Ramanujan's Ternary Quadratic Form

Frank Thorne

October 24, 2005

Primary Reference:

Ono, Ken and K. Soundararajan. *Ramanujan's Ternary Quadratic Form.* Inventiones Mathematicae, 130, 3, 1997, pp. 415-454.

Other references listed at end of respective sections.

1 Acknowledgements

The author gratefully acknowledges the assistance of Ben Kane and Jeremy Rouse.

2 Overview

We discuss the following conjecture:

Conjecture : Consider the ternary quadratic form

$$\phi_1(x, y, z) = x^2 + y^2 + 10z^2.$$

Then with the exception of the integers $4^\lambda(16\mu + 6)$, which can be eliminated by congruence conditions, ϕ_1 represents every sufficiently high integer.

As we discuss later, this conjecture is in fact true, and this follows from Siegel's lower bound for class numbers and an upper bound of Iwaniec and Duke for the Fourier coefficients of half-integral weight modular forms. Unfortunately, these results do not yield an **effective** bound; that is, we don't know how high 'sufficiently high' is.

If we assume the Riemann Hypothesis for Dirichlet L-functions $L(s, \chi)$ we can make the lower bound for class numbers effective and thus get an effective lower bound for our conjecture. However, we expect this bound to be enormous –

much higher than 10^{75}. We would greatly prefer to get a lower bound sufficiently low that the numbers below this bound could be checked by computer, allowing us to compile a complete list of exceptions.

We discuss a conditional proof of Ono and Soundararajan of a lower bound of approximately 2×10^{10}, which is numerically feasible. In particular they define an *eligible* integer one to be one not eliminated by congruence conditions and prove the following

Theorem [OS] : Suppose that the non-trivial zeros of all Dirichlet L-functions $L(s, \chi)$, with χ a primitive, real character, have real part $1/2$. Further suppose that the non-trivial zeros of the Hasse-Weil L-functions $L(E(-10N), s)$ (with N a squarefree integer coprime to 10) have real part 1. Then the only eligible integers which are not of the form $x^2 + y^2 + 10z^2$ are:

$$3, 7, 21, 31, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391, 679, 2719.$$

Our paper begins with an overview of the arithmetic theory of quadratic forms. Then, after some preliminary remarks and definitions, we present in detail Ono and Soundararajan's proof for the special case of N non-squarefree. Finally, we justify the above remarks and give a very brief overview of the remainder of Ono and Soundararajan's paper.

3 The Arithmetic of Quadratic Forms

3.1 Quadratic forms over $\mathbb{Q}$ and $\mathbb{Q}_p$

A quadratic form, roughly speaking, is something that looks like the following:

$$\phi(x, y, z) = x^2 + y^2 + 10z^2$$

In other words it is a quadratic expression in some number of variables, here with integer coefficients. From an arithmetic standpoint, we ask the question: what integers N can be represented by a particular form?

In the case $N = 0$, and over the rationals, we have the following theorem, an example of a 'local-to-global' principle:

Theorem (Hasse-Minkowski) : Suppose f is a quadratic form of nonzero determinant with rational coefficients. Then f represents zero nontrivially in Q if and only if it does so for all $\mathbb{Q}_p$ with $p \leq \infty$. (Notation: $\mathbb{Q}_\infty = \mathbb{R}$.)

The 'only if' is trivial, as a zero representation in $\mathbb{Q}$ is also one for all $\mathbb{Q}_p$. The 'if' is not trivial, and the proof divides into a number of cases with an induction. See, for example, Jones (pp. 69-73) or Serre (pp. 41-43).

One then derives the following corollary:

Corollary: Suppose f is a quadratic form with rational coefficients. Then $f = N$ has a solution in rational numbers if and only if it has a solution in all $\mathbb{Q}_p$.

Unfortunately the same is not true for $\mathbb{Z}$ and $\mathbb{Z}_p$. So, to analyze Diophantine equations in $\mathbb{Z}$ we are obliged to do more work. (You may have guessed that, by the fact that we are assuming GRH.) We therefore develop broader notions of equivalence for quadratic forms.

3.2 Quadratic Forms over $\mathbb{Z}$

Notation: Write $SL_n^{\pm}(\mathbb{Z})$ for the set of integer matrices with determinant ± 1. (Is there standard notation for this...?)

We observe that $SL_n^{\pm}(\mathbb{Z})$ acts in a natural fashion on the set of quadratic forms, corresponding to an invertible, integral change of variables. It is clear that such a change of variables does not affect the list of integers that can be represented, and so we make the following definition:

Definition: Two quadratic forms are said to be **equivalent**, or be in the same **class**, or to **represent one another**, if they are in the same orbit of $SL_n^{\pm}(\mathbb{Z})$.

More generally a form f represents g if there is an integral, nonsingular change of variables taking f to g. For example, the form $x^2 + 2y^2$ represents the form $4x^2 + 18y^2$ by the change of variables $x \to 2x, y \to 3y$.

We observe that quadratic forms can be represented in a canonical form by symmetric matrices. For example, the form $f = x^2 + 3y^2 + 2z^2 + 4xy$ is represented by the matrix

$$M = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix},$$

and then if $\mathbf{x} = \begin{pmatrix} x & y & z \end{pmatrix}^{\mathbf{T}}$ then $\mathbf{x^T M x} = \mathbf{f}$. Then we may state the above definition in terms of matrices: f represents g if there is a matrix T over the integers so that if A and B are the matrices of f and g, then $T^T A T = B$.

