Adv. appl. Clifford alg. 18 (2008), 665–676

0188-7009/030665-12, *published online* May 27, 2008
DOI 10.1007/s00006-008-0090-y

Advances in Applied Clifford Algebras

Quadratic Forms over $\mathbb{Z}$ from Diophantus to the 290 Theorem

Alexander J. Hahn

Abstract. What follows[1] is a brief historical survey of the representation theory of quadratic forms over the integers. It starts with questions considered by Diophantus about 1800 years ago, dashes past classical contributions of Euler, Lagrange, and Sylvester, considers work of Ramanujan and Dickson, continues with theorems of Conway and Schneeberger, and ends with a short sketch of the proof of the 290-Theorem by Bhargava and Hanke. This survey is self-contained in the sense that all the basic definitions and concepts are provided.

Mathematics Subject Classification (2000). 11R04, 11E88.

Keywords. Rings, integers, quadratic forms, representation, Clifford algebras.

1. Classic Quadratic Forms

Let R be a commutative ring with 1. A *quadratic form* in n variables over R is a homogeneous polynomial

$$q = q(X_1, \ldots, X_n) = \sum_{1 \le i \le j \le n} a_{i,j} X_i X_j$$

of degree two with coefficients $a_{i,j}$ in R. An element $s \in R$ is a *value* of q if there is a vector $(r_1, \ldots, r_n) \in R^n$ such that $q(r_1, \ldots, r_n) = s$. In this case q is said to *represent* s. If q represents 0 non-trivially then q is *isotropic*, and q is *anisotropic* if 0 is represented only by the zero vector.

The Babylonians in the 18th century B.C. already knew about triples (a, b, c) of positive integers that satisfy the equation $a^2 + b^2 = c^2$. So they had insight into the ways that the quadratic form $X_1^2 + X_2^2 - X_3^2$ over the integers $\mathbb{Z}$ represents 0. In the 6th century B.C., the Pythagoreans appear to have been unsettled by the fact that the quadratic form $2X_1^2 - X_2^2$ over $\mathbb{Z}$ is anisotropic. However, the story of quadratic forms, in any reasonably systematic sense, begins with Diophantus and his *Arithmetica* [11] in the 3rd century A.D. For example, wanting to find two squares of rational numbers having a given difference, Diophantus saw that $60 = (x+3)^2 - x^2$ with $x = 8\frac{1}{2}$. In particular, the quadratic form $X_1^2 - X_2^2$ over

[1]This article is dedicated to a wonderful and exceptional mathematician, human being, and friend: to Timothy O'Meara on the occasion of his 80-th birthday.

$\mathbb{Q}$ represents 60. Of course, nowadays, we would simply observe that if R is a field of characteristic not 2, then $r = (\frac{r+1}{2})^2 - (\frac{r-1}{2})^2$ for any r in R. So $X_1^2 - X_2^2$ over R represents everything. Over $\mathbb{Z}$, $X_1^2 - X_2^2$ represents any odd integer because $2n+1 = (n+1)^2 - n^2$. Also, $2(2n) = (n+1)^2 - (n-1)^2$. On the other hand, $X_1^2 - X_2^2$ over $\mathbb{Z}$ does not represent any integer of the form $2k$ with k odd, because $n^2 - m^2 = (n-m)(n+m) = 2k$ with k odd is impossible. In particular, 2 is not represented by $X_1^2 - X_2^2$. Diophantus also considered the quadratic form $2X_1^2 - X_2^2$ over $\mathbb{Z}$ and proved that it represents 1 in infinitely many ways. He started with a representation $2x_1^2 - x_2^2 = 1$, set $2(c+x_1)^2 - (2c-x_2)^2 = 1$ with $c \neq 0$, and found that $c = 2(x_1 + x_2)$. Taking $x_1 = x_2 = 1$, he got $c = 4$ and the representation $2 \cdot 5^2 - 7^2 = 1$. Repeating this with $x_1 = 5$ and $x_2 = 7$, he got $2 \cdot 29^2 - 41^2 = 1$, and with $x_1 = 29$ and $x_2 = 41$, he got $2 \cdot 169^2 - 239^2 = 1$, and so on.

