)z^{k-s} + i^k C N^{-\frac{k}{2}} f(z)(\frac{-1}{Nz})^{-s})\frac{1}{z}dz = \tag{13}$$

$$i^k C N^{-\frac{k}{2}}(-N)^s \int_{i\sqrt{N}}^{\infty} (f(z)z^s + i^k C N^{-\frac{k}{2}} f(z)(\frac{-1}{Nz})^{s-k})\frac{1}{z}dz = \tag{14}$$

$$i^k C N^{-\frac{k}{2}}(-N)^s \mathcal{D}(s) \tag{15}$$

thus we see that $\mathcal{D}$ has both an analytic continuation and a functional equation, exactly what we want from an L-function. For more information, see [2]. The other thing that we need to know is the following definition: Hecke operators.

Definition 9 (Hecke operators)**.** A Hecke operator is an operator on the space of modular forms of level N and character χ, which we denote $T_n f(z)$. Given a modular form in this space with q-expansion $\sum_{m=1}^{\infty} c_m q^m$, we have $T_n f(z) = \sum_{m=1}^{\infty} b_m q^m$ with $b_m = \sum_{d|\gcd(m,n)} c_{\frac{mn}{d^2}} d^{k-1}\chi(d)$.

While this may look like a horrible operator to work with, it does have some redeemable qualities. For example,

Theorem 5.1. *$T_m T_n(f(z)) = T_{mn}(f(z))$, given that* $\gcd(m,n) = 1$.

Proof. Given that

$$f(z) = \sum_{k=1}^{\infty} c_j q^j$$

is an arbitrary modular form of character χ, weight k, and level N, and given that

$$T_m T_n(f(z)) = \sum_{k=1}^{\infty} b_k q^k,$$

we will find b_j in terms of c_j. As the fth coefficient of $T_m(f(z))$ is

$$T_n(f(z)) = \sum_{d|\gcd(n,f)} c_{\frac{n\cdot f}{d^2}} d^{k-1}\chi(d),$$

so, using the formula for the Hecke operators, we see that

$$T_m(T_n f(z)) = \sum_{f|\gcd(m,j)} \chi(f) f^{k-1} \sum_{d|\gcd(n,\frac{m\cdot j}{f^2})} c_{\frac{n\cdot mj}{f^2 d^2}} d^{k-1}\chi(d).$$

We now bring everything inside of the summation and get

$$\sum_{f|\gcd(m,j)} \sum_{d|\gcd(n,\frac{m\cdot j}{f^2})} c_{\frac{n\cdot mj}{f^2 d^2}} (fd)^{k-1}\chi(fd).$$

We see that the gcd condition on the inner sum is equivalent to $d|\gcd(n, \frac{j}{f} \times \frac{m}{f})$; as $\gcd(n, \frac{m}{f}) = 1$, we see that this second gcd can be split off; thus, we get that $fd|\gcd(mn, j)$. Rewriting in terms of $fd = x$ gets us:

$$T_m T_n f = \sum_{x|\gcd(mn,j)} c_{\frac{n\cdot mj}{x^2}}(x)^{k-1}\chi(x) = T_{mn} f.$$

Thus $T_{mn} = T_m \circ T_n$. □

We especially care about modular forms such that $T_m(f(z)) = \lambda_m f(z)$. We note that $T_{p^n} f = T_{p^{n-1}} \circ T_p f - pn^{k-2}\chi(p)T_{p^{n-2}} f$; we call these forms eigenforms. Since $T_{mn} f(z) = T_m T_n f(z)$, we see that $\lambda_{mn} = \lambda_m \lambda_n$. By the above transformation law, we see that the λ_m expand into a series like so: $\sum \frac{\lambda_n}{n^s} = \prod_p \frac{1}{1-\lambda_p p^s + \chi(p)p^{k-1-2s}}$. For more discussion on Hecke eigenvalues and eigenforms, see [2].

6. Tunnell's Theorem

Theorem 6.1 (Shimura's theorem)**.** *Given an eigenform of weight k with Hecke eigenvalues $T_{p^2}(f) = \lambda_p f$, we see that $\sum_{n=1}^{\infty} a_n q^n \in S_{\frac{k}{2}}(\tilde{\Gamma}_0(N), \chi)$; and let $\sum_{n=1}^{\infty} \frac{b_n}{n^s} = \prod(\frac{1}{1-\lambda_p p^{-s} + \chi(p)^2 p^{k-2-2s}})$. We see that*

$$\sum_{n=1}^{\infty} b_n q^n$$

is a form of weight $k-1$ of character χ^2.

Theorem 6.2 (Waldspurger's theorem)**.** *$a(t) = \beta_1^2 A(t) n^{\frac{1}{4}}$ if $t \equiv 1 \mod 8$ and $a(t) = \beta_3^2 A(t) n^{\frac{1}{4}}$. Thus: $a(n) = \beta_1^2 L(E_n, 1) n^{\frac{1}{2}}, a(n) = \beta_3^2 L(E_n, 1) n^{\frac{1}{2}}$; otherwise, $L(E_n, 1) = 0$.*

With $a(t)$ being coefficients of a set of modular forms

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

with t odd, when t is even, we just use a different set of modular forms. However, the most important thing is that these modular forms have series $\sum a_n q^n$ with a_n being equal to $\sum_{n=32z^2+2x^2+y^2} 1 - \frac{1}{2}\sum_{n=8z^2+2x^2+y^2} 1$, so if a_n vanishes, then $L(E_n, 1)$ vanishes, and vice versa. Thus, we conclude Tunnell's theorem.

References

[1] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. 2nd. Vol. 84. Graduate Texts in Mathematics. New York, NY: Springer, 1990. ISBN: 978-0-387-97329-6. DOI: 10.1007/978-1-4757-1779-2.

[2] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms*. 2nd. Vol. 97. Springer Science & Business Media, 1993.

[3] Norbert Schappacher. *Diophantus of Alexandria: A text and its history*. Unprinted manuscript available via IRMA Université de Strasbourg. 1998. URL: https://irma.math.unistra.fr/~schappa/NSch/Publications_files/1998cBis_Dioph.pdf.

[4] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd ed. Vol. 106. Graduate Texts in Mathematics. New York, NY: Springer, 2009. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6.