We say that f represents g *rationally* (or over $\mathbb{Q}_p$, etc.) if we may take such a T with entries in the rationals, in $\mathbb{Q}_p$, etc. We also make the following definition:

Definition: A form f with matrix A represents g with matrix B *rationally without essential denominator* if for any positive integer k there is a matrix T over Q such that $T^T A T = B$, and the denominators of the entries of T are all

coprime to k. We say that two forms f and g are in the same **genus** if they represent each other rationally without essential denominator.

Proposition: If f and g are in the same genus then they have the same determinant.

Proof: For any k we have $T^T AT = B$, where T has denominators coprime to k. Taking determinants, $\det(T)^2 \det(A) = \det(B)$, so that $\det(B)/\det(A)$ has denominator coprime to all k, and is therefore an integer. Similarly $\det(A)/\det(B)$ is an integer, and so $\det(T) = \pm 1$ for any T under consideration. Squaring, $\det(A) = \det(B)$.

In the definition of genus above, we required that for any prime p, there exist matrices T with entries in $\mathbb{Q} \cap \mathbb{Z}_p$. It turns out that it is enough to assume that there exist matrices with entries in $\mathbb{Z}_p$:

Proposition: If f and g are integral forms the following are equivalent:
(1) f represents g rationally without essential denominator.
(2) f represents g with a rational matrix with denominators coprime to $2\det(f)\det(g)$.
(3) f represents g in all $\mathbb{Z}_p$.
(4) f represents g in all $\mathbb{Z}_p$ for p dividing $2\det(f)\det(g)$, and also in $\mathbb{R}$.

The nontrivial implications to prove are that (4) implies (3), and that (3) implies (1). That (3) implies (1) is particularly interesting; the proof is a bunch of matrix algebra. See Jones, pp. 110-113.

3.3 Ternary Quadratic Forms

We have the following theorem for ternary forms, which does not generalize to higher cases:

Theorem : Let G be a genus of ternary quadratic form of determinant d. Then a positive number N is represented integrally by a form in G if and only if it is so represented over the reals, and if for each prime p dividing $2d$,

$$f \equiv N \pmod{p^{r+1}}$$

is solvable in integers, where p^r is the highest power of p dividing $4N$.

The theorem follows from results similar to the ones considered above. (See Jones, p. 186.) Note that the theorem allows us to conclude which forms are representable by the *genus* simply by considering the behavior of a single form in the genus. Using this, we establish the following:

Proposition : We let f be the form

$$\phi_1(x, y, z) = x^2 + y^2 + 10z^2,$$

the form considered in [OS]. Let G be the genus of f. Then the positive numbers which are represented by G are exactly those not of the form

$$4^\lambda(16\mu + 6).$$

Proof : The determinant of ϕ_1 (and therefore of G) is 10, so we need to check the above conditions for the primes 2 and 5.

For the prime 2, we need to check that for any $N = 2^k m$ with m odd,

$$f \equiv N \pmod{2^{k+3}}$$

is solvable.

We break the proof into cases: ϕ_1 represents every odd number modulo 8 by 1, 11, 5, and 15, respectively. If $k = 1$, we need to consider numbers congruent to 2, 10, and 14 modulo 16, and each of these is represented exactly by f. If $k = 2$, we must consider numbers congruent to 4, 12, 20, 28 modulo 32; the first three are represented by f and $28 \equiv 92 = 1 + 1 + 90$.

Suppose now that $m \geq 3$; i.e., that 8 divides N. In this case one checks the value of f modulo 8 for even and odd values of x, y, and z, and find that x, y, and z must all be even. Therefore f represents N if and only if f represents $N/4$.

For the prime 5, if $N = 5^k m$, with m coprime to 5, we need to check that we can solve

$$f \equiv N \pmod{5^{k+1}}.$$

We first verify that we may solve $f \equiv c \pmod{25}$ for all $0 \leq c \leq 24$. (This can be done with f taking on values in the double digits.) But then by multiplying x, y, z by 5 we can solve $f \equiv c5^{2a} \pmod{5^{2a+2}}$ for all c and nonnegative integers a. Thus, if k is even we take $c = m$ and $a = k/2$ in the above equation; if k is odd we take $c = 5m$ and $a = (k-1)/2$.

We conclude from all this that a number N will be represented by a form in the genus of f if it is not of the form

$$4^\lambda(16\mu + 6).$$

Conversely we need to check that any N congruent to 6 modulo 16 is not represented. To see this, modulo 16, x^2 and y^2 can each represent 0, 1, 4, and 9; $10z^2$ can represent 10, 8, or 0. We check that there is no way to add these modulo 16 and get 6. This completes the proof.

Notation : Following [OS], call a non-negative integer N **eligible** if there are no congruence conditions prohibiting f from representing N. That is, in this case, the eligible integers are those not of the form $4^\lambda(16\mu + 6)$.