Toulouse's famous son Pierre de Fermat knew, and Leonhard Euler (1760) proved, that the form $X_1^2 + X_2^2$ over $\mathbb{Z}$ represents all primes of the form $4n+1$ in exactly one way. Fermat also knew, and Luigi Lagrange (1775) proved, that $X_1^2 + 2X_2^2$ over $\mathbb{Z}$ represents all primes of the form $8n+1$ and $8n+3$ in exactly one way. Euler (1761) proved that the form $X_1^2 + 3X_2^2$ over $\mathbb{Z}$ represents all primes of the form $3n+1$ in exactly one way. Adrien-Marie Legendre (1798) informed us that the form $X_1^2 + X_2^2 + X_3^2$ over $\mathbb{Z}$ represents all positive integers except those that are the product of a power of 4 and a number congruent to -1 modulo 8. The most famous of these assertion is Lagrange's Theorem (1770) telling us that the form $X_1^2 + X_2^2 + X_3^2 + X_4^2$ over $\mathbb{Z}$ represents all positive integers. Evidence in the *Arithmetica* suggests that Diophantus had discovered the theorems of Legendre and Lagrange empirically.

These and more representation results about quadratic forms over $\mathbb{Z}$ are discussed in the *Disquisitiones Arithmeticae* [7] of Carl Friedrich Gauss. It is with this famous treatise of 1801 that the modern theory of quadratic forms begins.

There are connections between quadratic forms and some famous unsolved problems. A very elusive question was communicated by Christian Goldbach to Euler in 1742. Could it be that for each positive integer $k \geq 2$, there are two odd primes p and p' such that $2k = p + p'$? Surprisingly, see [8], this conjecture can be recast into a representation question about the quadratic form $X_1^2 - X_2^2$ over $\mathbb{Z}$. If the conjecture is true, then for a given positive integer k, there are primes $p \leq p'$ and an integer m satisfying $0 \leq m \leq k-2$, such that $p = k-m$ and $p' = k+m$. But then $k^2 - m^2 = pp'$. Conversely, if for each $k \geq 2$, there is an m with $0 \leq m \leq k-2$ such that $k^2 - m^2 = pp'$, with p and p' primes and $p \leq p'$, then we must have $p = k-m$, $p' = k+m$, and hence $2k = p + p'$. Thus Goldbach's conjecture is equivalent to the following assertion about the quadratic form $X_1^2 - X_2^2$. For every integer $k \geq 2$, there exist an integer m with $0 \leq m \leq k-2$ and primes p and p', such that $k^2 - m^2 = pp'$.

Suppose that in the statement above, $m = 1$ works infinitely often. That is, suppose that there are infinitely many k such that $k^2 - 1 = pp'$ for some primes $p \leq p'$. Then $p = k-1$ and $p' = k+1$ are primes for infinitely many k. This is the

Twin Prime Conjecture. So both the Goldbach and Twin Prime conjectures can be formulated in terms of properties of the quadratic form $X_1^2 - X_2^2$ over $\mathbb{Z}$.

Being able to factor large numbers is important in the encryption of messages. Fermat had a strategy for factoring a composite odd number $n = uv$ that goes like this. Because this equality is equivalent to $n = (\frac{u+v}{2})^2 - (\frac{u-v}{2})^2$, the idea is to take $x > \sqrt{n}$ and look for y such that $n = x^2 - y^2$, and then to solve for u and v. But this is another representation question about the form $X_1^2 - X_2^2$.

Let's return to a general quadratic form

$$q = q(X_1, \ldots, X_n) = \sum_{1 \le i \le j \le n} a_{i,j} X_i X_j$$

over a commutative ring R. If all the coefficients $a_{i,j}$ with $i < j$ are in the ideal 2R, then the form q is a *classic* quadratic form. Let q be such a form. For any $a_{i,j}$ with $i < j$, let $a_{i,j} = 2t_{i,j}$ for some $t_{i,j} \in R$. Now set $b_{i,j} = b_{j,i} = t_{i,j}$, and set $b_{i,i} = a_{i,i}$. Note that $b_{i,j} + b_{j,i} = a_{i,j}$ for any $i < j$. Let B be the $n \times n$ symmetric matrix $B = [b_{i,j}]$. Then

$$(X_1, \cdots, X_n) \begin{bmatrix} b_{1,1} & \cdots & b_{1,n} \\ \vdots & & \vdots \\ b_{n,1} & \cdots & b_{n,n} \end{bmatrix} \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = \sum_{1 \le i,j \le n} X_i b_{i,j} X_j$$

$$= \sum_n b_{i,i} X_i^2 + \sum_{1 \le i \ne j \le n} b_{i,j} X_i X_j = \sum_n a_{i,i} X_i^2 + \sum_{1 \le i < j \le n} a_{i,j} X_i X_j$$

$$= \sum_{1 \le i \le j \le n} a_{i,j} X_i X_j = q(X_1, \ldots, X_n).$$

So a classic quadratic form is given by multiplication by a symmetric matrix (and conversely). Classic quadratic forms over $\mathbb{Z}$ are also called *matrix-integral* forms or forms *having integer matrix* in the literature. See [5] or [1] for example. About 2/3 of the almost 500 pages of the *Disquisitiones Arithmeticae* [7] is devoted to the development of the theory of classic binary quadratic forms $aX_1^2 + 2bX_1X_2 + cX_2^2$.

