Universal Quadratic Forms and the 15-Theorem and 290-Theorem

Yong Suk Moon
Department of Mathematics
Stanford University

June 8, 2008

Abstract

We study the problem of universal quadratic forms, whose solution is given by the recent paper of Bhargava and Hanke on the 15-Theorem and 290-Theorem. The main purpose of this paper is to explicate Bhargava and Hanke's proofs of the 15-Theorem and 290-Theorem, basically following their methods throughout the paper. We provide some details omitted in their original proof, and work out several examples to illustrate the idea clearly.

Contents

1 Introduction

A positive definite quadratic form is called **universal** if it represents all positive integers. In 1770, Lagrange proved his Four Squares Theorem which states that the form $x^2+y^2+z^2+t^2$ is universal. Legendre showed later exactly which numbers are represented by $x^2+y^2+z^2$ and which needs all four squares. Mathematicians such as Gauss, Eisenstein and Dirichlet opened up a new venue for studying representability of various forms, by introducing the notions of genus and p-adic numbers, and by developing an analytical approach to the theory. However, the classification of universal quadratic forms had not been studied deeply until the twentieth century.

In 1916, Ramanujan asserted which diagonal quaternary quadratic forms are universal by giving a list of those forms. Although his list had some errors, it motivated the study of finding the complete list of universal quaternary forms and universal forms of higher dimensions. The universal quadratic form problem can be divided into two cases, depending on the definition of an "integral" form. A quadratic form is said to be "classically integral" or described with the term "integer-matrix" if the associated matrix has only integer entries, and it is called "integer-valued" if all the values taken by the form are integers. Therefore, an integer-valued form may have half-integers for off-diagonal elements of its associated matrix. In 1993, J. H. Conway succeeded to solve the universal quadratic form problem for integer-matrix forms in his 15-theorem, and Manjul Bhargava and Jonathan Hanke solved the problem for integer-valued quadratic forms in the 290-theorem.

The main purpose of this paper is to explicate Bhargava and Hanke's proofs of the 15-Theorem and 290-Theorem, basically following their methods throughout the paper. In order to convey the underlying idea thoroughly, I tried to provide sufficient details omitted in their original proof, illustrating with examples worked out by myself. For example, using the theory of modular forms, I give my own solution for finding the number of representations as a sum of four squares, although the answer is well-known. I also concentrated on explaining how the relevant theories are used to solve the universality problem, so that any reader with a reasonable mathematical background could understand the result without much difficulty.

2 Statement of the 15-Theorem and 290-Theorem

We state the 15-theorem and 290-theorem from the papers [1] and [2]. The proofs will be given in the subsequent sections.

2.1 The 15-Theorem

Theorem 2.1. **("The Fifteen Theorem")** *If a positive-definite quadratic form having integer-matrix represents the nine numbers* 1, 2, 3, 5, 6, 7, 10, 14, *and* 15, *then it represents every positive integer.*

We call the above nine numbers the **critical integers** for integer-matrix forms. These integers are indeed critical in the following sense.

Theorem 2.2. *If t is any one of the above critical numbers, then there is a quaternary diagonal form that fails to represent t, but represents every other positive integer.*

This theorem shows that the Fifteen Theorem is the best possible statement for the universal quadratic form (with integer-matrix) problem. The following theorems show that the number 15 is rather special.

Theorem 2.3. *If a positive-definite quadratic form having integer-matrix represents every number below* 15, *then it represents every number above* 15.

Theorem 2.4. *There are forms which miss infinitely many integers starting from any of the eight critical numbers not equal to* 15.

In the proof of the Fifteen Theorem, we eventually show the following result which gives a complete solution to the universal integer-matrix form problem:

Theorem 2.5. *There are exactly* 204 *universal quaternary forms having integer-matrix.*

2.2 The 290-Theorem

We now state the 290-Theorem, which is similar to the 15-Theorem except that we are considering integer-valued quadratic forms.

Theorem 2.6. **("The 290-Theorem")** *If a positive-definite quadratic form with integer coefficients represents the twenty-nine integers*

$$1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26,$$
$$29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, \textit{ and } 290$$

then it represents all positive integers.

We call the integers listed in the theorem the **critical integers** for integer-valued forms. Similarly to the 15-Theorem, we prove the following theorems:

Theorem 2.7. *For each of the twenty-nine critical integer t, there exits a positive definite quadratic form with integer coefficients which fails to represent t but represents every other positive integer.*

Theorem 2.8. *If a positive-definite quadratic form with integer coefficients represents every positive integer below* 290*, then it represents every integer above* 290*.*

We conclude with the following theorem which gives the final answer for the universal quadratic form problem:

Theorem 2.9. *There are exactly* 6436 *universal quaternary forms.*

Although the 290-Theorem seems similar to the 15-Theorem, the proof involved is much more complex and requires analytical theories. We will prove the 15-Theorem first, and present the proof of the 290-Theorem subsequently. Throughout the paper, the brief term "a form" or "a quadratic form" means "a positive definite quadratic form."

3 Lattices and P-adic numbers

3.1 Escalation of lattices

It is convenient to work in terms of lattices for proving the 15-Theorem and 290-Theorem. There is a natural bijection between equivalence classes of integer coefficient quadratic forms and lattices having integer norms. Namely, with a quadratic form representing an equivalence class and having Minkowski-reduced Gram $n \times n$ matrix (a_{ij}), we associate the n-dimensional lattice $\{\mathbb{Z}e_i\}$ with $< e_i, e_j >= a_{ij}$ and vice versa.

As defined in the introduction, a quadratic form is said to be universal if it represents every positive integer. If a form f is not universal, then we define the **truant** of f (or its corresponding lattice $L(f)$) to be the smallest positive integer not represented by f. One of the frequently used notions in the proofs of the 15-Theorem and 290-Theorem is "escalator lattices." An **escalation** of a nonuniversal lattice L is defined to be any lattice which is generated by L and a vector whose norm is equal to the truant of L. An **escalator lattice** is a lattice obtained by a sequence of successive escalations of the zero-dimensional lattice.

3.2 P-adic numbers and genus

The representatibility of a number over the rings larger than $\mathbb{Z}$ sometimes give useful information about its representability over $\mathbb{Z}$. For a prime p, we define a valuation such that for any $r \in \mathbb{Q}$ written as $r = p^{\rho}\frac{u}{v}$, $|r|_p = p^{-\rho}$. For $p = \infty$, $|\ |_\infty$ is the absolute value norm. We complete the rational numbers $\mathbb{Q}$ under a valuation $|\ |_p$ to get the **p-adic field** $\mathbb{Q}_p$, and define the **p-adic integers** $\mathbb{Z}_p$ by the numbers $\alpha \in \mathbb{Q}_p$ such that $|\alpha|_p \leq 1$ (cf. [3]).

For a quadratic form Q in n variables, we say that a number m is **locally represented at** p if it is represented by Q over $\mathbb{Z}_p$. We say that m is **locally represented** if it is locally represented at p for all p including the ∞. In fact, we can reduce the problem of local representatbility at p to certain modular conditions as shown in Hanke's paper [5]. Before stating the relevant theorem, we first make following definitions.

Definition. Let $Q(x_1, \ldots, x_n)$ be a positive definite quadratic form having integer coefficients. Let A be the $n \times n$ matrix

$$A = \left(\frac{\partial^2 Q}{\partial x_i \partial x_j}\right).$$

We define the **level** of Q to be the smallest positive integer N such that NA^{-1} is an even matrix, that is, has integer entries with even integers on the diagonal.

If $\vec{x} \in \mathbb{Z}^n$ and P is a partition of $\{1, \ldots, n\}$, then for each $j \in P$ we let $\vec{x}_j$ denote the vector whose components are x_i for all $i \in j$. Similarly, for any $\mathbb{S} \subseteq P$ we take $\vec{x}_{\mathbb{S}}$ to be the vector whose components are x_i for all $i \in \bigcup_{j \in \mathbb{S}} j$. Then, we can prove that Q can be written in the local normalized form

$$Q(\vec{x}) \cong \sum_j p^{v_j} Q_j(\vec{x}_j) \quad \text{over } \mathbb{Z}_p$$

with $\dim(Q_j) \leq 2$ (cf. [5]).

We define

$$R_Q(m) = \{\vec{x} \in \mathbb{Z}^n \mid Q(\vec{x}) = m\},$$
$$R_{p^k,Q}(m) = \{\vec{x} \in \mathbb{Z}^n/p^k\mathbb{Z}^n \mid Q(\vec{x}) \equiv m \pmod{p^k}\},$$

and we let $r_Q(m) = \sharp R_Q(m)$, $r_{p^k,Q}(m) = \sharp R_{p^k,Q}(m)$. We say that $\vec{x} \in R_{p^k,Q}(m)$ is of **Zero type** if $\vec{x} \equiv \vec{0}$ mod p, of **Good type** if $p^{v_j}\vec{x}_j \not\equiv \vec{0}$ mod p for some j, and of **Bad type** otherwise.

Let $\vec{x}$ denote a general solution of a given type. We now describe reduction maps on each type of soutions, allowing the possiblity that $\vec{x}$ satisfies additional congruence conditions of the form $\vec{x}_j \equiv \vec{0}$ or $\vec{x}_j \not\equiv \vec{0} \pmod{p}$ for each j so long as these extra conditions do not contradict the reduction-type congruence conditions on $\vec{x}$. If such conditions on $\vec{x}_j$ are allowed for all $j \in \mathbb{S}$, then we denote them by $\vec{x}_{\mathbb{S}} \in C$.

By applying Hensel's lemma (cf. [3]), it is shown in [5] that

Lemma 3.1.
$$r^{Good}_{p^{k+l},Q}(m) = p^{(n-1)l} r^{Good}_{p^k,Q}(m)$$
for all $k \geq 2\ ord_p(2) + 1$.

For Good-type solutions, we have the map
$$R^{Good,\ \vec{x}\in C}_{p^k}(m) \xrightarrow{\pi_G} R^{Good,\ \vec{x}\in C}_{p^{k-1}}(m),$$
given by reducing $\vec{x}$ mod p^{k-1}. By above lemma, this map is surjective with multiplicity p^{n-1}, so the number of Good-type solutions can be determined either from the mod p solutions (if $p \nmid 2$) or from the solutions mod $4p$ (if $p \mid 2$).

The Zero-type solutions are characterized by $\vec{x} \equiv \vec{0}$ mod p and therefore occur only when $p^2 \mid m$. We have the map
$$R^{Zero}_{p^k}(m) \xrightarrow{\pi_Z} R_{p^{k-2}}\left(\frac{m}{p^2}\right)$$
defined by $\vec{x} \mapsto \vec{x}'' = p^{-1}\vec{x}$ mod p^{k-2}. Note that this is well-defined since $p^{-1}\vec{x}$ is defined modulo p^{k-1}. The elements $\vec{x}'$ mod p^{k-1} which reduce to a fixed $\vec{x}''$ are in one-to-one correspondence with $\pi_Z^{-1}(\vec{x}'')$ under $\vec{x} = p\vec{x}'$, and there are p^n such $\vec{x}'$. Therefore, π_Z is surjective with multiplicity p^n.