We have now concluded that every eligible integer is represented by the genus of ϕ_1. This is very useful information, and if all forms in this genus are equivalent to ϕ_1, we could derive the result of [OS] very cheaply. Naturally, this is not the case, but we have the following:

Proposition : The form ϕ_1 is in a genus consisting of two equivalence classes, represented by

$$\phi_1(x,y,z) = x^2 + y^2 + 10z^2$$
$$\phi_2(x,y,z) = 2x^2 + 2y^2 + 3z^2 - 2xz.$$

Sketch of Proof : To prove this one recalls that we may apply arbitrary transformations in $SL_3(\mathbb{Z})$ to the coefficients, and give a definition of a *reduced* form for a transformation. One then proves that every form is equivalent to a reduced form, and that no two reduced forms are equivalent. The proof of this is long and tedious; see Jones, p. 188, for at least a proper definition.

3.4 From Quadratic Forms to Modular Forms

We have the following general principle:

By constructing generating functions out of the number of representations of integers by n-ary quadratic forms, we obtain modular forms of weight $n/2$.

In particular Ono and Soundararajan's analysis proceeds by constructing a modular form from the numbers of representations of integers N by ϕ_1 and ϕ_2, and this modular form turns out to belong to $S_{\frac{3}{2}}(40, \chi_{10})$.

We give a brief overview of this general principle. A sample theorem of this variety is found in Zagier's survey article, p. 245: (note that this result is not due to Zagier)

Theorem: Let $Q : \mathbb{Z}^r \to \mathbb{Z}$ be a quadratic form in r variables. Define a **theta function** $\theta_Q(z)$ by

$$\theta_Q(z) = \sum_{x \in Z^r} q^{Q(x)}.$$

Then θ_Q is a modular form of weight $r/2$ on the group $\Gamma_0(N)$, with character χ, where N and χ are determined as follows:

Writing $Q(x) = 1/2 x^T A x$ with a symmetric matrix A, then N is defined to be the smallest positive integer so that NA^{-1} is even.

The character χ is given by $\chi(d) = \left(\frac{D}{d}\right)$, where $D = (-1)^{r/2} \det A$.

The general proof of this is somewhat involved (see, for example, Gunning, pp. 77-85). It is simpler in the case of the "standard" theta function

$$\theta(z) = \sum_{n=-\infty}^{n=\infty} e(n^2 z)$$

and its kth power

$$\theta^k(z) = \sum_{n=0}^{n=\infty} r_k(n) e(nz)$$

where $r_k(n)$ counts the number of representations of n as a sum of k squares. Key to the proof is some kind of Poisson summation; then one makes some sort of further analytic argument (Gunning uses the Jacobi Inversion formula) to show that the function θ^k satisfies functional equations which correspond to the generators of the group $\Gamma_0(N)$.

3.5 References

Gunning, R.C. *Lectures on Modular Forms.* Princeton University Press, 1962.

Jones, Burton. *The Arithmetic Theory of Quadratic Forms.* MAA, Carus 10, 1967.

Koblitz, Neal. *Introduction to Elliptic Curves and Modular Forms.* GTM 97, Springer-Verlag.

Serre, Jean-Pierre. *A Course in Arithmetic.* Springer-Verlag, 1977.

Zagier, Don. *Introduction to Modular Forms.* From M. Waldschmidt et al., ed., *From Number Theory to Physics.* Springer-Verlag, 1992.

4 Ramanujan's Ternary Quadratic Form

Here we begin to follow the paper of Ono and Soundararajan. In particular we review the main result that they prove:

Theorem [OS] : Assume the Generalized Riemann Hypothesis. Then all eligible integers over 2,719 are represented by the form $x^2 + y^2 + 10z^2$.

We start by eliminating numbers coprime to 10:

Proposition: All eligible integers divisible by 2 or 5 are represented by ϕ_1.

If N is of the form $10n + 5$ we use a theorem of Legendre ([OS] quotes Dickson, *History of the Theory of Numbers*; however, a straightforward proof is not to

be found there) that $2n+1 = x^2+y^2+2z^2$ has a solution for all positive n. Multiplying by 5,

$$10n+5 = 5(x^2+y^2) = (2x+y)^2+(x-2y)^2+10z^2$$

is a representation of the desired form.

In case N is even the proposition is clear.

"If you don't know how to prove something, just say it's clear." -Anonymous

4.1 Automorphs and Essentially Distinct Representations

We let A_1 and A_2 be the matrices of ϕ_1 and ϕ_2:

$$A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 10 \end{pmatrix} \quad A_2 = \begin{pmatrix} 2 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 3 \end{pmatrix}.$$

Definition : A matrix $B \in SL_3(\mathbb{Z})$ is called an **automorph** of A_i if $B^T A_i B = A_i$. We are interested in automorphs of A_1 and A_2. These correspond to linear, invertible changes of variables in ϕ_1 and ϕ_2 with determinant 1, that don't change the form. For example, in ϕ_1 we may switch x and y, and/or replace any or all of x, y, z by their negatives, but we can't do anything else. This gives 16 transformations, and exactly half have determinant 1. We have the following

Proposition: The automorphs of A_1 are given by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The automorphs of A_2 are given by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & -1 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

We now make the following

Definition : Two representations of N by ϕ_i (i.e., ϕ_1 or ϕ_2), denoted (x, y, z) and (x', y', z') are **essentially distinct** if there is no automorph B of A_i with the property that

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = B \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

For example, with ϕ_1, $(3,5,2)$ and $(5,3,-2)$ are 'essentially similar' representations of 74, and we can see that they indeed represent 74 in 'essentially' the same way.