Two quadratic forms

$$\sum_{1 \le i \le j \le n} a_{i,j} X_i X_j \quad \text{and} \quad \sum_{1 \le i \le j \le n} c_{i,j} Y_i Y_j$$

over R are *equivalent*, if there is a linear substitution of variables $X_i = \sum_j d_{i,j} Y_j$, $i = 1, \ldots, n$, with $[d_{i,j}]$ an invertible $n \times n$ matrix over R, that transforms the first form into the second. If this is so, then by using the inverse of $[d_{i,j}]$, the second form can also be transformed into the first. The forms $X_1^2 + X_2^2$ and $29Y_1^2 + 24Y_1Y_2 + 5Y_2^2$ "look" totally different. However they are equivalent, because the transformation $X_1 \to 5Y_1 + 2Y_2$ and $X_2 \to 2Y_1 + Y_2$ takes the first form to the second (and is invertible).

2. Quadratic Modules

We now turn to a more general *geometric* concept of quadratic form. As before, R is any commutative ring. The group of invertible elements of R is denoted R^*. Let M be a free R-module with basis $\{x_1, \ldots, x_n\}$. Let

$$q(X_1, \ldots, X_n) = \sum_{1 \le i \le j \le n} a_{i,j} X_i X_j$$

be a quadratic form in n variables over R and define $q : M \to R$ by setting

$$q(r_1 x_1 + \cdots + r_n x_n) \;=\; q(r_1, \ldots, r_n) \;=\; \sum_{1 \le i \le j \le n} a_{i,j} r_i r_j \,.$$

Now let M be any R-module. With a focus on the properties of the above construction, define a *quadratic form* on M to be a map

$$q : M \to R$$

such that $q(rx) = r^2 q(x)$ for all $r \in R$ and $x \in M$, and

$$(\ ,\ )_q : M \times M \to R$$

defined by $(x, y)_q = q(x+y) - q(x) - q(y)$ is bilinear. Because $(\ ,\ )_q$ is also symmetric, this is the *symmetric bilinear form associated to* q. The composite $M = (M, q)$ is a *quadratic* R-module. Earlier terminology carries over. For example, a quadratic module is *isotropic* if $q(x) = 0$ for some non-zero $x \in M$, and q represents $s \in R$ if $q(x) = s$ for some $x \in M$.

There is an immediate connection between the definitions of quadratic module and Clifford algebra. Let M be any R-module. Let's suppose that we wish to place M into an R-algebra A with identity 1_A, such that for all x and y in M both x^2 and $xy + yx$ are scalars in A. In other words, we'd like to construct an algebra A with 1_A that contains M in such a way that

$$x^2 \in R1_A \quad \text{and} \quad xy + yx \in R1_A$$

for all x and y in M. Suppose that we have such an algebra. For x and y in M, put $x^2 = c_x 1$ and $xy + yx = d_{x,y} 1$ with c_x and $d_{x,y}$ in R. From $(rx)^2 = c_{rx} 1$ we get $c_{rx} = r^2 c_x$, and from $(x + y)^2 = c_{x+y} 1$ we get that $d_{x,y} = c_{x+y} - c_x - c_y$. It is now a routine matter to check that $q(x) = c_x$ defines a quadratic form on M with associated bilinear form given by $(x, y)_q = d_{x,y}$. So if such an algebra A is to exist, the scalars involved in the products x^2 and $xy + yx$ need to be organized by a quadratic form on M. And if the scalars are so organized, can such an algebra A be constructed? In a uniquely "minimal" way? These questions (and their positive answers) begin the algebraic theory of Clifford algebras.