To obtain the reduction maps for Bad-type solutions, we divide into two cases. First, we define
$$\mathbb{S}_0 = \{j \mid v_j = 0\}, \quad \mathbb{S}_1 = \{j \mid v_j = 1\}, \quad \mathbb{S}_2 = \{j \mid v_j \geq 2\}.$$
and let $s_i = \sum_{j\in\mathbb{S}_i} \dim(Q_j)$. Then, the Bad-type solutions are characterized by $\vec{x} \not\equiv \vec{0}$ and $\vec{x}_{\mathbb{S}_0} \equiv \vec{0}$ (mod p). We have two reduction maps $\pi_{B'}$ and $\pi_{B''}$, which correspond to division by p and p^2 respectively. In the process, we introduce two auxiliary forms Q' and Q'', whose data is denoted with a $'$ or $''$, accordingly. For these we have $Q_j = Q'_j = Q''_j$ for all j.

We perform division by p for the case $\mathbb{S}_1 \neq \emptyset$ and $\vec{x}_{\mathbb{S}_1} \not\equiv \vec{0}$. We have
$$R^{Bad,\ \vec{x}_{\mathbb{S}_1}\not\equiv\vec{0},\ \vec{x}_{\mathbb{S}_1\cup\mathbb{S}_2}\in C}_{p^k,Q}(m) \xrightarrow{\pi_{B'}} R^{Good,\ \vec{x}_{\mathbb{S}_1\cup\mathbb{S}_2}\in C}_{p^{k-1},Q'}\left(\frac{m}{p}\right),$$
defined for each index j by
$$\vec{x}_j \mapsto p^{-1}\vec{x}_j, \quad v'_j = v_j + 1 \quad \text{if } j \in \mathbb{S}_0,$$
$$\vec{x}_j \mapsto \vec{x}_j, \quad v'_j = v_j - 1 \quad \text{if } j \notin \mathbb{S}_0.$$
This map is surjective with multiplicity $p^{s_1+s_2}$, since we can freely choose lifts of the components of the images at $\mathbb{S}_1 \cup \mathbb{S}_2$.

We perform division by p^2 for the remaining case where $\mathbb{S}_1 = \emptyset$ or $\vec{x}_{\mathbb{S}_1} \equiv \vec{0}$, which can occur only if $\mathbb{S}_2 \neq \emptyset$. For this case, we let
$$R^{Bad,\ \vec{x}_{\mathbb{S}_1}\equiv\vec{0},\ \vec{x}_{\mathbb{S}_2}\in C}_{p^k,Q}(m) \xrightarrow{\pi_{B''}} R^{\vec{x}_{\mathbb{S}_2}\not\equiv\vec{0},\ \vec{x}_{\mathbb{S}_2}\in C}_{p^{k-2},Q'}\left(\frac{m}{p^2}\right),$$

given by

$$\vec{x}_j \mapsto p^{-1}\vec{x}_j, \quad v_j'' = v_j \quad \text{if } j \in \mathbb{S}_0 \cup \mathbb{S}_1,$$
$$\vec{x}_j \mapsto \vec{x}_j, \quad v_j'' = v_j - 2 \quad \text{if } j \in \mathbb{S}_2.$$

Note that the map is p-to-1 over the $\mathbb{S}_0 \cup \mathbb{S}_1$ components by the same reasoning as for π_Z, and is p^2-to-1 over the $\mathbb{S}_2$ components since the inverse map corresponds to multiplication by p^2. Therefore, the map is surjective and has multiplicity $p^{2n-s_0-s_1}$.

We are now ready to state the following definition.

Definition. We define the **depth** of each type of solution of $R_{p^k,Q}(m)$ to be the maximal difference $k-k'$ for any $\vec{x} \in R_{p^k,Q}(m)$ to be mapped into $R_{p^{k'},\hat{Q}}(\hat{m})$ under consecutive application of the maps π_G, π_Z, and $\pi_{B^*} \in \{\pi_{B'}, \pi_{B''}\}$ described above of only that type (for some $\hat{Q}$ and $\hat{m}$).

The following lemma is proven in [5].

Lemma 3.2. *The Good-, Zero-, and Bad-type depths of $R_{p^k,Q}(m)$ are bounded above by $k-1$, $ord_p(m)$, and $ord_p(N)+1$ respectively, where N is the level of Q.*

The lemma clearly implies the following corollary, which will be used frequently for checking local conditions.

Corollary. *When $n \geq 3$ and $p \nmid N$, every number m is locally represented at p (by Q). For $n \mid N$, m is locally represented at p if and only if any of the quotients of m by a square factor are represented mod $p^{ord_p(4N)+2}$.*

For example, consider the form $Q(\vec{x}) = x_1^2 + 2x_2^2 + 2x_3^2$. The associated matrix A as in the definition of the level is given by $A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{pmatrix}$, which gives $A^{-1} = \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 1/4 & 0 \\ 0 & 0 & 1/4 \end{pmatrix}$. We thus have $N = 8$, and it suffices to check the local condition for square-free integers mod $2^{ord_2(4N)+2}$, that is, mod 128. By direct computation, we can show that the sqaure-free numbers which are represented mod 128 are precisely those not congruent to 7 (mod 8). Since the square of an odd integer is congruent to 1 (mod 8) and $2 \times 7 \not\equiv 7 \pmod 8$, an integer m has a square-free divisor congruent to 7 (mod 8) if and only if m is of the form $2^e(8k+7)$ where e is even. Therefore, the numbers locally represented by Q are precisely those not of the form $2^e(8k+7)$ with e even.

We now define a **genus** to be the set of $\mathbb{Z}$-equivalence classes of forms which are equivalent over $\mathbb{Z}_p$ for all p including the infinity. The number of classes in a given genus is finite (cf. [3]), and it is clear that even if a form f represents an integer a over $\mathbb{Z}_p$ for all p, f does not necessarily represent a over $\mathbb{Z}$. However, such a is represented by some form in the same genus as f, which is stated explicitly in the following theorems from Cassels' book [3].

Theorem 3.3. *Let rational integers $n \geq 1$ and $d \neq 0$ be given. For each $p \neq \infty$, let $f_p(\boldsymbol{x})$ be a $\mathbb{Z}_p$-integral form of determinant d in the variables $\boldsymbol{x} = (x_1, \ldots, x_n)$. Suppose that there* *exists a rational form $g(\boldsymbol{x})$ which is $\mathbb{Q}_p$-equivalent to $f_p(\boldsymbol{x})$ for each p. Then there is a $\mathbb{Z}$-integral form $f(\boldsymbol{x})$ which is $\mathbb{Z}_p$-equivalent to $f_p(\boldsymbol{x})$ for each p and $\mathbb{Q}$-equivalent to g.*

Proof. First, note that by the corollary following Lemma 3.2, there is only one $\mathbb{Z}_p$-equivalence class of forms of determinant d if $p \nmid 2d$. Therefore, it suffices to prove the existence of an integral form $f(\mathbf{x})$ which is $\mathbb{Z}_p$-equivalent to $f_p(\mathbf{x})$ for each $p \mid 2d$, and $\mathbb{Q}$-equivalent to g.

If $n = 1$, then $f_p(\mathbf{x}) = dx_1^2$ for all p and $g(\mathbf{x}) = dx_1^2$. Thus, we can simply let $f(\mathbf{x}) = dx_1^2$. For $n \geq 2$, we proceed with induction on n. The following lemma is useful:

Lemma 3.4. *Let $n \geq 2$ and suppose that the theorem holds for $n-1$. Let d, $f_p(\boldsymbol{x})$, and $g(\boldsymbol{x})$ as in the hypothesis of the theorem for n, and let $a \neq 0$ be a rational integer represented primitively by each f_p over $\mathbb{Z}_p$ and by $g(\boldsymbol{x})$ over $\mathbb{R}_\infty = \mathbb{Z}$. Then there exists an $f(\boldsymbol{x})$ which satisfies the properties in the theorem and which represents a primitively over $\mathbb{Z}$.*

Proof of Lemma. Replacing $f_p(\mathbf{x})$ for each p by a $\mathbb{Z}_p$-equivalent form if necessary, we may assume without loss of generality that

$$f_p(1, 0, \ldots, 0) = 1 \text{ for all } p.$$

By the Strong Hasse Principle (cf. [3]), the form $g(\mathbf{x})$ represents a over $\mathbb{Q}$. Replacing $g(\mathbf{x})$ by a $\mathbb{Q}$-equivalent form if necessary, we may assume that

$$g(1, 0, \ldots, 0) = a.$$

By completing the square, we have

$$af_p(\mathbf{x}) = (ax_1 + b_{2p}x_2 + \ldots + b_{np}x_n)^2 + f_p^*(x_2, \ldots, x_n) \tag{1}$$

for some $b_{2p}, \ldots, b_{np} \in \mathbb{Z}_p$, where f_p^* is a $\mathbb{Z}_p$-integral form in $n-1$ variables with determinant $d^* = a^{(n-2)}d$.

Similarly,

$$ag(\mathbf{x}) = (ax_1 + c_2x_2 + \ldots + c_nx_n)^2 + g^*(x_2, \ldots, x_n) \tag{2}$$

for some $c_2, \ldots, c_n \in \mathbb{Q}$ and some rational form g^* in $n-1$ variables.

Since $f_p(\mathbf{x})$ and $g(\mathbf{x})$ are $\mathbb{Q}_p$-equivalent, by (1) and (2), Witt's lemma (cf. [3]) implies that $f_p^*(x_2, \ldots, x_n)$ and $g^*(x_2, \ldots, x_n)$ are $\mathbb{Q}_p$-equivalent. Hence, by inductional hypothesis for f_p^* with determinant d^* and for g^*, there exists an integral form $f^*(x_2, \ldots, x_n)$ of determinant d^* which is $\mathbb{Z}_p$-equivalent to all p and $\mathbb{Q}$-equivalent to g^*.

There exists an integral form which is equivalent to f^* and arbitrarily close p-adically to f_p^* for all p dividing $2ad$ (cf. [3]). We replace f^* by such an equivalent form. By Chinese Remainder Theorem, we can find $b_2, \ldots, b_n \in \mathbb{Z}$ which are arbitrarily close p-adically to $b_{2p}, \ldots, b_{np}$ respectively, for all $p \mid 2ad$. Let

$$f(\mathbf{x}) = a^{-1}(ax_1 + b_2x_2 + \cdots + b_nx_n)^2 + a^{-1}f^*(x_2, \ldots, x_n) \tag{3}$$

Then, $f(\mathbf{x})$ has determinant d and is arbitrarily close to $f_p(\mathbf{x})$ for all $p \mid 2ad$. Clearly, $f(\mathbf{x})$ has only rational coefficients. If f is chosen to be sufficiently close to f_p for the p dividing a, then the coefficients of $f(\mathbf{x})$ will be integers, which we shall suppose.

Since f is arbitrarily close to f_p in the p-adic sense for $p \mid 2d$, we can ensure that f and f_p are $\mathbb{Z}_p$-equivalent for those p (cf. [3]). Thus, f and f_p are $\mathbb{Z}_p$-equivalent for all p.

Since f^* and g^* are $\mathbb{Q}$-equivalent, by (2) and (3), f is $\mathbb{Q}$-equivalent to g. By (3), $f(1, 0, \ldots, 0) = a$, so a is represented primitively by f, which proves the lemma.

Now, in order to prove the theorem, we suppose that the theorem holds for $n-1$. By the lemma, it suffices to show that an integer a exists satisfying the conditions of the lemma.

Let b be a non-zero integer represented by g over $\mathbb{Q}$, and let P be the set of primes dividing $2db$. Since there is only one $\mathbb{Z}_p$-equivalence class for $p \in P$, b is primitively represented by f_p over $\mathbb{Z}_p$ for such p's. For $p \notin P$, f_p represents b over $\mathbb{Q}_p$ because f_p and g are $\mathbb{Q}_p$-equivalent. If $b = f(\mathbf{b}_p)$, $\mathbf{b_p} \in \mathbb{Q}_\mathbf{p}^\mathbf{n}$, we can choose $\beta(p) \in \mathbb{Z}$ so that $p^{\beta(p)}\mathbf{b_p}$ is a primitive element in $\mathbb{Z}_p^n$.