We want to count the number of essentially distinct representations of numbers by forms, and observe that automorphs partition these representations into equivalence classes. I claim the following:

Proposition : If N is squarefree and coprime to 10, then no two distinct automorphs of representations of N by ϕ_i (for $i = 1, 2$) are equal.

Proof : We prove this for ϕ_1, the other case being similar. We observe that the automorphs form a subgroup of $SL_3(\mathbb{Z})$, and in particular all of them are invertible, so that it suffices to show that no automorph is equal to the identity automorph.

Considering the diagonal automorphs in the first row, if, for example, we have

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

then $x = -x = 0$, $y = -y = 0$, so our representation is of the form $10z^2$ which is divisible by 10. Similarly the other diagonal automorphs give representations $N = x^2$ or $N = y^2$, which imply N is not squarefree.

In the second row, if one of the first two automorphs gives the same representation we have $z = -z = 0$ and either $x = y$ or $x = -y$. In either case $x^2 = y^2$ and so our representation is of the form $N = x^2 + y^2 = 2x^2$, which is not squarefree. In the case of the last two automorphs in the second row we have $x = y$ and $x = -y$, so that $x = y = 0$, and our representation is again of the form $10z^2$.

In light of this proposition, if we let $G(N)$ denote the number of essentially distinct primitive representations of a squarefree number N by the genus G of ϕ_1 and ϕ_2, and $R_1(N)$ and $R_2(N)$ the number of representations of N by ϕ_1 and ϕ_2 respectively, we have

$$G(N) = R_1(N)/8 + R_2(N)/4.$$

We also have the following different formula for $G(N)$:

Proposition (OS, Prop. 1, p.7): If $N > 1$ is an eligible integer coprime to 10 then

$$G(N) = \frac{1}{4} h(-40N).$$

Here $h(-40N)$ is the **class number** , the number of properly primitive classes of positive or indefinite binary forms $ax^2 + 2bxy + cy^2$ of determinant $-40N =$

$ac - b^2$. Note that the class number also refers to the cardinality of the quotient

$$H = I/P$$

where I is the (multiplicative) group of the **fractional ideals** of the **quadratic field** $Q[\sqrt{-40N}]$, and P is the subgroup of principal fractional ideals. One can prove that classes of binary forms correspond to classes of ideals, so that in fact the two notions of class number coincide.

Remark: (in lieu of a proof): We quote, as do Ono and Soundararajan, Theorem 86 of Jones's book. This theorem is to the effect that if one is given a ternary quadratic form, one can write a formula like the one above. The exact formula requires that N be coprime to the determinant d of the form, and breaks up into a large number of special cases based on the congruence class of dN modulo 8.

4.2 Representations of Non-squarefree Integers

We wish to work towards a proof of the following.

Theorem (OS, 1) : Let N be an eligible integer (i.e., one not of the form $4^\lambda(16\mu + 6)$ which is not square-free. Then it is of the form $x^2 + y^2 + 10z^2$.

We note that such a representation could either be *primitive* , with $\gcd(x, y, z) = 1$, or it could come from a representation of $N/(\gcd(x, y, z))^2$.

We work towards the proof. To do that we introduce some notation; for a positive integer n denote by $r_1(n)$ the number of representations of n by ϕ_1, and by r_2 the number of representations by

$$\phi_2 = 2x^2 + 2y^2 + 3z^2 - 2xz.$$

Then define

$$a(n) = \frac{1}{4}(r_1(n) - r_2(n))$$

and a generating function

$$f(z) = \sum_{n=1}^{\infty} a(n)$$

where $q = e^{2\pi iz}$ as usual. We define a Dirichlet character χ_{10} to be the character modulo 40 given by $\left(\frac{10}{\cdot}\right)$. Then, by methods analogous to those discussed previously, we obtain the following

Proposition : $f(z) \in S_{\frac{3}{2}}(40, \chi_{10})$.

We recall that $S_{\frac{3}{2}}(40, \chi_{10})$ is a finite-dimensional vector space. Therefore by computing the first few terms of $f(z)$

$$f(z) = q - q^3 - q^7 - q^9 + 2q^{13} + q^{15} + \dots$$

we uniquely determine $f(z)$ and its properties turn out to be well known. We quote the following without proof:

Proposition :

(1) $F(z)$ is an eigenform for all of the Hecke operators $T(p^2)$.

Therefore, in particular, we may consider its Shimura lift

$$F(z) = \sum_{n=1}^{\infty} A(n)q^n = q - 2q^3 - q^5 + 2q^7 + q^9 + 2q^{13} + 2q^{15} - 6q^{17} - \dots$$

and then the following hold:

(2) $F(z) \in S_2(20)$, and moreover, $F(z)$ is a newform.

(3) $F(z) = \eta^2(2z)\eta^2(10z)$, where

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)$$

is Dedekind's eta function.

(4) $F(z)$ is the inverse Mellin transform of $L(E, s)$, where $L(E, s)$ is the Hasse-Weil L-function for the elliptic curve

$$E : y^2 = x^3 + x^2 + 4x + 4.$$

(5) In light of (4), by a theorem of Hasse, $|A(p)| \leq 2\sqrt{p}$ for every prime p.