Let $M = (M, q)$ be a quadratic R-module. Let M^* be the dual module of M. Consider the linear map $M \to M^*$ defined by

$$x \to \{y \to (x, y)_q, \text{ for all } y \in M\}.$$

If this map is an isomorphism, then q is *non-singular*. Suppose that M is free of rank n and let $\{x_1, \ldots, x_n\}$ be a basis of M. It is easy to check that

$$(r_1x_1 + \cdots + r_nx_n\,, s_1x_1 + \cdots + s_nx_n)_q = \sum_{1\le i,j\le n} r_i(x_i, x_j)_q s_j$$

$$= (r_1 \cdots r_n) \begin{bmatrix} (x_1,x_1)_q & \cdots & (x_1,x_n)_q \\ \vdots & & \vdots \\ (x_n,x_1)_q & \cdots & (x_n,x_n)_q \end{bmatrix} \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}.$$

The matrix $[(x_i, x_j)_q]$ is *the matrix of* $(\ ,\ )_q$ *in the basis* $\{x_1, \ldots, x_n\}$. Note that $[(x_i, x_j)_q]$ is a symmetric matrix. By basic linear algebra,

$$q \text{ is non-singular} \iff [(x_i, x_j)_q] \text{ is invertible} \iff \det [(x_i, x_j)_q] \in R^*.$$

Let M be a free R-module with basis $\{x_1, x_2\}$. Using X_1X_2 and the earlier construction, we get the quadratic form $q(r_1x_1+r_2x_2) = r_1r_2$ on M. The associated bilinear form is

$$(r_1x_1 + r_2x_2, s_1x_1 + s_2x_2)_q = (r_1 + s_1)(r_2 + s_2) - r_1r_2 - s_1s_2 = r_1s_2 + r_2s_1.$$

The matrix of $(\ ,\ )_q$ is $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, so that q is non-singular.

The translation of the notion of equivalence into the geometric context is this: two quadratic modules (M, q) and (M', q') over R are *equivalent* or *isometric* if there is an invertible linear map $\varphi : M \to M'$ such that $q'(\varphi x) = q(x)$ for all x in M. If this is so, we will write $M \cong M'$. The notation

$$M \cong \sum_{1\le i\le j\le n} a_{i,j}X_iX_j$$

means that the quadratic module M is isometric to the free quadratic module constructed from the quadratic form $\sum_{1\le i\le j\le n} a_{i,j}X_iX_j$ in the way described earlier.

Let S be a commutative ring containing R. More precisely, let S be a commutative R-algebra. A quadratic form

$$q(X_1, \ldots, X_n) = \sum_{1\le i\le j\le n} a_{i,j}X_iX_j$$

over R is clearly also a quadratic form over S. In terms of quadratic modules, this "change of scalars" is captured by going from M to the tensor product $M \otimes_R S$ and by extending q to $M \otimes_R S$ by $q(x \otimes s) = s^2q(x)$.

We turn to some very basic facts about quadratic forms over fields of characteristic not 2 beginning with the "diagonalization theorem." See O'Meara [18] for a comprehensive account of all these matters.

Theorem. *Let F be a field of characteristic not 2. Let M be a finite dimensional quadratic module over F with* $\dim M = n$. *Then*

$$M \cong a_1X_1^2 + a_2X_2^2 + \cdots + a_nX_n^2$$

with all a_i in F. Given such an isometry, M is non-singular if and only if all a_i are non-zero.

Corollary. *Let M be a finite dimensional non-singular quadratic module over the complex numbers $\mathbb{C}$ with* $\dim M = n$. *Then*

$$M \cong X_1^2 + X_2^2 + \cdots + X_n^2.$$

Theorem (Sylvester). *Let M be a finite dimensional non-singular quadratic module over the real numbers $\mathbb{R}$. Then*

$$M \cong X_1^2 + \cdots + X_k^2 - X_{k+1}^2 - \cdots - X_{k+m}^2,$$

where $k + m = \dim M$, and k and m are uniquely determined by M.

If only pluses arise in the conclusion of this theorem, the quadratic module (M, q) over $\mathbb{R}$ is called *positive*. If only minuses arise, then (M, q) is *negative*. Both of these cases are anisotropic. Note that in all other situations, (M, q) is isotropic. In a given dimension n, how many isometry classes of non-singular quadratic modules over $\mathbb{R}$ are there? And over $\mathbb{C}$?