Then, $a = b \prod_{p \in P} p^{2\beta(p)}$ satisfies the conditions of the lemma. This completes the proof of the theorem.

We further state the following theorem.

Theorem 3.5. *Let $f(\boldsymbol{x})$ be an integral form in n variables of determinant $d \neq 0$. Let $a \neq 0$ be an integer represented by $f(\boldsymbol{x})$ over $\mathbb{R}$ and primitively represented by $f(\boldsymbol{x})$ over $\mathbb{Z}_p$ for all $p \mid 2d$ (if $n \geq 3$), all $p \mid 2ad$ (if $n = 2$). Then a is primitively represented over $\mathbb{Z}$ by some form f^* in the same genus as f.*

Proof. The proof of Theorem 3.3 shows that a is primitively represented by f over $\mathbb{Z}_p$ for all p. We apply Lemma 3.4 putting $g(\mathrm{x})$ and $f_p(\mathrm{x})$ for all p in the lemma equal to the $f(\mathrm{x})$ of the present theorem. Then there exists an integral form $f^*(\mathrm{x})$ which is $\mathbb{Z}_p$-equivalent to $f(\mathrm{x})$ for all p, i.e., which is in the same genus as f, and represents a primitively.

Theorem 3.5 clearly implies the following corollary.

Corollary. If f in Theorem 3.5 is in a genus of one class, then f primitively represents a over $\mathbb{Z}$.

Note that the condition "primitively represented"in Theorem 3.5 and the corollary can be replaced by "represented," and we will directly use the replaced version of the corollary throughout the paper.

We now present the method of obtaining the genus of a given three-dimensional quadratic form (which is due to the unpublished method by Conway), as it is frequently used in the proof of the theorems. Let L_3 be a given three-dimensional lattice whose genus we want to find. We first embed L_3 into $\mathbb{Z}_6$ which has class number 1, and obtain vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ which generate the lattice. Then, we find a basis of the orthogonal complement to $\mathrm{span}\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$. Denoting by L_3' the lattice generated by the basis, we embed L_3' into $\mathbb{Z}_6$ and get the orthogonal complement lattices with the same procedure. Then, the lattices obtained at the end are in the same genus as L_3, and considering all possible ways to get the final lattices, we obtain the complete list of the genus.

To illustrate this method explicitly, we consider the lattice L_3 having Gram matrix $\begin{pmatrix}1 & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & 2\end{pmatrix}$. By embedding L_3 into $\mathbb{Z}_6$, we get

$$\mathbf{v}_1 = (1,0,0,0,0,0), \mathbf{v}_2 = (0,1,1,0,0,0), \mathbf{v}_3 = (0,0,0,1,1,0).$$

The orthogonal complement is $\{(0,a,-a,b,-b,c)\}$, which is spanned by

$$(0,1,-1,0,0,0), (0,0,0,1,-1,0), (0,0,0,0,0,1).$$

The lattice generated by these vectors has the Gram matrix $\begin{pmatrix}1 & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & 2\end{pmatrix}$, which is the same as that of L_3. Therefore, the only final lattice obtained through this process is L_3, which shows that L_3 is unique in its genus.

4 Modular forms and theta functions

We define a group action of $g = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in SL_2(\mathbb{R})$ on the upper half complex plane H by

$$gz = \frac{az+b}{cz+d}; \quad g\infty = \frac{a}{c}.$$

Letting $\Gamma = SL_2(\mathbb{Z})$, we define a subgroup

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

for some positive integer N. A subgroup of Γ is called a **congruence subgroup of level N** if it contains $\Gamma(N)$. We further let

$$\Gamma_0(N) = \{\begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \Gamma \mid c \equiv 0 \pmod{N}\};$$

$$\Gamma_1(N) = \{\begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \Gamma_0(N) \mid a \equiv 1 \pmod{N}\}.$$

Let $f(z)$ be a function on $\bar{H} = H \cup Q \cup \{\infty\}$ with values in $\mathbb{C} \cup \{\infty\}$, and let $k \in \mathbb{Z}$. We define

$$f(z)|[\gamma]_k = (\det\gamma)^{k/2}(cz+d)^{-k} f(\gamma z) \text{ for } \gamma = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in GL_2^+(\mathbb{Q}).$$

Definition. Let $f(z)$ be a meromorphic function on H, and let $\Gamma' \subset \Gamma$ be a congruence subgroup of level N, i.e., $\Gamma' \supset \Gamma(N)$. Let $k \in \mathbb{Z}$. We call $f(z)$ a **modular function** of weight k for Γ' if

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

and if, for any $\gamma_0 \in \Gamma = SL_2(\mathbb{Z})$,

$$f|[\gamma_0]_k \text{ has the form } \sum a_n q_N^n \text{ with } a_n = 0 \text{ for } n \ll 0. \tag{4}$$

where $q_N = e^{2\pi iz/N}$.

We call such an $f(z)$ a **modular form** of weight k for Γ', whose set is denoted by $M_k(\Gamma')$, if it is holomorphic on H and if for all $\gamma_0 \in \Gamma$ we have $a_n = 0$ for all $n < 0$ in (4). We call a modular form a **cusp form** if in addition $a_0 = 0$ in (4) for all $\gamma_0 \in \Gamma$, and denote the set of cusp forms by $S_k(\Gamma')$.

We use the notation $M_k(N, \chi)$ with χ a Dirichlet character mod N to denote the subspace of $M_k(\Gamma_1(N))$ consisting of $f(z)$ for which $f|[\gamma]_k = \chi(d)f$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. It is shown in [4] that $M_k(\Gamma_1(N)) = \oplus M_k(N, \chi)$, where the sum is over all Dirichlet characters modulo N.

Now, we define the theta function

$$\Theta(z) = \sum_{n\in\mathbb{Z}} e^{2\pi izn^2} = \sum_{n\in\mathbb{Z}} q^{n^2} \quad \text{for } z \in H,\ q = e^{2\pi iz}.$$

We can show that $\Theta^2 \in M_1(\Gamma_1(4)) = M_1(4, \chi_{-1})$ where $\chi_{-1}(d) = (-1)^{(d-1)/2}$. Then, by multiplicativity, we have for k even $\Theta^k \in M_{k/2}(4, \chi_{-1}^{k/2})$ (cf. [4]).

We now interpret modular functions as functions on lattices. We consider the congruence subgroup $\Gamma_1(N)$ specifically, as it is sufficient for our purpose. Define a **modular point** for $\Gamma_1(N)$ to be a pair (L, t) where L is a lattice in $\mathbb{C}$ and $t \in \mathbb{C}/L$ is a point of exact order N.

Let $k \in \mathbb{Z}$. We consider complex-valued functions F on the set of modular points which are of "weight k" in the following sense. For $\lambda \in \mathbb{C}^*$, let $\lambda L = \{\lambda l \mid l \in L\}$ and $\lambda t \in \mathbb{C}/\lambda L$. Then, F is defined to be of weight k if for all $\lambda \in \mathbb{C}^*$, $F(\lambda L, \lambda t) = \lambda^{-k} F(L, t)$ for all modular points (L, t).

Given a function F of weight k, we define two corresponding functions $\tilde{F}$ and f as follows. $\tilde{F}(\omega)$ is a complex-valued function on column vectors $\omega = \binom{\omega_1}{\omega_2}$ such that $\omega_1/\omega_2 \in H$. $f(z)$ is a function on the upper half-plane H. Let L_ω be the lattice spanned by ω_1 and ω_2, and let L_z be the lattice spanned by z and 1. Define $\tilde{F}(\omega) = F(L_\omega, \omega_2/N)$, and $f(z) = \tilde{F}\binom{z}{1}$.

For $\gamma \in SL_2(\mathbb{Z})$, let $\gamma\tilde{F}(\omega) = \tilde{F}(\gamma\omega)$. The following proposition is shown in [4].

Proposition 4.1. *The above association of F with $\tilde{F}$ and f gives a one-to-one correspondence between the following sets of complex-valued functions:* (1) *F on modular points which have weight k;* (2) *$\tilde{F}$ on column vectors ω which are invariant under γ for $\gamma \in \Gamma_1(N)$ and satisfy $\tilde{F}(\lambda\omega) = \lambda^{-k}\tilde{F}(\omega)$;* (3) *$f$ on H wihch are invariant under $[\gamma]_k$ for $\gamma \in \Gamma$.*

We now discuss the Hecke operators acting on modular forms of weight k for $\Gamma_1(N)$. Let $\mathcal{L}$ denote the $\mathbb{Q}$-vector space of formal finite linear combinations of modular points, i.e., $\mathcal{L} = \oplus\mathbb{Q}e_{L,t}$ is the direct sum of infinitely many one-dimensional spaces, one for each pair (L, t), where L is any lattice in $\mathbb{C}$ and $t \in \mathbb{C}/L$ is any point of exact order N. For each positive n, we define a linear map $T_n : \mathcal{L} \to \mathcal{L}$ by the following formula giving the image of the basis vector $e_{L,t}$:

$$T_n(e_{L,t}) = \frac{1}{n} \sum e_{L',t}$$

where the summation is over all lattice L' containing L with index n such that (L', t) is a modular point. We have the following proposition from [4].

Proposition 4.2. (1) *If g.c.d.$(m, n) = 1$, then $T_{mn} = T_m T_n$. In particular, T_m and T_n commute.*
(2) *If p is a prime dividing N, then $T_{p^l} = T_p^l$.*

Furthermore, for d an integer prime to N, let $[d] : \mathcal{L} \to \mathcal{L}$ be the linear map defined on basis elements by $[d]e_{L,t} = e_{L,dt}$ (cf. [4]). Then, we have the following lemma proven in [4].

Lemma 4.3. *Suppose that $F(L,t)$ corresponds to a function $f(z)$ on H which is in $M_k(\Gamma_1(N))$. Then $[d]F$ and T_nF also correspond to functions (denoted $[d]f$ and T_nf) in $M_k(\Gamma_1(N))$. If f is a cusp form, the so are $[d]F$ and T_nF. Thus, $[d]$ and T_n can be regarded as linear maps on $M_k(\Gamma_1(N))$ or on $S_k(\Gamma_1(N))$. In this situation, let χ be a Dirichlet character modulo N. Then, $f \in M_k(N, \chi)$ if and only if $[d]F = \chi(d)F$, i.e., if and only if*

$$F(L, dt) = \chi(d)F(L, t) \text{ for } d \in (\mathbb{Z}/N\mathbb{Z})^* \tag{5}$$

We saw before that a function $f \in M_k(\Gamma_1(N))$ can be written as a sum of functions in $M_k(N, \chi)$ for different Dirichlet characters χ. Thus, by one-to-one correspondence in Proposition 4.1, we can write a modular form $F(L,t)$ as a direct sum of $F's$ satisfying the equation (5) for various χ. Further, we have the following propositions shown in [4].

Proposition 4.4. *The operators T_n commute with $[d]$, and preserve the space of $F(L,t)$ of weight k which satisfy* (5). *Therefore, T_n preserves $M_k(N, \chi)$ and also $S_k(N, \chi)$*

Proposition 4.5. *Let $f(z) = \displaystyle\sum_{n=0}^{\infty} a_n q^n, f \in M_k(N, \chi)$, and let $T_p f(z) = \sum_{n=0}^{\infty} b_n q^n$. Then,*

$$b_n = a_{pn} + \chi(p)p^{k-1}a_{n/p}$$

where we take $\chi(p) = 0$ if $p|N$ and $a_{n/p} = 0$ if n is not divisible by p.