We wish to recall the following theorem from Shimura's *Annals* paper:

Theorem (Shimura, 1.7) . Let p be a prime number, and let $f \in S_{k/2}(N, \chi)$. Denote by $a(n)$ and $b(n)$ the coefficients of the Fourier expansions:

$$f(z) = \sum_{n=0}^{\infty} a(n)q^n$$

$$(f|T(p^2))(z) = \sum_{n=0}^{\infty} b(n)q^n$$

Then

$$b(n) = a(p^2n) + \chi(p)(\frac{-1}{p})^{\frac{k-1}{2}}(\frac{n}{p})p^{\frac{k-3}{2}}a(n) + \chi(p^2)p^{k-2}a(n/p^2).$$

We take $a(n/p^2) = 0$ where p^2 does not divide n.

Specializing to the case of interest, and recalling that our $f(z)$ is an eigenform of the Hecke algebra, denote by $\alpha(p)$ the eigenvalue for the prime p and we have

$$a(n)\alpha(p) = a(p^2n) + \chi_{10}(p)(\frac{-n}{p})a(n) + \chi_{10}(p^2)pa(n/p^2).$$

As $F(z)$ is a newform we have that $\alpha(p) = A(p)$. We pause to justify this assertion:

Proposition : In the preceding formula $\alpha(p) = A(p)$.

Proof: We see that $F(z)$ is a newform and therefore an eigenform of the entire Hecke algebra. We recall the definition of the Hecke operator (see Ono, p. 21): If $F(z) = \sum_{n=0}^{\infty} A(n)q^n$ then

$$F(z)|T_p = \sum_{n=0}^{\infty}(A(pn) + \chi(p)p^{k-1}a(n/p))q^n.$$

If $F(z)|T_p = \lambda F(z)$ (and since $F(z)$ is a cusp form) then

$$\sum_{n=1}^{\infty}\lambda A(n)q^n = \sum_{n=1}^{\infty}(A(pn) + \chi(p)p^{k-1}a(n/p))q^n.$$

Comparing the $q = 1$ terms we have

$$\lambda A(1) = A(p) + \chi(p)p^{k-1}a(1/p);$$

as the $a(1/p)$ term drops out,

$$\lambda A(1) = A(p).$$

Finally we assume that $F(z)$ is *normalized* so that $A(1) = 1$, and thus $\lambda = A(p)$.

Conversely, it is well-known (see, for example, Ono, Cor. 3.16) that the Shimura correspondences commute with the Hecke operators of integral and half-integral weight. That is, we have

$$F(z)|T_p = f(z)|T_{p^2}.$$

In particular if f, and therefore F, are eigenforms of the respective integer and half-integer weight modular forms then the eigenvalues must be the same: As $F(z)|T_p = \lambda F(z)$ and $f(z)|T_{p^2} = \alpha(p)$ we have that $\lambda = \alpha(p)$, and hence the result follows.

At this point we confine ourselves to considering the case where n is square-free. In view of the proposition, our equation then simplifies to

$$a(n)A(p) = a(p^2n) + \chi_{10}(p)(\frac{-n}{p})a(n).$$

We write the above as

$$a(p^2n) = \left(A(p) - \chi_{10}(p)(\frac{-n}{p})\right) a(n)$$

and plug in the definition $a(n) = \frac{1}{4}(r_1(n) - r_2(n))$ to write

$$\frac{1}{4}(r_1(p^2n) - r_2(p^2n)) = \left(A(p) - \chi_{10}(p)(\frac{-n}{p})\right) (\frac{1}{4}(r_1(n) - r_2(n)))$$

and so

$$r_1(p^2n) - r_2(p^2n) = \left(A(p) - \chi_{10}(p)(\frac{-n}{p})\right) (r_1(n) - r_2(n)).$$

Now suppose M is a non-squarefree integer which is not represented by ϕ_1. Then M is divisible by p^2 for some prime p; and by our previous comments p is not 2 or 5.

Let N denote the squarefree part of M (i.e., we divide M by all squares of primes that divide it). As M is not represented by ϕ_1, it follows that Np^2 is not either: $M/(Np^2)$ is a square number (possibly 1) and therefore a representation of Np^2 by ϕ_1 gives a representation of M in an obvious manner: simply multiply x, y, and z by $\sqrt{M/(Np^2)}$.

Accordingly $r_1(Np^2) = 0$ and thus also $r_1(N) = 0$. Plugging this into the above,

$$-r_2(p^2N) = \left(A(p) - \chi_{10}(p)(\frac{-n}{p})\right) (-r_2(N))$$

and so

$$\frac{r_2(Np^2)}{r_2(N)} = A(p) - \chi_{10}(p)(\frac{-n}{p}).$$

We make the simple observation that if χ is any real Dirichlet character, then $\chi(m) \leq 1$ for all m to obtain the inequality

$$\frac{r_2(Np^2)}{r_2(N)} \leq A(p) + 1.$$

Recall that R_1 and R_2 denote the number of *primitive* representations of a number by ϕ_1 and ϕ_2, respectively, where by *primitive* we mean a representation where x, y, z have no common factor. As N is squarefree, all representations of N will be primitive, and representations of Np^2 will either be primitive or come from those of N. Thus we have

$$r_2(Np^2) = R_2(Np^2) + R_2(N) = R_2(Np^2) + r_2(N).$$

Now we recall that if $G(N)$ is the number of essentially distinct primitive representations of N by the genus of ϕ_1 and ϕ_2, then

$$G(N) = R_1(N)/8 + R_2(N)/4.$$

In particular, we are assuming that N is not represented by ϕ_1, so that $G(N) = R_2(N)/4 = r_2(N)/4$. Moreover, as $Np^2 \neq 0$, every primitive essentially distinct representation of Np^2 by ϕ_2 has at least 2 different automorphs. To see this, we write $Np^2 = 2z^2 + 2y^2 + 3z^2 - 2xz$, and the identity transformation is trivially an automorph of the representation; moreover, if x or z is nonzero (or if both are) then $x \to -x$, $z \to -z$ is a different automorph. If instead both x and z are zero, then the latter two of the four matrices previously considered give the automorph $y \to -y$.