3. Classic and Unimodular Quadratic Modules

Let's start with an example. Let M be a free R-module with basis $\{x_1, x_2\}$ and use $X_1^2 - X_2^2$ to define the quadratic form $q(r_1x_1 + r_2x_2) = r_1^2 - r_2^2$ on M. The associated bilinear form $(\ ,\ )_q$ satisfies

$$(r_1x_1 + r_2x_2, s_1x_1 + s_2x_2)_q = 2r_1s_1 - 2r_2s_2.$$

The matrix of $(\ ,\ )_q$ is $\begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix}$. So (M, q) is non-singular $\iff$ $2 \in R^*$. In particular, (M, q) is *not* non-singular over $\mathbb{Z}$. Similarly, none of the forms $X_1^2 + X_2^2, X_1^2 + X_2^2 + X_3^2, X_1^2 + X_2^2 - X_3^2$, and $X_1^2 + X_2^2 + X_3^2 + X_4^2$ over $\mathbb{Z}$ mentioned in Section 1 defines a non-singular quadratic module.

This is an unhappy situation: the most basic examples of quadratic forms over $\mathbb{Z}$, indeed over any commutative ring R in which 2 is not a unit, fall outside the fundamental concept of non-singularity. A return to classic forms provides a resolution of this difficulty.

Let M be an R-module over a commutative R and let $b : M \times M \to R$ be bilinear and symmetric. Define $q : M \to R$ by $q(x) = b(x, x)$ for all x. It is easy to see that q is a quadratic form on M and that the associated bilinear form $(\ ,\ )_q = 2b$. In this case we will say that (M, q) is a *classic* quadratic R-module (defined by the form b). If (M, q) is classic, then clearly $(x, y)_q \in 2R$ for

all x and y in M. If M is a free quadratic R-module defined by a quadratic form $q = \sum_{1 \le i \le j \le n} a_{i,j} X_i X_j$, then by a construction in Section 1,

$$M \text{ is classic} \iff q \text{ is classic} \iff a_{i,j} \in 2R \text{ for all } i < j.$$

Suppose that (M, q) is a classic quadratic module defined by the symmetric bilinear form $b : M \times M \to R$. If

$$x \to \{y \to b(x, y), \text{ for all } y \in M\}$$

defines an isomorphism $M \to M^*$, then q is *unimodular*. It follows from the fact that $(\ ,\ )_q = 2b$, that a classic q is non-singular if and only if $2 \in R^*$ and q is unimodular.

Consider an R-module M with basis $\{x_1, x_2\}$. Recall that the quadratic polynomial $X_1^2 - X_2^2$ defines a quadratic form q on M by $q(r_1x_1 + r_2x_2) = r_1^2 - r_2^2$. Define the bilinear from $b : M \times M \to R$ by

$$b(r_1x_1 + r_2x_2, s_1x_1 + s_2x_2) = r_1s_1 - r_2s_2\,.$$

Because $b(x, x) = q(x)$ for all $x \in M$, q is classic. The fact that

$$\begin{bmatrix} b(x_1, x_1) & b(x_1, x_2) \\ b(x_2, x_1) & b(x_2, x_2) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

is invertible, tells us that q is unimodular. Turn next to the symmetric bilinear form $b : M \times M \to R$ with

$$b(r_1x_1 + r_2x_2, s_1x_1 + s_2x_2) = r_1s_2 + r_2s_1,$$

already considered in Section 2. The matrix of b in the base $\{x_1, x_2\}$ is the invertible matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Because the quadratic form defined by b satisfies $q(r_1x_1 + r_2x_2) = 2r_1r_2$, it follows that the quadratic module (M, q) defined by $2X_1X_2$ is unimodular. This (M, q) is a *hyperbolic plane*.

By using the strategy of the earlier example, it is easy to see that the forms $X_1^2 + X_2^2$, $X_1^2 + X_2^2 + X_3^2, X_1^2 + X_2^2 - X_3^2$, and $X_1^2 + X_2^2 + X_3^2 + X_4^2$, all define unimodular quadratic modules. But what about $2X_1^2 - X_2^2$ and $X_1^2 + 3X_2^2$?

4. Representation by Quadratic Forms over $\mathbb{Z}$

Everything discussed so far has been elementary. While the statements of the theorems in this last section continue to be elementary, this is no longer the case for their proofs. For the classical results and their proofs that follow next, refer to Serre [20], especially Chapter V.