Most of the important examples of modular forms turn out to be eigenvectors ("eigenforms") for the action of all of the T_m on the given space of modular 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, as shown in the following proposition (cf. [4]).

Proposion 4.6. *Suppose that $f \in M_k(N, \chi)$ is an eigenform for all of the operators T_m with eigenvalues λ_m, $m = 1, 2, \ldots$. Let $f(z) = \displaystyle\sum_{m=0}^{\infty} a_m q^m$. Then $a_m = \lambda_m a_1$ for $m = 1, 2, \ldots$. In* *addition, $a_1 \neq 0$ unless $k = 0$ and f is a constant function. Finally, if $a_0 \neq 0$, then λ_m is given by the formula*

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

If f is an eigenform as in Proposition 4.6 (with $k \neq 0$), then we can multiply it by a suitable constant to get the coefficient of q equal to 1, i.e., $a_1 = 1$. Such an eigenform is called **normalized**.

Now, in order to extend our definition of Hecke operators for a large class of congruence subgroups of $\Gamma = SL_2(\mathbb{Z})$, we make the following definitions. Let S^+ be a nonzero additive subgroup of the integers, i.e., $S^+ = M\mathbb{Z}$ for some positive integer M. Let $S^\times$ be a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$. We also use $S^\times$ to denote the subset of $\mathbb{Z}$ whose image modulo N is in $S^\times$ (If $N = 1$, then we take $S^\times = \mathbb{Z}$). Let n be a positive integer. Define

$$\triangle^n(N, S^\times, S^+) = \{\text{integer matrices } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid N|c, a \in S^\times, b \in S^+, \det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = n\}.$$

$\triangle^1(N, S^\times, S^+)$ is clearly a congruence subgroup of Γ, since it contains $\Gamma(N')$ where N' is the least common multiple of M and N. We have, for example, $\Gamma_0(N) = \triangle^1(N, (\mathbb{Z}/N\mathbb{Z})^*, \mathbb{Z})$.

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

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

We then have the following proposition.

Proposition 4.7. *$f(z)|[\Gamma'\alpha\Gamma']_k$ does not change if α is replaced by any other representative α' of the same double coset: $\Gamma'\alpha'\Gamma' = \Gamma'\alpha\Gamma'$. Nor does it depend on the choice of representatives γ'_j of Γ' modulo Γ''. If $f \in M_k(\Gamma')$, then $f(z)|[\Gamma'\alpha\Gamma']_k \in M_k(\Gamma')$.*

Now, we extend the definition of the Hecke operators.

Definition. Let $\Gamma' = \triangle^1(N, S^\times, S^+)$, and let n be a positive integer. Let $f \in M_k(\Gamma')$. Then

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

where the sum is over all double cosets of Γ' in $\triangle^n(N, S^\times, S^+)$.

By the above proposition, we have $T_n f \in M_k(\Gamma')$.

Equivalently, we can define

$$T_n f = n^{(k/2)-1} \sum f|[\alpha_j]_k$$

where $\Gamma'\alpha_j$ runs through the right cosets of Γ' in $\triangle^n(N, S^\times, S^+)$.

Our earlier definition of the Hecke operators can be shown to agree with the new definition, by applying the following proposition (cf. [4]).

Proposition 4.8. *Let $\triangle^n = \triangle^n(N, \{1\}, \mathbb{Z})$. For each $a \in (\mathbb{Z}/N\mathbb{Z})^*$ we fix $\sigma_a \in \Gamma$ such that $\sigma_a \equiv \left(\begin{smallmatrix} 1/a & 0 \\ 0 & a \end{smallmatrix}\right)$ mod N. We then have*

$$\triangle^n = \bigcup_{disjoint} \Gamma_1(N)\sigma_a \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

where the disjoint union is taken over all postivie a dividing n and prime to N, and for each such a we set $d = n/a$ and take $b = 0, 1, \ldots, d-1$.

Equipped with these concepts, we prove the following theorem.

Theorem 4.9. *Let n be a positive integer. The number of ways that n can be written as a sum of four squares is given by:*

$$a_n = \begin{cases} 8\sigma_1(n) & \textit{for } n \textit{ odd;} \\ 24\sigma_1(n_0) & \textit{for } n = 2^r n_0 \textit{ even, } n_0 \textit{ odd.} \end{cases}$$

where $\sigma_1(n) = \sum_{d|n} d$

Proof. We let $F = \sum_{n\ odd} \sigma_1(n)q^n$, $\Theta^4 = \sum_n a_n q^n \in M_2(\Gamma_0(4))$. a_n is then the number of ways n can be written as a sum of four squares. By Proposition 4.5, since $2|4$ and all the coefficients of even powers of q for F are 0, we have

$$T_2 F = 0.$$

It is shown in [4] that Θ^4 and F span $M_2(\Gamma_0(4))$. Thus, $T_2\Theta^4 = s\Theta^4 + tF$ for some constants s and t. By Proposition 4.5, letting $T_2\Theta^4 = \sum_n b_n q^n$, we have $b_1 = a_2 = 24$ and $b_2 = a_4 = 24$. This yields $s = 1, t = 16$, so

$$T_2\Theta^4 = \Theta^4 + 16F.$$

Therefore, $\{F, \frac{2}{3}F + \frac{1}{24}\Theta^4\}$ is a normalized eigenbasis for T_2.

Consider the case n is odd. T_n commutes with T_2 by Proposition 4.2. Thus, it preserves each one-dimensional eigenspace obtained above, so F and $\frac{2}{3}F + \frac{1}{24}\Theta^4$ are eigenvectors of T_n.

For any n, $n = 2^r n_0$ for some $r \geq 0$ and n_0 odd. By Proposition 4.2, $T_n = T_2^r T_{n_0}$, so $\frac{2}{3}F + \frac{1}{24}\Theta^4$ is an eigenvector for T_n for all $n = 1, 2, \ldots$. Let $f = \frac{2}{3}F + \frac{1}{24}\Theta^4$ and $T_n f = \lambda_n f$.

Denote the n^{th} Fourier coefficient of f by c_n. $c_0 = \frac{1}{24}a_0 = \frac{1}{24}$, which is nonzero. Writing $n = 2^r n_0$ and applying Proposition 4.6, we then have

$$\lambda_n = \sum_{d|n} \chi_{triv}(d) d^{2-1} = \sum_{d|n, 2\nmid d} d = \sigma_1(n_0),$$

and $a_n = \lambda_n = \sigma_1(n_0)$ (which is equal to $\sigma_1(n)$ if n is odd).

If n is odd, then $c_n = \frac{2}{3}\sigma_1(n) + \frac{1}{24}a_n = \sigma_1(n)$, so $a_n = 8\sigma_1(n)$. Otherwise, $n = 2^r n_0$ with $r \geq 1$, so $c_n = \frac{1}{24}a_n = \sigma_1(n_0)$, which yields $a_n = 24\sigma_1(n_0)$. This proves the desired result.

We have just seen that the study of the theta function Θ^k may give the exact answer for the number of ways of writing an integer as a sum of k squares. More generally, given a quadratic form $\sum_{j,l=1}^{k} A_{jl}n_j n_l = [n]^t A[n]$, where $A = [A_{jl}]$ is a given symmetric matrix and $[n]$ is a column vector with k even, we can use $\sum_n q^{[n]^t A[n]}$ to construct modular forms of weight $k/2$. The properties of modular forms are then useful in studying the number of representations $m = [n]^t A[n]$. Therefore, it is necessary to define modular forms of half integer weight for the study of quadratic forms in odd number of variables.

First, we define

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

$$\tilde{\Gamma'} \equiv \{(\gamma, j(\gamma, z)) | \gamma \in \Gamma'\}, \quad \tilde{\gamma} \equiv (\gamma, j(\gamma, z)).$$

Definition. Let k be any integer, and let $\Gamma' \subset \Gamma_0(4)$ be a subgroup of finite index. Let $f(z)$ be a meromorphic function on the upper half-plane H which is invariant under $[\tilde{\gamma}]_{k/2}$ for all $\tilde{\gamma} \in \tilde{\Gamma}'$. We say that $f(z)$ is a **modular function of weight** $k/2$ for $\tilde{\Gamma}'$ if f is meromorphic at every cusp of Γ'. We say that such an $f(z)$ is a modular form and write $f \in M_{k/2}(\tilde{\Gamma}')$, if it is holomorphic on H and at every cusp. We say that a modular form f is a cusp form and write f $\in S_{k/2}(\tilde{\Gamma}')$, if it vanishes at every cusp.

For a quadratic form Q in n variables, we define its theta function to be

$$\Theta_Q(z) = \sum_{m \in \mathbb{Z}} r_Q(m) e^{2\pi i m z}$$

where $r_Q(m)$ is the number of representations of m by Q. It is shown in Shimura [6] that

Theorem 4.10. *Let N be the level of Q. Then,*

$$\Theta_Q \in M_{n/2}(N, \chi_d)$$

where $d = det(A)$ if $n \equiv 0 \pmod 4$, $d = -det(A)$ if $n \equiv 2 \pmod 4$, and $d = det(A)/2$ if n is odd.

The study of such theta functions involves a special kind of modular form known as "Eisenstein series." The **Eisenstein series** for an even integer $k \geq 4$ is defined to be

$$E_k(z) = \sum \frac{1}{(mz+n)^k}$$

where the sum is over $m, n \in \mathbb{Z}$ with $g.c.d.(m,n) = 1$ and only one pair taken from $(m,n), (m,-n)$. It is a modular form of weight $k/2$, and we can show as in [4] that

$$E_k(z) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} j(\gamma, z)^{-k}$$

This motivates us to have the following definition:

Definition. Let k be an odd integer, $k \geq 5$.

$$E_{k/2}(z) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(4)} j(\gamma, z)^{-k}.$$

Given a quadratic form Q in n variables with $n > 4$, its theta function can be written as

$$\Theta_Q(z) = E(z) + f(z)$$

as the sum of an Eisenstein series $E(z)$ and a cusp form $f(z)$ (cf. [7]). If the genus of the form Q contains only one class, then due to Siegel, $\Theta_Q(z) = E(z)$ and we can obtain the exact formulas for the theta function coefficients, i.e., the number of representations n by the form Q (cf. [7]). Otherwise, it is necessary to find the cusp form $f(z)$. We can use this method for the quadratic forms in n variables with $n \leq 4$, by extending the definition of Eisenstein series to the case $n \geq 2$ as in Vepkhvadze [7].

5 The Proof of the 15-Theorem

5.1 Escalators of dimension 1, 2 and 3

The zero-dimensional lattice can be escalated uniquely to the lattice generated by a single vector of norm 1. This one-dimensional escalator lattice corresponds to the form x^2, or in the matrix form, (1). This does not represent 2, so its escalator can be written in matrix form that

$$\begin{pmatrix} 1 & a \\ a & 2 \end{pmatrix}$$

By Cauchy-Schwarz inequality, $a^2 \leq 2$, which implies $a = 0, \pm 1$. The matrices with $a = \pm 1$ are isometric, so the non-isometric Minkowski-reduced Gram matrices for the two-dimensional escalators are:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

In the same manner, we obtain exactly 9 non-isometric three-dimensional escalators whose Minkowski-reduced Gram matrices are given by:

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

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}.$$

5.2 Four-dimensional Escalators

Escalating the nine three-dimensional escalators given in the previous section, we get exactly 207 non-isomorphic four-dimensional escalator lattices. All such lattices are of the form $(1) \oplus L$, and the 207 values of L are listed in Table 3 of [1].