From this discussion we conclude that $2G(Np^2) \leq R_2(Np^2)$. Therefore,

$$\frac{r_2(Np^2)}{r_2(N)} = 1 + \frac{R_2(Np^2)}{r_2(N)} \geq 1 + \frac{2G(Np^2)}{4G(N)} = 1 + \frac{G(Np^2)}{2G(N)}.$$

We plug this into our previous inequality to derive the equation

$$\frac{G(Np^2)}{2G(N)} \leq A(p).$$

But we recall that $G(N) = \frac{1}{4}h(-40Np^2)$, and similarly with $G(Np^2)$, so that

$$\frac{G(Np^2)}{2G(N)} = \frac{h(-40Np^2)}{2h(-40N)}.$$

We now cite the **index formula** for $h(-D)$, due to Gauss, to the effect that $\frac{h(-40Np^2)}{h(-40N)} = p - \left(\frac{-40N}{p}\right)$ (see Cox, p. 148, Cor. 7.28) so that we get

$$\frac{h(-40Np^2)}{h(-40N)} = p - \left(\frac{-40N}{p}\right) \geq p - 1$$

so that combining these inequalities

$$\frac{p-1}{2} \leq A(p).$$

We recall that by Hasse's upper bound, mentioned previously, $|A(p)| \leq 2\sqrt{p}$, and now we are done: Writing

$$\frac{p-1}{2} \leq 2\sqrt{p}$$

this rules out all $p \geq 19$. For primes $\neq 2, 5$ less than 19 we read out the coefficients of $F(z)$: $A(3) = -2$, $A(7) = 2$, $A(11) = 0$, $A(13) = 2$, $A(17) = -6$. None of these satisfy the above inequality.

In conclusion, what we have shown is that if N is an eligible squarefree integer not represented by ϕ_1, then Np^2 is represented by ϕ_1 for all primes $p \neq 2, 5$. In case this happens, Np^2k^2 will be represented by ϕ_1 for all $k \geq 1$, so that all eligible non-squarefree numbers are represented by ϕ_1.

Q. E. D.

4.3 Ineffective and Impractical Bounds

We wish to discuss how we might prove the desired result for squarefree eligible integers. Naively speaking, there is a lot of 'wiggle room' in our quadratic form and we expect that we might be able to find some lower bound above which all integers will be represented.

From results considered previously we have the following

Corollary : Let N be an eligible integer. Then N is not of the form $x^2 + y^2 + 10z^2$ if and only if N is a squarefree integer coprime to 10, and

$$r_2(N) = R_2(N) = h(-40N).$$

We recall that if $a(n) = r_1(n) - r_2(n)/4$, then $f(z) = \sum_{n=1}^{\infty} a(n)e(nz)$ is a weight $3/2$ cusp form. The 'trivial' upper bound for Fourier coefficients of cusp forms gives us $|a(n)| << N^{1/2+\epsilon}$ for any ϵ; conversely for N not represented by ϕ_1 we have $|a(n)| = h(-40N)/4$ and therefore by Siegel's (ineffective) bound for class numbers we have $|a(n)| >> N^{1/2-\epsilon}$. We can see that these two bounds just barely miss crossing, and just barely miss giving useful information.

The bound for the upper bound has been improved by work of Iwaniec and Duke; in the case of our modular form we have

$$|a(n)| << \tau(N)N^{3/7}(log 2N)^2$$

where $\tau(N)$ is the number of divisors of N.

Remark: I am guessing this bound is effective although this is not stated in the paper.

Comparing this with Siegel's bound we have the following

Proposition : There is some number C so that for $N > C$ all eligible N are represented by Ramanujan's form.

The problem, naturally, is that Siegel's bound is **ineffective** and it does not tell us what C is.

If, however, we assume the Riemann Hypothesis for Dirichlet L-functions, a result of Littlewood shows effectively that $h(-40N) >> \sqrt{N}/\log\log N$. Combined with the Iwaniec-Duke results this will allow us to find an appropriate value of C conditional on GRH. Let us give a coarse estimate for what such a C would be: Assume that Littlewood's bound implies the much stronger bound $h(-40N) \geq N$, so that $|a(N)| \geq \sqrt{N}/4$. Assume also that the Iwaniec-Duke results imply $|a(N)| \leq \tau(N)N^{3/7}(\log 2N)^2$, although again this is much too much to assume. Then we have a contradiction if $N \geq (4\tau(N)(\log 2N)^2)^{14}$ which

happens only if $N \geq 10^{75}$.

A realistic interpretation of the Littlewood and Iwaniec-Duke results would in fact give a lower bound that is *much, much larger* . Accordingly, if we want to prove the theorem without recourse to BSD, it probably suffices to check by hand the first 10^{200} eligible integers. A list of representations for these integers is given in the appendix.