Let (M, q) be a quadratic $\mathbb{Z}$-module and consider the quadratic $\mathbb{R}$-module $M \otimes_{\mathbb{Z}} \mathbb{R}$. Suppose that $M \otimes_{\mathbb{Z}} \mathbb{R}$ is finite dimensional and non-singular. Refer to the remarks that follow Sylvester's Theorem and call M *positive definite, negative definite,* or *indefinite*, according as $M \otimes_{\mathbb{Z}} \mathbb{R}$ is positive, negative, or isotropic. For a unimodular quadratic $\mathbb{Z}$-module (M, q), it is straightforwardly true that the $\mathbb{Z}$-module generated by $\{q(x) \mid x \in M\}$ is either $2\mathbb{Z}$ or $\mathbb{Z}$. In the first case, all $q(x)$

are even, so that (M, q) is called *even*. In the second case, there exist x in M with $q(x)$ odd, and (M, q) is called *odd*.

It follows from the discussion in Section 3 that the quadratic forms $X_1^2 + X_2^2$, $-X_1^2 - X_2^2$, and $X_1^2 - X_2^2$ define positive definite, negative definite, and indefinite quadratic modules, respectively. Notice that they are all unimodular and odd. The form $2X_1X_2$ defines an even indefinite unimodular quadratic module (the hyperbolic plane). An example of an even positive definite unimodular quadratic module over $\mathbb{Z}$ is more difficult to come by. It turns out that of all such quadratic modules, the one defined by the quadratic form

$$\begin{aligned} Q(X_1, \ldots, X_8) = \\ 2X_1^2 - 2X_1X_3 + 2X_2^2 - 2X_2X_4 + 2X_3^2 - 2X_3X_4 + 2X_4^2 - 2X_4X_5 \\ +2X_5^2 - 2X_5X_6 + 2X_6^2 - 2X_6X_7 + 2X_7^2 - 2X_7X_8 + 2X_8^2 \end{aligned}$$

(associated to the root lattice E_8) has the smallest rank (of 8).

The definite/indefinite distinction is fundamental in the theory of unimodular quadratic modules over $\mathbb{Z}$. In the definite case, it is known that for a given rank there are only finitely many isometry classes of such modules. There are also restrictions on the rank. For instance, the rank of an even definite unimodular quadratic module is known to be divisible by 8. In ranks 8, 16, and 24 all such quadratic modules have been described up to isometry, with the number of isometry classes respectively given by 1 (the class of $Q(X_1, \ldots, X_8)$), 2, and 24. Beyond that things begin to explode. For instance, there are over 80 million isometry classes of even definite unimodular quadratic modules of rank 32. The particularity of the examples that have been constructed leaves little doubt that a complete classification of definite unimodular quadratic modules is impossible. For indefinite unimodular quadratic modules on the other hand, there is a complete structure/classification theory. It tells us, in particular, that all such quadratic modules are sums of examples that we have already considered.

Theorem. [2] *Let (M, q) be an indefinite unimodular quadratic module over $\mathbb{Z}$ of rank n. If (M, q) is odd, then*

$$M \cong a_1X_1^2 + a_2X_2^2 + \cdots + a_nX_n^2,$$

with all $a_i = \pm 1$ (but not all $a_i = 1$ nor all $a_i = -1$).

It follows that there are exactly $n - 1$ isometry classes of odd indefinite unimodular quadratic $\mathbb{Z}$-modules for a given rank n. There is a classification theory in the even case as well. Denote by $Q_{j,i}$ the quadratic form obtained from $Q(X_1, \ldots, X_8)$ by replacing the indeterminates $X_1, \ldots, X_8$ by $X_{2j+8i-7}$, $X_{2j+8i-6}, \ldots, X_{2j+8i}$ respectively.

[2] This theorem is incorrectly stated in Hahn [10]. See Theorem 9 in Section 6. The quadratic module M needs to be unimodular not non-singular. It is also misstated in Exercise 2 of Section 6.3 of [16], as the assumption $b(M, M) = \mathbb{Z}$ is not sufficient.

Theorem. *Let (M, q) be an indefinite unimodular quadratic module over $\mathbb{Z}$ of rank n. If (M, q) is even, then either*

$$M \cong 2X_1X_2 + \cdots + 2X_{2j-1}X_{2j} + Q_{j,1} + \cdots + Q_{j,k}, \quad \text{or}$$

$$M \cong 2X_1X_2 + \cdots + 2X_{2j-1}X_{2j} - Q_{j,1} - \cdots - Q_{j,k},$$

where $j \geq 1$ and $2j + 8k = n$.