We now show that 201 of these 207 escalators are universal and cannot be escalated more. For each four-dimensional escalator lattice L_4, we find three-dimensional sub-lattice L_3 which represents a large set of integers. We typically achieve this by choosing L_3 to be unique in its genus, in which case L_3 represents all integers it represents locally. We let the Gram matrix of the orthogonal complement of L_3 in L_4 be (m), so that the direct sum $L_3 \oplus (m)$ lies in L_4. Then, the direct sum can be shown to represent all sufficiently large integers $n \geq N$. By a direct check of the representability of numbers less than N by L_4, we get the desired result.

For example, we consider escalator lattices (denoted L_4) of the three-dimensional escalator lattice L_3 having the Gram matrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \text{ (labelled (4) of Table 1, [1])}$$

As we checked in Section 3.2, L_3 is unique in its genus, and represents all numbers except those of the form $2^e(8k+7)$ where e is even. Suppose L_4 is not universal, and let u be the least positive integer not represented by L_4. Since the direct sum $L_3 \oplus (m)$ lies in L_4, u must be of the form $2^e(8k+7)$. Moreover, u is square-free (Otherwise, $u = rt^2$ with $t > 1$, and r is not represented by L_4 and less than u). Thus, $u \equiv 7 \pmod 8$.

If $m \not\equiv 0, 3,$ or $7 \pmod 8$, then clearly $u - m$ is not of the form $2^e(8k+7)$. If $m \equiv 3$ or $7 \pmod 8$, then $u - 4m$ is not of the form $2^e(8k+7)$. Thus, if $m \not\equiv 0 \pmod 8$, either $u - m$ or $u - 4m$ is represented by L_3, hence u is represented by L_4. This shows that in the case $m \not\equiv 0 \pmod 8$, L_4 represents all numbers $\geq 4m$.

By direct calcualtion, it is easy to see that $m \leq 28$ for all the 26 escalations. For example, one of the escalations has Gram matrix $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 7 \end{pmatrix}$, and contains the lattice with the associate matrix $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 2 & 28 \end{pmatrix}$ which is isometric to $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 26 \end{pmatrix}$, so $m = 26$ in this case. The explicit computation up to $4 \times 28 = 112$ reveals that L_4 is universal for the case $m \not\equiv 0 \pmod 8$. We call the escalations for which m happens to be a multiple of 8 "exceptional." It turns out that exactly two of the 26 escalations of L_3 are exceptional. For these lattices, we find new sub-lattices L_3 which are unique in their genus, and apply the exactly same argument. For example, we consider the lattice with the Gram matrix $\begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 2 & 1 & 1 & 7 \end{pmatrix}$. We note that L_3 having the Gram matrix $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 3 \end{pmatrix}$ lies in L_4 and is unique in its genus. A local check shows that L_3 represents all numbers except those of the form

$5^d u_+$ (where d is odd and u_+ denotes a number which is a quadratic residue modulo 5), so denoting u to be first integer not represented by L_4, u is of this form. Since we get $m = 40$, either $u - m$ or $u - 4m$ is not of the form $5^d u_+$. A direct check up to 160 shows that the lattice is indeed universal.

All of the 3-dimensional escalator lattices in Table 1 of [1] except the one labeled (6), which has the Gram matrix $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 4 \end{pmatrix}$, can be easily shown to be unique in their genus, and the same argument works for the most of their escalations with a few exceptions. The escalator (6) contains the lattice $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 2 \\ 0 & 2 & 8 \end{pmatrix}$, which is unique in its genus, and the lattices $\begin{pmatrix} 2 & -2 & 2 \\ -2 & 5 & 2 \\ 2 & 2 & 8 \end{pmatrix}$ and $\begin{pmatrix} 3 & 0 & 0 \\ 0 & 5 & 4 \\ 0 & 4 & 5 \end{pmatrix}$, which together form a genus. A local check shows that the first genus represents all numbers which are $\not\equiv 2$ or $3 \pmod 4$, and that the second genus represents all numbers $\not\equiv 1 \pmod 3$. Therefore, the lattice (6) represents all positive integers $\not\equiv 7$ or $10 \pmod{12}$. We now can apply the identical method as above to prove the universality of non-exceptional four-dimensional escalators of the lattice (6). The details are summarized in Table 1 in [1].

"Exceptional" lattices arise only from the lattices labeled (4), (6), and (7) in Table 1 of [1]. Two arise for escalator (4). Four exceptional ones arise for escalator (6), but two of them are non-exceptional escalations of (1) and (8) respectively, which are proven to be universal. Similarly, two arise for escalator (7), and one of them is a non-exceptional escalation of (9). Therefore, we need to consider only five exceptional escalators, and these can be handled similarly as the exceptional case for (4) shown earlier. Namely, we find new sub-lattice L_3 unique in its genus and apply the identical argument. The relevant details are illustrated in Table 2 in [1]. This proves the universality of the 201 four-dimensional escalators.

5.3 Five-dimensional Escalators

The remaining six nonuniversal four-dimensional lattices are italicized in Table 3 of [1]. They go through all the arguments in the second paragraph of the previous section, except for the final check. The final check reveals that they represent all numbers except a single integer as given in Table 4, [1]. Therefore, the five-dimensional lattices escalated from these six escalators are universal. By explicit calculation, we obtain 1630 five-dimensional universal escalators.

In summary, there are only a finite number of escalators for quadratic forms having integer matrices: 1 of dimension zero, 1 of dimension one, 2 of dimension two, 9 of dimension three, 207 of dimension four, and 1630 of dimension five, for a total of 1850.

5.4 The Proof of the Fifteen Theorem

The analysis done in previous sections essentially proves the Fifteen Theorem. It is obvious that

Theorem 5.1 *Any universal lattice L contains a universal sub-lattice of dimension at most five.*

This is true since there exists an escalator sequence $0 = L_0 \subseteq L_1 \subseteq \ldots$ within L, and by Section 5.2 and 5.3, either L_4 or (when defined) L_5 gives a universal escalator sub-lattice of L.

Since only the critical integers defined in the Fifteen Theorem arise as truants of escalator lattices, Theorem 2.1 clearly holds. Furthermore, it can be shown that for each critical number t, there is a quaternary diagonal form that fails to represent t, but represents every other positive integer. Nine such forms of minimal determinant are $[2, 2, 3, 4]$ with truant 1, $[1, 3, 3, 5]$ with truant 2, $[1, 1, 4, 6]$ with truant 3, $[1, 2, 6, 6]$ with truant 5, $[1, 1, 3, 7]$ with truant 6, $[1, 1, 1, 9]$ with truant 7, $[1, 2, 3, 11]$ with truant 10, $[1, 1, 2, 15]$ with truant 14, and $[1, 2, 5, 5]$ with truant 15 (here, $[a, b, c, d]$ denotes the form $ax^2 + by^2 + cz^2 + dw^2$). This proves Theorem 2.2.

We find that there are only four escalator lattices having truant 15. As shown in Section 5.3, each of these four escalators represents every integer greater than 15, from which Theorem 2.3 follows. For each critical number t less than 15, we can find a form which fails to represent infinitely many integers including t. This proves Theorem 2.4. Lastly, Theorem 2.5 follows from Section 5.2. The list of the 204 universal quaternary forms is given in Table 5, [1].

6 The Proof of the 290-Theorem

Although proving the Fifteen Theorem was rather simple, the proof of the 290-Theorem involves much more complicated methods using modular forms. As in the previous section, we first consider small-dimensional escalators for quadratic forms with integer coefficients.

6.1 Escalators of dimension 1, 2, and 3

The zero-dimensional lattice can be escalated uniquely to the lattice generated by a single vector of norm 1. This one-dimensional escalator lattice corresponds to the form x^2, or in the matrix form, (1). This does not represent 2, so its escalator can be written in matrix form that

$$\begin{pmatrix} 1 & a \\ a & 2 \end{pmatrix}$$

By Cauchy-Schwarz inequality, $a^2 \leq 2$, which implies $a = 0, \pm 1/2$ or ± 1. The matrices with $a = \pm 1/2$ are isometric, and so do the matrices with $a = \pm 1$. Therefore, we have exactly three non-isometric two-dimensional escalators having Gram matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1/2 \\ 1/2 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}.$$

The truants of these escalators are $3, 3$, and 5 respectively. In the same manner, we escalate each of these to obtain precisely 34 non-isometric three-dimensional escalators with Gram matrices:

$$\begin{pmatrix}1&1/2&0\\1/2&1&1/2\\0&1/2&1\end{pmatrix},\ \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},\ \begin{pmatrix}1&1/2&0\\1/2&1&1/2\\0&1/2&2\end{pmatrix},\ \begin{pmatrix}1&1/2&0\\1/2&1&0\\0&0&2\end{pmatrix},\ \begin{pmatrix}1&0&0\\0&1&1/2\\0&1/2&2\end{pmatrix},$$

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&2\end{pmatrix},\ \begin{pmatrix}1&0&1/2\\0&1&1/2\\1/2&1/2&3\end{pmatrix},\ \begin{pmatrix}1&1/2&1/2\\1/2&2&-1/2\\1/2&-1/2&2\end{pmatrix},\ \begin{pmatrix}1&0&1/2\\0&1&0\\1/2&0&3\end{pmatrix},\ \begin{pmatrix}1&0&0\\0&1&0\\0&0&3\end{pmatrix},$$

$$\begin{pmatrix}1&1/2&1/2\\1/2&2&1/2\\1/2&1/2&2\end{pmatrix},\ \begin{pmatrix}1&1/2&0\\1/2&2&1/2\\0&1/2&2\end{pmatrix},\ \begin{pmatrix}1&1/2&0\\1/2&2&0\\0&0&2\end{pmatrix},\ \begin{pmatrix}1&0&0\\0&2&1/2\\0&1/2&2\end{pmatrix},\ \begin{pmatrix}1&0&0\\0&2&0\\0&0&2\end{pmatrix},$$

$$\begin{pmatrix}1&1/2&-1/2\\1/2&2&1/2\\-1/2&1/2&3\end{pmatrix},\ \begin{pmatrix}1&0&1/2\\0&2&1\\1/2&1&3\end{pmatrix},\ \begin{pmatrix}1&1/2&1/2\\1/2&2&0\\1/2&0&3\end{pmatrix},\ \begin{pmatrix}1&1/2&0\\1/2&2&1/2\\0&1/2&3\end{pmatrix},$$

$$\begin{pmatrix}1&1/2&0\\1/2&2&0\\0&0&3\end{pmatrix},\ \begin{pmatrix}1&0&1/2\\0&2&1/2\\1/2&1/2&3\end{pmatrix},\ \begin{pmatrix}1&0&1/2\\0&2&0\\1/2&0&3\end{pmatrix},\ \begin{pmatrix}1&0&0\\0&2&1/2\\0&1/2&3\end{pmatrix},\ \begin{pmatrix}1&0&0\\0&2&0\\0&0&3\end{pmatrix},$$

$$\begin{pmatrix}1&0&0\\0&2&1\\0&1&4\end{pmatrix},\ \begin{pmatrix}1&0&1/2\\0&2&1/2\\1/2&1/2&4\end{pmatrix},\ \begin{pmatrix}1&0&0\\0&2&1/2\\0&1/2&4\end{pmatrix},\ \begin{pmatrix}1&0&0\\0&2&0\\0&0&4\end{pmatrix},\ \begin{pmatrix}1&0&1/2\\0&2&1\\1/2&1&5\end{pmatrix},$$

$$\begin{pmatrix}1&0&1/2\\0&2&1/2\\1/2&1/2&5\end{pmatrix},\ \begin{pmatrix}1&0&1/2\\0&2&0\\1/2&0&5\end{pmatrix},\ \begin{pmatrix}1&0&0\\0&2&1/2\\0&1/2&5\end{pmatrix},\ \begin{pmatrix}1&0&1/2\\0&2&1\\1/2&1&5\end{pmatrix},\ \begin{pmatrix}1&0&0\\0&2&0\\0&0&5\end{pmatrix}.$$

These are all nonuniversal, having truants respectively:

14, 7, 5, 10, 21,
14, 6, 10, 22, 6,
6, 13, 5, 10, 7,
17, 14, 10, 5,
6, 7, 10, 23, 10,
7, 29, 31, 14, 10,
7, 29, 10, 13, 10.