4.4 Proof of the Main Theorem

We give a *very brief* overview of the proof of Ono and Soundarajan.

4.4.1 Relation to Elliptic Curves

Let E be the elliptic curve previously considered

$$E : y^2 = x^3 + x^2 + 4x + 4$$

and denote by $E(D)$ its *quadratic twist* :

$$E(D) : y^2 = x^3 + Dx^2 + 4D^2x + 4D^3.$$

Then we have the following

Theorem 2 [OS]: Let N be a squarefree eligible integer not of the form $x^2 + y^2 + 10z^2$. If $L(E(-10N))$ be the Hasse-Weil L-function of $E(-10N)$, and $\Omega(E(-10))$ is its *real period* , then

$$h^2(-40N) = \frac{4\sqrt{N}}{\Omega(E(-10N))} L(E(-10N), 1).$$

The proof proceeds by using a theorem of Waldspurger to connect the Fourier coefficients of half-integral weight cusp forms to the central value of the L-function of their Shimura lift. We can then connect the Hasse-Weil L-function $L(E(-10N), 1)$ to the values $a(N)$.

We mention a corollary, which is not needed for the proof of the main theorem:

Corollary [OS] : Assume the Birch and Swinnerton-Dyer conjecture for elliptic curves of rank 0. Then if N is not of the form $x^2 + y^2 + 10z^2$ we have

$$h^2(-40N) = |Ш(E(-10N))| \prod_p \omega_p(E(-10N)).$$

The proof of this is not deep; one writes out the statement of the Birch and Swinnerton-Dyer Conjecture

$$L(E(-10N),1) = \frac{\Omega(E(-10N))|Ш(E(-10N))|}{|E_{tor}(-10N)|^2} \prod_p \omega_p(E(-10N))$$

where $E_{tor}(-10N)$ is the **torsion subgroup** of $E(-10N)$, the group of points of finite order,

$\omega_p(E(-10N))$ is the **local Tamagawa number** at p, which is 1 at any point of good reduction, and

$Ш(E(-10N))$ is the **Tate-Shafarevich group**

$$Ker\left(H^1(Gal(\overline{\mathbb{Q}}/\mathbb{Q}), E(-10N)(\overline{\mathbb{Q}})) \to \prod_{p\leq\infty} H^1(Gal(\overline{\mathbb{Q}_p}/\mathbb{Q}_p), E(-10N)(\overline{\mathbb{Q}_p}))\right).$$

We observe that $E_{tor}(-10N) \cong Z/2Z$ for all such N, and we know that $\Omega(E(-10N)) = \sqrt{N}/\Omega(E(-10))$, so that we can shuffle terms around to get the desired result.

The effect of this corollary is to be able to say something about the Tate-Shafarevich group in terms of class numbers (which are at least somewhat better understood). We call a positive integer N *exceptional* if it satisfies the equation given in Theorem 2. By Theorem 2, all numbers not represented by Ramanujan's form are exceptional, and there are a few others, but not too many: There are only six below 10^7, and the proof of the main theorem proves (conditional on GRH) that there are no exceptional integers above 2×10^{10}. Using this corollary and assuming BSD (and bringing in some additional theory) we can calculate Tate-Shafarevich groups for exceptional N. For example, we have

$$Ш(E(-27190)) \cong Z/6Z \oplus Z/6Z.$$

4.4.2 Analytic Estimates

If $N \geq 2\times 10^{10}$ is an eligible not represented by Ramanujan's form we write $\chi = \left(\frac{-40N}{\cdot}\right)$ and

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$$

$$L_a(s) = L(E(-10N),s) = \sum_{n=1}^{\infty} A(n)\chi(n)n^{-s}.$$

Then, considering the functional equations for these L-functions, determining the conductor of the curve $E(-10N)$ and applying Theorem 2 and Dirichlet's

class number formula we obtain an inequality

$$\frac{L_a(1)}{L(1)^2} \geq \frac{2}{7}\left(\frac{1600N^2}{4\pi^2}\right)^{1/4}$$

and the proof proceeds by showing that this is impossible given GRH.

Considering the equation

$$F(s) = \left(\frac{\sqrt{q}}{2\pi}\right)^{s-1} \frac{L_a(s)\Gamma(s)}{L(s)L(2-s)}$$

one uses the so called Phragmen-Lindelöf Principle to obtain

$$F(1) \leq \max_t |F(\sigma + it)|$$

for any σ satisfying $1 \leq \sigma < 3/2$.

Choosing (somewhat arbitrarily) $\sigma = 7/6$, Ono and Soundararajan obtain explicit formulae for $L_a'(s)/L_a(s)$ and $-L'(s)/L(s)$ in terms of convergent Dirichlet series, contributions from non-trivial zeroes, and remainder terms. Then they use these to obtain a lower bound for $\log|L(5/6+it)|$ and an upper bound for $\log|L_a(7/6+it)|$.

The proofs of these bounds are quite involved, and although we do not go into them in detail, we do remark that, broadly speaking, the proof involves a large number of numerical constants which were chosen because computer experiments revealed them to be close to optimal. One expects, somehow, that minor details of the proof could be changed, and that certain bounds could perhaps be improved, but the bounds considered by Ono and Soundararajan proved sufficient for their results.