How many isometry classes of even indefinite unimodular quadratic forms are there? Set $n = 2l + 8m$ with $1 \leq l \leq 4$. It is a straightforward consequence of the theorem that there are $2m + 1$ isometry classes of such quadratic modules. Combining the theorems above with remarks about the quadratic form $X_1^2 - X_2^2$ over $\mathbb{Z}$ from Section 1, quickly provides the next two corollaries. The second corollary (in which (M, q) is automatically indefinite and odd) leads our discussion in the direction of the celebrated representation theorems for definite quadratic forms by Conway and Schneeberger as well as Bhargava and Hanke.

Corollary. *Let (M, q) be an indefinite unimodular quadratic module over $\mathbb{Z}$. If* rank $M \geq 2$ *and (M, q) is even, then q represents all even integers. If* rank $M \geq 3$ *and (M, q) is odd, then q represents all integers.*

Corollary. *Let (M, q) be a unimodular quadratic module over $\mathbb{Z}$. If q represents -1 and 2, then q represents all integers.*

The remainder of the discussion focuses on positive definite quadratic forms over $\mathbb{Z}$. The condition of unimodularity will no longer be required.

Let's begin with "diagonal" quaternary quadratic forms. These are the forms of type $aX_1^2 + bX_2^2 + cX_3^2 + dX_4^2$ over $\mathbb{Z}$. We denote such a form by $[a, b, c, d]$ for short. The current focus on positive definite forms means that a, b, c, and d are all positive. It follows from earlier considerations that any such form is classic and that it is unimodular only if $a = b = c = d = 1$. Ramanujan (1916) proved that precisely the following such forms (up to isometry) represent all positive integers:

$[1, 1, 1, d]$ with $1 \leq d \leq 7$, $[1, 1, 2, d]$ with $2 \leq d \leq 14$,
$[1, 1, 3, d]$ with $3 \leq d \leq 6$, $[1, 2, 2, d]$ with $2 \leq d \leq 7$,
$[1, 2, 3, d]$ with $3 \leq d \leq 10$, $[1, 2, 4, d]$ with $4 \leq d \leq 14$,
$[1, 2, 5, d]$ with $5 \leq d \leq 10$.

Dickson (1927) confirmed this, except to point out that $[1, 2, 5, 5]$ does not belong on the list (because it does not represent 15). The list of Ramanujan is an easy consequence of the theorem of Conway and Schneeberger:

Theorem. *Let (M, q) be a positive definite classic quadratic module over $\mathbb{Z}$. If q represents all the numbers in the set $\{1, 2, 3, 5, 6, 7, 10, 14, 15\}$, then q represents all positive integers.*

Notice that it is not assumed that (M, q) is unimodular. This "Fifteen Theorem" is "best possible" in the following sense: if t is any number in the set singled

out in the theorem, then there is a positive definite classic quadratic form (in fact a quaternary diagonal form) that fails to represent t but represents every other positive integer. The original proof of the theorem, see [5] for a flavor, was complicated and never written up. The article [1] provides a simplified proof within the framework of quadratic modules. Bhargava, see [2], has extended his ideas to prove the following generalization of the Fifteen Theorem:

Theorem. *Let S be any subset of the nonnegative integers. Then there is a unique smallest finite subset T of S such that a classic positive definite quadratic form represents S if and only if it represents T.*

For the following three cases Barghava has explicitly determined the finite set T that corresponds to the given S:

A. *If S is the set of natural numbers, then* $T = \{1, 2, 3, 5, 6, 7, 10, 14, 15\}$.

B. *If S is the set of odd natural numbers, then* $T = \{1, 3, 5, 7, 11, 15, 33\}$.

C. *If S is the set of primes, then* $T = \{\text{primes up to } 47\} \cup \{67, 73\}$.

The theorem below–until recently referred to as the 290-conjecture–and now proved by Bhargava and Hanke [3] removes the assumption classic from the hypothesis of the Fifteen Theorem.

The 290 Theorem (Bhargava and Hanke). *Let (M, q) be a positive definite quadratic module over $\mathbb{Z}$ (not necessarily classic). If q represents the set* $\{1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290\}$, *then q represents every positive integer.*

This theorem is also "best possible". The fact is that for each of the 29 numbers on the list, there is a quadratic form (satisfying the conditions of the theorem) that represents all positive integers with the exception of this one number.