6.2 The Basic four-dimensional escalators

Escalating each of the above 34 three-dimensional escalators, we obtain exactly 6560 nonisometric four-dimensional escalator lattices. We call these the **basic** four-dimensional escalators. Other four-dimensional escalators can be obtained by a sequence of escalations of the basic escalators. Since most of the basic escalators turn out to be either universal or represent a large set of numbers, we essentially need to study only these escalators. To determine precisely which numbers are represented by these lattices, we adopt two methods. One is the arithmetic method as we did in the proof of the Fifteen Theorem, and another is the analytic method invoking modular forms.

6.3 Arithmetic methods

We apply the almost identical arguments used in Section 5.2, now for quadratic forms with integer coefficients. Of the 34 three-dimensional escalators lattices, 20 of them are unique in their genus and therefore represent all numbers they represent locally. Most of the four-dimensional escalators of the 20 lattices can be handled similarly as in Section 5.2. The exactly same procedure used for the form $x^2 + 2y^2 + 2x^2$ can be applied to the escalations of the 17 of the 20 escalators, which are $\sharp$1-8, 10-12, 17, 19, 21, 22, 24, and 34 listed in Section 6.1. This determines what integers are represented by 1658 of the 6560 basic four-dimensional escalators.

However, the arithmetic method does not work for the most of the escalations of other L_3's. Direct calculation shows that more than 2300 of the 6560 escalators contain no three-dimensional form of class number one. Thus, an alternative method is necessary to deal with the remaining four-dimensional escalators.

6.4 Analytic methods

In order to determine what numbers are represented by the four-dimensional escalators which could not be dealt with the arithmetic method in the previous section, we invoke the theory of modular forms. For a positive definite integer-valued quadratic form Q in n variables, the theta function

$$\Theta_Q(z) = \sum_{m \in \mathbb{Z}} r_Q(m) e^{2\pi i m z}$$

is a modular form of weight $n/2$ for some congruence subgroup $\Gamma_0(N) \subseteq SL(2, \mathbb{Z})$ where N is the level of the form Q and $r_Q(m)$ is the number of representations of m by Q. As in Section 4, we write

$$\Theta_Q(z) = E(z) + f(z)$$

as the sum of an Eisenstein series $E(z)$ and a cusp form $f(z)$.

We say that a prime p is **anistropic** for Q if for every vector $\vec{x} \in \mathbb{Q}_p^n$ with $Q(\vec{x}) = 0$, we have $\vec{x} = 0$. If this is not so, we say that a prime p is **isotropic** for Q. By local consideration, all of the basic four-dimensional escalators can be shown to have no anistropic primes.

Then, we can obtain a bound for each basic escalator Q such that if m is locally represented by Q and greater than the bound, then m is represented by Q. The Fourier coefficients of its Eisenstein series and cusp form have different growth rates as $m \to \infty$. The Eisenstein coefficients $a_E(m)$ are always non-negative and grow more quickly than the cusp form coefficients $a_f(m)$. We will determine an effective lower bound for $a_E(m)$ and an effective upper bound for $|a_f(m)|$. From those bounds, we can obtain a bound for m to ensure $\frac{a_E(m)}{|a_f(m)|} > 0$, which implies $r_Q(m) > 0$ so that m is represented by Q.

6.4.1 Eisenstein coefficients $a_E(m)$

Due to Siegel, we have the Eisenstein coefficients of a quadratic form Q in n variables as weighted averages over the genus of Q denoted by Gen(Q):

$$a_E(m) = \frac{\sum_{Q' \in \mathrm{Gen}(Q)} \frac{r_{Q'}(m)}{|\mathrm{Aut}(Q')|}}{\sum_{Q' \in \mathrm{Gen}(Q)} \frac{1}{|\mathrm{Aut}(Q')|}}$$

as shown in [5].

On the other hand, we define the **local representation density** $\beta_v(m)$ at a place v of $\mathbb{Q}$ by

$$\beta_v(m) = \lim_{U \to \ \{m\}} \frac{\mathrm{Vol}(Q^{-1}(U))}{\mathrm{Vol}(U)},$$

where U is an open neighborhood of m in $\mathbb{Q}_v$, the completion v of $\mathbb{Q}$. We use the usual measure on $\mathbb{R}$, and the Haar measure on $\mathbb{Q}_p$ normalized so that $\mathrm{Vol}(\mathbb{Z}_p) = 1$. The $\beta_v(m)$ gives a measure of the number of local representations of m over $\mathbb{Q}_v$. The real local density at $\beta_\infty(m)$ can be computed as the volume of the real ellipsoid $Q(x) = m$, while the local density at each prime p is given by reduction mod p^r as

$$\beta_p(m) = \lim_{r \to \infty} \frac{\sharp\{\vec{x} \in (\mathbb{Z}/p^r\mathbb{Z})^n | Q(\vec{x}) \equiv m \pmod{p^r}\}}{p^{(n-1)(r-1)}}$$

This counts roughly the normalized number of representations of m by Q over $\mathbb{Z}_p$.

When $n \geq 3$, due to Siegel, we have that

$$a_E(m) = \prod_v \beta_v(m)$$

where the product runs over all places v of $\mathbb{Q}$ (cf. [5]).

The effective lower bound for $a_E(m)$ will therefore follow from reasonable lower bounds for each of the local densities $\beta_v(m)$. Before stating the theorem giving a lower bound for the case $n = 4$, we make some relevant definitions.

Definition. We define a number m to be **p-stable** if m is locally represented at p, and for all $k \gg 1$, the quantity $r_{p^k}^{Good}(p^{2v}m) + r_{p^k}^{Bad}(p^{2v}m)$ is constant for all $v \geq 1$.

When $n \geq 4$, for each $T \in \mathbb{Z}$ we let Stable(T) be the set of all primes p such that T is p-stable.

We say that an integer $m \in \mathbb{Z}$ is **supported** on some set $\mathbb{S}$ of primes if $|m|_p = 1$ for all $p \notin \mathbb{S}$. Let $\mathcal{J}$ to be a finite union of square classes $t(\mathbb{Z})^2$ with $t \in \mathbb{Z}$ and $\mathrm{ord}_p(t) \leq 1$ at all primes p. We denote $\mathcal{B}_\mathcal{J} \subset \mathcal{J}$ be a minimal finite subset such that any locally represented $m \in \mathcal{J}$ can be written as $m = T'(m')^2$ with $T' \in \mathcal{B}_\mathcal{J}$ and $m' \in \mathbb{Z}$ supported on Stable(T'). Without loss of generality, we can assume that $\prod_v |T'|_v = 1$ for all $T' \in \mathcal{B}_\mathcal{J}$ (cf. [5]).

We further denote the quadratic Dirichlet character $\Phi_n(\cdot) = \left(\frac{(-1)^{n/2}D}{\cdot}\right)$ (when n is even) where D is the determinant of a given quadratic form.

Theorem 6.1. *When $n = 4$ and m is locally represented by Q which is a basic four-dimensional escalator form with level N and determinant D, we have the lower bound*

$$a_E(m) \geq C_E m \prod_{p|m,\ p\nmid N,\ \chi(p)=-1} \frac{p-1}{p+1}$$

where

$$C_E = \min_{T' \in \mathcal{B}_{\mathcal{J}}} \{ \frac{2\omega_4 D^{-1/2}}{L(2,\chi)} \prod_{p|N} \frac{\beta_p(T')}{1-\chi(p)/p^2} \prod_{p \in Stable(T'),\ p|N} C'_p(T') \}.$$

Proof. We first note that Q has no anistropic prime. Let $T^{'} \in \mathbb{Z}$ with $\mathrm{ord}_p(T') \leq 1$ for all $p \nmid N$ and $\prod_v |T'|_v = 1$. Consider $m = T'(m')^2 \in T'\mathbb{Z}^2$ with m' supported on Stable(T').

Denoting the volumn of 4-dimensional sphere in $\mathbb{R}^4$ by ω_4, we know from Siegel's theory that

$$\beta_v(m) = \frac{4}{2}\omega_4 D^{-1/2} m^{\frac{4-2}{2}} = 2\omega_4 D^{-1/2} m$$

at a real valuation $v \mid \infty$ (cf. [5]).

Let

$$C_p(T') = \frac{p^2}{p^2-1} \frac{\beta_p^{Good \cup Bad}(p^2 T')}{\beta_p(T')}.$$

Then, by applying reduction maps, we can show that when m is p-stable,

$$\frac{a_E(mp^{2v})}{p^v} \to C_p(m) a_E(m) \text{ monotonically as } v \to \infty,$$

which implies $\beta_p(m) \geq C'_p(T')\beta_p(T')$ where $C'_p(T') = \min\{1, C_p(T')\}$ (cf. [5]).

Using these, we can show by applying reduction maps as in [5] that

$$a_E(m) \geq a_E(T')(m')^2 \prod_{p \in Stable(T')} C'_p(T').$$

It is clear that the quadratic character Φ_4 (associated to Q) is independent of m. Since $\mathrm{ord}_p(T') \leq 1$ for all $p \nmid N$, by Table 1 in [5],

$$\begin{aligned}
\prod_{p\nmid N} \beta_p(T') &= \prod_{p \nmid NT'} \left(1 - \frac{\Phi_4(p)}{p^{4/2}}\right) \prod_{p|T',\ p\nmid N} \frac{(p^{(4-2)/2} + \Phi_4(p))(p^{4/2} - \Phi_4(p))}{p^{4-1}} \\
&= \prod_{p\nmid N} \left(1 - \frac{\Phi_4(p)}{p^2}\right) \prod_{p|T',\ p\nmid N} \frac{(p+\Phi_4(p))(p^2 - \Phi_4(p))}{p(p^2 - \Phi_4(p))} \\
&\geq \prod_{p\nmid N} \left(1 - \frac{\Phi_4(p)}{p^2}\right) \prod_{p|T',\ p\nmid N,\ \Phi_4(p)=-1} \left(1 - \frac{1}{p}\right).
\end{aligned}$$

This implies

$$a_E(T') \geq \frac{T'}{L(2,\chi)} \prod_{p|N} \frac{\beta_p(T')}{1-\chi(p)/p^2} \prod_{v|\infty} \beta_v(1) \prod_{p|T',\ p\nmid N,\ \chi(p)=-1} \left(1 - \frac{1}{p}\right).$$

By Table 2 of [5], $C'_p(T') = 1$ unless $p \nmid T'$ and $\Phi_4(p) = -1$, in which case $C'_p(T')$ is the local factor at p of $\zeta(4-2)/\zeta((4-2)/2) = \zeta(2)/\zeta(1)$. We thus have

$$\begin{aligned} a_E(m) \;\; &\geq \;\; \frac{m(2\omega_4 D^{-1/2})}{L(2,\chi)} \prod_{p|N} \frac{\beta_p(T')}{1-\chi(p)/p^2} \prod_{p \in Stable(T'),\; p|N} C'_p(T') \\ &\times \prod_{p|T',\; p\nmid N,\; \chi(p)=-1} \left(1 - \frac{1}{p}\right) \prod_{p|m',\; p\nmid N,\; \chi(p)=-1} \left(1 + \frac{1}{p}\right)^{-1}. \end{aligned}$$

Taking the minimum over all $T' \in \mathcal{B}_{\mathcal{J}}$, we have the desired inequality.