We skip straight to the end of the proof, which breaks up into two cases according to whether $50 \leq \log(\frac{q}{4\pi^2}) \leq 100$, or $100 \leq \log(\frac{q}{4\pi^2})$, where $q = 1600N^2$, the conductor of the elliptic curve $E(-10N)$. (The case $\log\frac{q}{4\pi^2} \leq 50$ corresponds roughly to N less than 2×10^{10}, and below this bound the theorem was verified by direct computation.) In the first case, for example, Ono and Soundararajan obtain a formula

$$\log F(s) \leq \frac{9}{2} + \frac{9}{67}\log\frac{q}{4\pi^2}$$

which contradicts the formula given previously.

4.5 References

Cox, D. *Primes of the form* $x^2 + ny^2$. Wiley, New York, 1989.

Ono, Ken. *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series.* CBMS 102, Amer. Math. Soc., Providence, 2003.

Ono, Ken and K. Soundararajan. *Ramanujan's Ternary Quadratic Form.* Inv. Math., 130, 3, 1997, pp. 415-454.

5 Appendix: Modular Forms

We give a brief overview of the theory of modular forms of integral and half-integral weight.

Suppose that Γ is a discrete subgroup of $GL_2^+(\mathbb{R})$. The prototypical example is the group $SL_2(\mathbb{Z})$, the group of 2x2 matrices over the integers of determinant one. We also like to consider **congruence subgroups** of $SL_2(Z)$; i.e., subgroups that contain

$$\Gamma(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}\}$$

for some N. We define an action of Γ on the complex upper half-plane H as follows: if $\gamma \in \Gamma$ is the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then

$$\gamma z = \frac{az+b}{cz+d}.$$

Then a holomorphic (or meromorphic) **modular form** of (integer) weight k for Γ is defined to be a holomorphic (meromorphic) function f defined on H which satisfies, for all $z \in \mathbb{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$,

$$f(\gamma)z = (cz+d)^k f(z).$$

Note that the 'point at infinity' is generally considered to be part of the domain of definition, and holomorphicity at infinity is defined in terms of the Fourier series.

We wish to consider the analogous notion where k is allowed to be a half-integer rather than an integer. Unfortunately the preceding definition does not carry over exactly, because if k is a half-integer the power $(cz+d)^k$ is defined only up to a sign. Therefore one defines a covering space G for $SL_2(\mathbb{Z})$ (or, more generally, for all of $GL_2^+(\mathbb{R})$, with a determinant in the equation below) by letting G be the set of all ordered pairs $(\alpha, \phi(z))$ where $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(R)$ and $\phi(z)$ is a holomorphic fuction on H satisfying

$$\phi(z)^2 = t(cz+d) \tag{1}$$

for some $t \in C$ of norm 1. We define multiplication of group elements as follows (and check that we in fact get a group):

$$(\alpha, \phi(z))(\beta, \psi(z)) = (\alpha\beta, \phi(\beta(z))\psi(z)).$$

We define a **Fuchsian subgroup** of G to be a subgroup Δ so that its projection onto $SL_2(\mathbb{Z})$ is an isomoprhism. That is, we only allow one 'automorphy factor' for each element of $SL_2(\mathbb{Z})$.

We define a **slashing operator** as follows: If $\xi = (\alpha, \phi) \in G$, we define the action of ξ on H to be the same as that of α, and define

$$(f|[\xi]_{k/2})(z) = f(\alpha z)(\phi(z))^{-k}.$$

Finally we make the definition we want:

Definition: Suppose that f is a meromorphic (holomorphic) function on H, and Δ is a Fuchsian subgroup of G. Then we call f a meromorphic (holomorphic) **modular form** of **weight** $k/2$ with respect to Δ if:

(1) $f|[\xi]_{k/2} = f$ for all $\xi \in \Delta$.
(2) f is meromorphic (holomorphic) at every cusp of $P(\Delta)$ (e.g., at infinity).

One then defines the **Hecke operators** $T(p^2)$ for primes p. These are operators from the space $G_{k/2}(\Delta_1(N))$ to itself, which also act on the subspace $S_{k/2}(\Delta_1(N))$ of **cusp forms** . One then establishes relationships between the Fourier coefficients of f and $f|T(p^2)$ for modular forms f, and can in particular speak about **simultaneous eigenforms** for all the Hecke operators. What is true, and not obvious, is that they exist.

If one has such a simultaneous eigenform, then it turns out that one can 'lift' it to a corresponding modular form of **integral weight**. This was proved by Goro Shimura in his 1973 *Annals of Mathematics* paper:

Theorem (Shimura): Let $k \geq 3$ be odd, and let $f(z) \in S_{k/2}(N, \chi)$ be a modular form of weight $k/2$ for $\Delta_0(N)$, and suppose that f is an eigenfunction of the Hecke operators $T(p^2)$ for all primes p. Then one can define a function $F(z)$, whose Fourier coefficients can be determined explicitly from those of f, that is a modular form of integral weight $k - 1$.

5.1 References

Shimura, Goro. *On Modular Forms of Half Integral Weight.* The Annals of Mathematics, 2nd Ser., Vol. 97, No. 3 (May, 1973), pp. 440-481.

Koblitz, Neal. *Introduction to Elliptic Curves and Modular Forms.* GTM 97, Springer-Verlag.