The essential strategy of the proof of the 290-Theorem is as follows. If a positive definite quadratic module L does not represent all positive integers, let the *truant* of L be the smallest integer not represented by L. An *escalation* of such a quadratic module L is any quadratic module of the form $L \oplus \mathbb{Z}x$ where $q(x)$ is a truant of L. Now let (M, q) satisfy the conditions of the theorem. Let $L_1 = \mathbb{Z}x$ with $x \in M$ and $q(x) = 1$. The truant of L_1 is 2, and L_1 has three possible escalators L_2 (up to isometry) inside M. They correspond to the forms $X_1^2 + X_2^2, X_1^2 + 2X_2^2$, and $X_1^2 + X_1X_2 + 2X_2^2$. The truants of the three L_2 are 3, 5, and 3, respectively. Escalating each of them leads to exactly 34 possible three dimensional submodules L_3 of M (up to isometry). Escalating each of these in turn, provides 6560 possible four dimensional submodules (again up to isometry). Each of these is analyzed by arithmetic methods (genus, class number), analytic methods (Tartakowsky's Theorem, modular forms, Eisenstein series) and computational methods (Magma, C++) and it turns out that 6402 of them represent all positive integers. In these cases, the proof is done. The remaining 158 need to be escalated again. Continuing

this process for at most three more dimensions, provides a submodule of M that represents all positive integers.

References

[1] Manjul Bhargava, *On the Conway-Schneeberger fifteen theorem. Quadratic forms and their applications*. (Dublin, 1999), 27-37, Contemporary Mathematics. 272, Amer. Math. Soc., Providence, RI, 2000.

[2] Manjul Bhargava, *The Fifteen Theorem and Generalizations*. Preprint

[3] Manjul Bhargava and Jonathan Hanke, *Universal quadratic forms and the 290-Theorem*. Preprint

[4] J. W. Cassels, *Rational Quadratic Forms*. Academic Press, New York, 1978.

[5] John Conway, *The sensual quadratic form*. Carus Mathematical Monographs, Mathematical Association of America 1997.

[6] Martin Eichler, *Quadratische Formen und orthogonale Gruppen*. 2nd ed. Grundlehren der Mathematischen Wissenschaften 63, Springer-Verlag, Berlin, 1974.

[7] Carl Friedrich Gauss, *Disquisitiones Arithmetica*. New Haven and London, Yale University Press, 1966.

[8] L. J. Gerstein, *A reformulation of the Goldbach conjecture*. Mathematics Magazine vol. 66 (1993), 44-45.

[9] Alexander J. Hahn, *Quadratic Algebras, Clifford Algebras, and Arithmetic Witt Groups*. Springer-Verlag, New York, 1994.

[10] Alexander J. Hahn, *The Clifford Algebra in the Theory of Algebras, Quadratic Forms, and Classical Groups*. Chapter 19 in Clifford Algebras: Applications to Mathematics, Physics, and Engineering Birkhäuser, 2004.

[11] Thomas Heath, *Diophantus of Alexandria*. Dover Publications Inc. New York, 1964.

[12] H. J. S. Hsia, Y. Y. Shao and F. Xu, *Representations of indefinite quadratic forms*. J. Reine und Angew. Math. **494** (1998), 129-140.

[13] Don James, *Local Densities and the Representations of an Integer by a Definite Quadratic Form*. Contemporary Mathematics **344** Amer. Math. Soc. Providence, RI, (2004), 185-196.

[14] Burton Jones, *The Arithmetic Theory of Quadratic Forms*. Carus Mathematical Monographs, Mathematical Association of America, 1950.

[15] Myung-Hwan Kim, *Recent Developments on Universal Forms*. Contemporary Mathematics, **344** Amer. Math. Soc. Providence, RI, (2004), 215-228.

[16] Kitaoka, *Arithmetic of Quadratic Forms*. Cambridge University Press, 1993.

[17] John Milnor and Dale Husemoller, *Symmetric Bilinear Forms*. Springer-Verlag, 1973.

[18] O.Timothy O'Meara, *Introduction to Quadratic Forms*. Springer-Verlag, 1963. Reprinted in the Classics of Mathematics Series, Springer-Verlag, 2000.

[19] Rainer Schultze-Pillot, *Representations by integral quadratic forms – a survey*. Contemporary Mathematics 344, Amer. Math. Soc. Providence, RI, (2004), 303-321.

[20] Jean Pierre Serre, *A Course in Arithmetic*. Springer-Verlag, 1973.

Alexander J. Hahn
Department of Mathematics
University of Notre Dame
Notre Dame, IN 46556, USA
e-mail: hahn@nd.edu

Received: October 26, 2005.
Accepted: May 17, 2007.