The actual computation of C_E involves calculations of all possible local densities $\beta_p(m)$ at all primes. When $p \mid 2\det(2Q)$ this is accomplished using the explicit reduction maps with congruence conditions as described in [5], while for $p = 2$, we additionally need to count points on certain ellipsoids (with congruence conditions) over $\mathbb{Z}/8\mathbb{Z}$.

6.4.2 The cusp form coefficients $a_f(m)$

For the cusp form $f(z)$ appearing in the theta function $\Theta_Q(z)$, we write

$$f(z) = \sum_{i=1}^{r} \gamma_i f_i(z) \text{ for some } \gamma_i \in \mathbb{C}$$

as a linear combination of the Hecke eigenforms $f_i(z)$ normalized so that their first nonzero Fourier coefficients $a_i(m) = 1$. By the theory of new forms and Deligne's bound on Hecke eigenvalues, we have

$$|a_f(m)| \leq C_f \tau(m) \sqrt{m}$$

where $C_f = \sum |\gamma_i|$ and $\tau(m)$ is the number of positive divisors of m (cf. [5]). To find the γ_i's, we write the new part $f^{new}(z)$ of $f(z)$ as a sum over Galois-conjugate newforms $f_j(z)$. Since all $a_f(m)$ are rational, $\gamma_{i'} = \gamma_i^\sigma$ if $f_{i'} = f_i^\sigma$ for some embedding $\sigma : K_j := \mathbb{Q}(a_i(m)) \to \bar{\mathbb{Q}}$, and we have that

$$f(z) = \sum_j \sum_{\sigma : K_j \to \bar{\mathbb{Q}}} (\gamma_j f_j(z))^\sigma = \sum_{m>0} \sum_j \operatorname{Tr}_{K_j/\mathbb{Q}}(\gamma_j a_j(m)).$$

By regarding both γ_j and $a_j(m)$ as vectors over $\mathbb{Q}$ in the basis given by powers of some α_j such that $K_j = \mathbb{Q}(\alpha_j)$, and by finding the rational trace matrix for this basis, we can exactly determine the γ_i's by simultaneously solving these rational linear equations for sufficiently many m. By repeating this procedure to solve for the components of $f - f^{new}$ in $\operatorname{Span}\{f_j(dz)\}$ for each possible $d \mid N$, we can completely decompose f into its Galois-conjugate components. Then, C_f can be obtained by summing the absolute values of all embeddings γ_i^σ over all possible d.

6.4.3 The explicit bound for representability

Combining the bounds for $a_E(m)$ and $a_f(m)$ yields that if m is locally represented by Q and satisfies

$$\frac{\sqrt{m}}{\tau(m)} \prod_{p \nmid N, p|m, \chi(p)=-1} \frac{p-1}{p+1} > \frac{C_f}{C_E} \tag{6}$$

then m is represented by Q.

Lemma 6.2. *Let*

$$B(m) = \frac{\sqrt{m}}{\tau(m)} \prod_{p \nmid N, p|m, \chi(p)=-1} \frac{p-1}{p+1}.$$

Then B(m) is a multiplicative function and for any prime p, we have

$$B(mp^v) > B(m)$$

when either $p \geq 11$ and $v \geq 1$, $p = 7$ or 5 and $v \geq 2$, $p = 3$ and $v \geq 5$, or $p = 2$ and $v \geq 11$.

Proof. $B(ab) = B(a)B(b)$ trivially when $\gcd(a,b) = 1$, so $B(m)$ is multiplicative.

Now, write $m = m_1 p^{v_1}$ where $p \nmid m_1$. Then,

$$\begin{aligned} B(mp^v) &= \frac{p^{v/2}\sqrt{m_1 p^{v_1}}}{(1+v_1+v)\tau(m_1)} \prod_{p' \nmid N, p'|mp, \chi(p')=-1} \frac{p'-1}{p'+1} \\ &\geq \frac{p^{v/2}(p-1)}{p+1} \frac{1+v_1}{1+v_1+v} B(m) \\ &\geq \frac{p^{v/2}(p-1)}{p+1} \frac{1}{1+v} B(m). \end{aligned}$$

We note that if either p or v is sufficiently large, then

$$\frac{p^{v/2}(p-1)}{p+1} \frac{1}{1+v} > 1.$$

By direct calculation, we see that the above inequality is satisfied when either $p \geq 11$ and $v \geq 1$, $p = 7$ or 5 and $v \geq 2$, $p = 3$ and $v \geq 5$, or $p = 2$ and $v \geq 11$.

The lemma implies that we need to check the representability for only finitely many numbers.

In general, the size of the Eisenstein bound C_E is small whereas the cusp form bound C_f is large, which makes it difficult to check the representability of numbers not satisfying the inequality. For example, of the 6560 quaternary escalator forms, the largest bound $\frac{C_f}{C_E}$ arises from $Q(\vec{x}) = x^2 + 2y^2 + 4z^2 + 31w^2 + yz - yw + 3zw$, which has level $N = 3744$ and $\chi(\cdot) = (\frac{104}{\cdot})$. For this form, we can compute $C_E = \frac{36}{125}$ and $C_f \approx 2331.99 < 2332.99$, giving the overall bound $\frac{C_f}{C_E} < 8100.65$.

6.5 Computational methods

We call an integer m **eligible** for a quaternary quadratic form Q if m is locally represented by Q but (6) does not hold. There are only finitely many eligible numbers as shown in the previous section, and we now present the computational methods to quickly determine which of them are represented by Q.

6.5.1 Generating eligible numbers

We let $B(m)$ denote the left side of (6). It is clear that $B(m)$ is multiplicative (from Lemma 6.2) and $B(p) > 1$ for all primes $p > 7$. Therefore, all prime divisors p of an eligible number m satisfy

$$B(p) < \frac{C_f/C_E}{B(2)B(3)B(5)B(7)}$$

This gives an explicit set of possible prime divisors of m. We call such primes p **eligible primes**, although they may not themselves be eligible numbers. We also reorder the eligible primes so that their "size" refers to the size of their $B(p)$.

We then take the product of the smallest eligible primes p_i and check how many primes are needed to ensure that $p_1 \cdots p_{s+1}$ is not eligible. This determines the maximum possible number of distinct prime divisors in any eligible number m, and we can efficiently generate all eligible numbers as products of at most s eligible primes.

The process of generating the list of square-free eligible numbers $t = p_1 \cdots p_r$ arising as products of r eligible distinct primes is as follows. We first take the p_i's to be the smallest r eligible primes, and increase p_r until t is no longer eligible. When this happens, we increment p_{r-1} to the next eligible prime, and set p_r to be the first eligible primes $> p_{r-1}$. If this t is eligible, then we keep increasing p_r as before, but if not, then we increment p_{r-2} and set p_{r-1} and p_r equal to the next two eligible primes greater than p_{r-2}. Repeating this step for each $r \leq s$, we produce all square-free eligible numbers t.

Since it is time-consuming to compute the exact value of $B(p)$ for all eligible primes p, we only compute this for all $p < 10^4$ and approximate $B(p) \approx \frac{\sqrt{p}}{2}\left(1 - \frac{1}{p}\right) < B(p)$, for $p > 10^4$.

6.5.2 Checking eligible numbers

After generating a set of eligible numbers m, we need to find a method to quickly check if m is represented by Q. We exactly follow Bhargava's method for the computation here. Theoretically, by computing the first $m + 1$ Fourier coefficients of the theta function of Q by finding the lengths of all vectors in some large ellipsoid, we can check whether the coefficient $r_Q(m) = 0$ for each m. However, this way is not practical, since computing the theta function up to precision X takes time $\approx X^{\dim(Q)/2} = X^2$, which is slow for large precisions, and the precision we need may be too large to reasonably store.

We resolve this problem by reducing the required theta function precision by finding a **split local cover** for each quaternary Q, by which we mean a sublattice of L on which the form Q splits as $Q' = dx^2 \oplus T$ for some $d \in \mathbb{N}$ and some ternary form T, with Q and Q' representing the same numbers locally. We choose a split local cover for which d is minimal, and calculate whether each m is represented by Q' (hence by Q), and then determine the representability by Q of the remaining set of possible exceptions of Q'. Bhargava did this calculation for the quadratic forms by computing $\Theta_Q(z)$ up to precision $10,000$, which suffices for all possible exceptions that arise.

Given a split local cover Q', we check if Q' represents m by finding the largest value of dx_0^2 less than m and checking if $m - dx_0^2$ is represented by T. If not, then we decrement x_0 and repeat the step, until either we find that Q' represents m or we exceed the precomputed precision Y of the ternary theta function $\Theta_T(z)$. To ensure $m - dx_0^2 < Y$, we must have ternary precision $Y \approx 2d\sqrt{X}$. Bhargava computed the $\Theta_T(z)$ to precision $\approx 10d\sqrt{X}$, which allowed him at least 5 attempts for each eligible number m to verify $r_{Q'}(m) > 0$.

The time needed to compute the ternary theta function $\Theta_T(z)$ up to precision Y is $\approx Y^{\frac{3}{2}}$. In order to decrease the time, we instead compute an **approximate Boolean theta function**, which keeps a single bit describing whether $T(\vec{y}) = m$ has a solution in an appropriately chosen small rectangular cylinder in the ellipsoid $T(\vec{y}) \leq Y$. It can be shown that the eligible numbers we are considering are primitively represented by the spinor genus of T, which means they have a bounded divisibility at the anisotropic primes, and we avoid the certain numbers in finitely many "spinor square classes" (cf. [2]). Therefore, by the equidistribution results of Duke and Shulze-Pillot, the intersection of the cylinder with the ellipsoid $T(x) = m$ has a roughly constant number of integer points (cf. [2]). This implies that we need to check about $\sqrt{Y}$ vectors. By choosing the short dimensions of the cylinder to be large enough, we can find most of the numbers represented by T, although a few may be missed. These few omissions are not important because we make several attempts to verify the representability of each m.

The combined use of a split local cover and an approximate Boolean theta function to check representability of all $m < X$ by Q requires us to store $\sqrt{X}$ bits and takes $O(X^{\frac{1}{4}})$ time, which is good enough.

6.5.3 Error checking and precision issues

In this section, we consider the errors that can possibly occur during the computation and the related precisions, which is entirely due to Bhargava's computer programming codes. Bhargava wrote the code for this computation in Magma for escalations and embeddings and in C++ for the analytic method. Its source can be found at Bhargava and Hanke's website [8].

Local density and lower bound accuracy checking - The local density computations for finding the Eisenstein constant C_E are complicated when $p \mid 2\det(2Q)$, hence prone to subtle errors. For each form Q and all $m < 100$, Bhargava verified Siegel's formula by computing the infinite product of local densities in C++ and checking that this agrees with $E(z)$ computed as the weighted average of theta functions over all classes in the genus of Q (in Magma).

Furthermore, the lower bound C_E is checked for accuracy by comparing it with the naive constant satisfied by the first $10,000$ coefficients of $E(z)$. In all cases, this naive constant is turned out to be $\geq C_E$, and their difference is less than 10^{-3}.

Roundoff error tolerance - All C++ integer computations with the potential to be large have used the GMP arbitrary precision integer type **mpz_class**, and all local densities and Eisenstein coefficients are computed exactly with the corresponding rational number type **mpq_class**. The cuspidal constants C_f were computed exactly over $\mathbb{Q}$ in MAGMA until the very last step, where the complex embeddings were found. Although the accuracy of the embedding appears to be valid to at least 150 decimal places, Bhargava used instead the more permissive bound $C_f + 1$ to ensure accuracy. When the degree of the coefficient fields K_j are > 100, it is time-consuming to solve for the exact coefficients in K_j. Bhargava used the approximate cuspidal constants provided by William Stein with an accuracy of 3 decimal places.

6.5.4 The largest example

We present here the specific computation done by Bhargava for the locally universal form (Form ♯6414 in [2]) $Q(\vec{x}) = x^2 + 2y^2 + 4z^2 + 31w^2 + yz - yw + 3zw$. This has the largest overall bound $\frac{C_f}{C_E} < 8100.65$. By direct computation, we see that this form has $36,795,947$ eligible primes and its squarefree eiligible numbers m can have at most 14 prime factors. It is clear that $Q' = x^2 \oplus T$ where $T = 2y^2 + 4z^2 + 31w^2 + yz - yw + 3zw$ is a minimal split local cover. We estimate the largest eligible m to be $< 8.17 \times 10^{16}$ by solving for m in (7). Then, we compute an approximate Boolean theta function of T to precision 5.14×10^9 by performing LLL-reduction on T, which in this case leaves T unchanged, and finding the lengths of all vectors $\vec{v} = (y, z, w)$ in the rectangular cylinder $0 \leq y, z \leq 800$ and $w \geq 0$ inside the ellipsoid $T(\vec{v}) < 5.14 \times 10^9$.

We generate the 28 billion eligible squarefree numbers m and check that some $m - x^2$ is represented by T, which verified that there are no square-free exceptions. Therefore, Q represents all non-negative integers.

6.5.5 The Kneser form

Another example we consider is the Kneser form $Q(\vec{x}) = x^2 + 3y^2 + 5z^2 + 7w^2$ for which the computations are due to Hanke [5]. This form has level $N = 420$ and $\chi = (\frac{105}{\cdot})$. By direct computation, we obtain the bound $\frac{C_f}{C_E} < 177.03$. We find that this form has 11,765 eligible primes, which leads to $4,265,930$ square-free numbers to check. The largest of these is $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots 31 \approx 2 \times 10^{11}$. The split local cover is $Q' = 5x^2 \oplus T$ where $T = y^2 + 3z^2 + 7w^2$. By computing the first 10^7 coefficients of the ternary theta function, we find that the Kneser form represents all positive integers except 2 and 22.

6.6 Types of escalator lattices

From the arithmetic, analytic, and computational methods, we can determine precisely which integers are represented by each of the basic four-dimensional escalators. It follows that these 6560 escalator lattices L can be divided into three types:

- Type I: L is universal.

- Type II: L is not universal but does not represent at most three positive integers, each of which appears on the critical integers list.

- Type III: L is not locally universal, but is regular, and represents all integers not of the form $4^a(16k+14)$.

Of the 6560 basic four-dimensional escalators, 6402 of them are of Type I, 153 are of Type II, and 5 are of Type III.

6.7 Higher dimensional escalators

6.7.1 Higher escalator

We call any escalator resulting from a sequence of escalations of some basic four-dimensional escalator a **higher escalator**. We note that any basic escalator of Type II will become universal in at most three escalations steps. Therefore, we need to consider only the higher escalators from the basic quaternary escalators of Type III, whose Gram matrices are:

$$\begin{pmatrix} 1 & 0 & 1/2 & -3 \\ 0 & 2 & 1 & 0 \\ -1/2 & 1 & 5 & 1 \\ -3 & 0 & 1 & 10 \end{pmatrix}, \begin{pmatrix} 1 & 0 & -1/2 & -2 \\ 0 & 2 & 1 & -2 \\ -1/2 & 1 & 5 & 3 \\ -2 & -2 & 3 & 10 \end{pmatrix}, \begin{pmatrix} 1 & 0 & -1/2 & -2 \\ 0 & 2 & 1 & -2 \\ -1/2 & 1 & 5 & 1 \\ -2 & -2 & 1 & 10 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 & -1/2 & -1 \\ 0 & 2 & 1 & 0 \\ -1/2 & 1 & 5 & 3 \\ -1 & 0 & 3 & 10 \end{pmatrix}, \begin{pmatrix} 1 & 0 & -1/2 & -1 \\ 0 & 2 & 1 & 0 \\ -1/2 & 1 & 5 & 1 \\ -1 & 0 & 2 & 10 \end{pmatrix}.$$

Each of these forms has truant 14, and arises as an escalation of the three dimensional escalator L_3 given by $\begin{pmatrix} 1 & 0 & 1/2 \\ 0 & 2 & 1 \\ 1/2 & 1 & 5 \end{pmatrix}$ which has truant 10.

The escalations of these five basic escalators lead to 14221 higher escalators, each of which has dimension four or five. Each of these escalators are obtained by escalating L_3 first by a vector of norm 10 and then by a vector of norm 14. These two operations commute clearly, and we consider switching the order of the operations ("10-14 switch"). The lattices generated by L_3 and a vector of norm 14 are 330 quaternary forms in total, which we call the **auxiliary quaternaries**. Any of the 14221 higher escalators mentioned above must contain one of these 330 auxiliary quaternaries.

It turns out that 226 of the 330 auxiliary quaternary forms already occurred among the 6555 basic four-dimensional escalators of Type I or II. For the remaining 104 auxiliary quaternaries, we apply the analytic method discussed in Section 6.4 and find that each of the 104 forms L is either of Type I, Type II, or of

- Type IV: L represents all integers except perhaps for those of the form $10n^2$ and $13n^2$.

6.7.2 Summary

It can be concluded that it is not possible to escalate the zero lattice more than seven times.

Proposition 6.3. *The zero lattice can be escalated at most seven times, and therefore there is no escalator of dimension greater than seven.*

Since any lattice will have at most finitely many escalations by Cauchy-Schwartz inequality, there are only finitely many escalator lattices. Investigating the list of possible integers not represented by the basic quaternary escalators and by the auxiliary quaternaries shows that any escalator has a truant contained in the set of 29 critical integers. Therefore, we have the following proposition:

Proposition 6.4. *There are only finitely many escalator lattices, each of which is either universal, or has truant which is contained in the list of* 29 *critical integers.*

6.8 The Proof of the 290-Theorem

Proof of Theorem 2.6. We first claim that
(i) Any universal lattice L must contain a universal escalator,
(ii) The truant of a nonuniversal lattice L must be the truant of some nonuniversal escalator.

If L is universal, then we can construct within L a sequence of escalation $\{0\} \subset L_1 \subset L_2 \subset \cdots$. In at most seven steps, we get a universal escalator by Proposition 6.3. This proves (i). Similarly, given a nonuniversal lattice L, by constructing a maximal escalation sequence $\{0\} \subset L_1 \subset L_2 \subset \cdots \subset L_k$ $(k \leq 7)$ within L, we see that truant$(L) =$ truant(L_k). This proves (ii).

Now the theorem follows by Proposition 6.4.

Proof of Theorem 2.7. We first show that for every critical integer t, there exists an escalator lattice L such that truant$(L) = t$. The truant 1 occurs for the zero lattice, the truant 2 for the one-dimensional escalator, and each of the truant 3 and 5 arises in one of the three two-dimensional escalators. The truants that occur for the 34 three-dimensional escalators are $5, 6, 7, 10, 13, 14, 17, 21, 22, 23, 29, 31$, and the truants that arise for the basic four-dimensional escalators are $10, 13, 14, 15, 19, 21, 23, 26, 30, 34, 35, 37, 42, 58, 93, 110$, and 145.

The five-dimensional escalator lattice

$$\begin{pmatrix} 1 & 0 & -1/2 \\ 0 & 2 & -1/2 \\ -1/2 & -1/2 & 4 \end{pmatrix} \oplus (29) \oplus (145)$$

has truant 290. Let

$$L_{145} := \begin{pmatrix} 1 & 0 & -1/2 \\ 0 & 2 & -1/2 \\ -1/2 & -1/2 & 4 \end{pmatrix} \oplus (29)$$

The only square multiples of 58 less than 209 are 0 and 58, and L_{145} represents neither 203 nor 145. Therefore, $L_{203} := L_{145} \oplus (58)$ does not represent 203. Since L_{145} has truant 145,

L_{203} represents $\{0, \ldots, 144\} \cup \{0+58, \ldots, 144+58\} = \{0, \ldots, 202\}$. Thus, L_{203} has truant 203.

L_{203} contains a vector $\vec{v}$ of norm 145. Thus, the lattice L'_{203} generated by L_{145} and $\vec{v}$ in L_{203} is an escalator with truant 203. Thus, every critical integer t occurs as the truant of some escalator.

Now, given any critical integer t, let L be an escalator with truant t. Consider the lattice $L' := L \oplus (t+1)^{\oplus 4} \oplus (2t+1)$. L' does not represent t clearly, and by universality of the form $x^2+y^2+z^2+w^2$, it represents all multiples of $(t+1)$. Since $t+(t+1) = 2t+1$, all numbers greater than t is represented by L' by the division algorithm (dividing by $t+1$). Thus, L' represents all positive integers except for t, which proves the theorem.

Proof of Theorem 2.8. Any escalator lattice L having truant 290 must arise by a sequence of escalations of the escalator L_{145}, which fails to represent only the three integers $145, 203$, and 290. Any such L having truant 290 represents every positive integer greater than 290, and the theorem is proved.

Proof of Theorem 2.9. From the discussion in the proof of Theorem 2.7, we note that a universal quaternary form must have successive minima that are smaller than $1, 2, 5$, and 31 respectively. Applying the 290-Theorem to all Minkowski-reduced quaternary quadratic forms having such successive minima, we get the desired result.

7 Conclusion

The 15-Theorem and 290-Theorem give the complete answer for the universal quadratic form problem. For any given quadratic form, we can apply either the 15-theorem or the 290-theorem (depending on whether the form has integer-matrix or it is integer-valued) to determine whether it is universal. The two theorems further give the complete list of universal quaternary forms, which concludes the study of the universal quadratic forms.

8 Acknowledgements

I would like to express sincere thanks to my thesis advisor, Professor Kannan Soundararajan, for introducing me to this exciting topic of universal quadratic forms. I am truly grateful for his guidance and constant support on writing this paper.

References

[1] M. Bhargava, On the Conway-Schneeberger Fifteen Theorem. *Quadratic forms and their applications* (*Dublin, 1999*), 27-37, Contemp. Math., **272**, Amer. Math. Soc., Providence, RI, 2000.

[2] M. Bhargava and J. Hanke, *Universal quadratic forms and the 290-Theorem.* Invent. Math., 2005.

[3] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, London, 1978.

[4] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1993.

[5] J. Hanke, Local densities and explicit bounds for representability by a quadratic form. *Duke Math. J.* **124** (2004), no. 2, 351-388.

[6] G. Shimura, *On modular forms of half-integral weight.* Ann. of Math. (2) **97** (1973), 440-481.

[7] T. Vepkhvadze, *Modular properties of theta-functions and representation of numbers by positive quadratic forms.* Georgian Mathematical Journal, Vol. 4 (1997), no. 4, 385-400.

[8] M. Bhargava and J. Hanke, http://www.math.duke.edu/∼jonhanke/290/Universal-290.html. Website.