ACTA ARITHMETICA
164.3 (2014)

Euclidean quadratic forms and ADC forms II: integral forms

by

PETE L. CLARK (Athens, GA) and WILLIAM C. JAGY (Berkeley, CA)

Contents

1. Introduction. In [Cl12], the first author introduced *Euclidean quadratic forms* and *ADC forms* and proved some results about them. This paper continues that study by looking more closely at the case of integral quadratic forms.

1.1. Background and prior work. For a ring R, we write $R^\bullet$ for $R \setminus \{0\}$. Let R be a domain with fraction field K. A *norm function* on R is a map $|\cdot| : R^\bullet \to \mathbb{Z}^+$ such that $|x| = 1 \Leftrightarrow x \in R^\times$ and $|xy| = |x|\,|y|$ for all $x, y \in R^\bullet$. We set $|0| = 0$. A domain R endowed with a norm function is called a *normed ring*. We shall assume that the characteristic of R is not 2.

We consider quadratic forms $q = q(x_1, \ldots, x_n)$ over R and always assume them to be *nondegenerate*: $\operatorname{disc} q \neq 0$. If $(R, |\cdot|)$ is a normed ring, such a form q is *Euclidean* if, for all $x \in K^n \setminus R^n$, there exists $y \in R^n$ such that $0 < |q(x-y)| < 1$. For the most part we will consider *anisotropic* forms—i.e., forms such that $q(x) = 0 \Rightarrow x = 0$—and for such forms the Euclidean condition simplifies to: for all $x \in K^n$, there exists $y \in R^n$ such that $|q(x-y)| < 1$.

Let q be an anisotropic quadratic form over the normed domain $(R, |\cdot|)$. For each $x \in K^n$, we define the *local Euclideanity*

$$E(q, x) = \inf_{y \in R^n} |q(x-y)|,$$

2010 *Mathematics Subject Classification*: Primary 11E08, 11E12, 13F05, 13F07.
Key words and phrases: normed ring, Euclidean form, covering radius, ADC form, regular form, positive form, Voronoi cell, Lorentzian lattice.

DOI: 10.4064/aa164-3-4

which depends only on the class of x in K^n/R^n. We also define the *Euclideanity*

$$E(q) = \sup_{x \in K^n/R^n} E(q,x).$$

Let

$$C(q) = \{x \in K^n/R^n \mid E(q,x) = E(q)\}.$$

Elements of $C(q)$ are called *critical points*. We say that the Euclideanity *is attained* if $C(q) \neq \emptyset$. Thus, $E(q)$ is Euclidean if and only if either $E(q) < 1$, or $E(q) = 1$ and the Euclideanity is *not* attained. The attainment of the Euclideanity is in general a difficult problem. For positive forms over $\mathbb{Z}$, that the Euclideanity is attained follows from the elementary geometry of Voronoi cells, as we will recall in §4. Already for indefinite binary integral quadratic forms it is conjectured but not yet proven that the Euclideanity is always attained.

Example 1.1. For any $a \in R^\bullet$, $E(aq) = |a|E(q)$. This reduces us to the calculation of Euclideanities of *primitive forms* in the sense of §2.1.

Example 1.2. Let $R = \mathbb{Z}$ be endowed with the standard (Euclidean) norm $|\cdot|$. Then for any quadratic forms q_1, q_2 over $\mathbb{Z}$ we have

$$E(q_1 \oplus q_2) \leq E(q_1) + E(q_2). \tag{1}$$

In fact (1) holds over any normed domain $(R, |\cdot|)$ satisfying $|x+y| \leq |x|+|y|$ for all $x, y \in R$. When $R = \mathbb{Z}$ and q_1 and q_2 are positive forms, we have

$$E(q_1) \oplus E(q_2) = E(q_1) + E(q_2). \tag{2}$$

This, together with Example 1.1 and the fact that $E(x^2) = 1/4$ over $\mathbb{Z}$, implies that for $a_1, \ldots, a_n \in \mathbb{Z}^+$,

$$E(a_1x_1^2 + \cdots + a_nx_n^2) = \frac{a_1 + \cdots + a_n}{4}.$$

A quadratic form over a (not necessarily normed) domain R is an *ADC form* if for all $d \in R$, whenever there exists $x \in K^n$ such that $q(x) = d$, then there exists $y \in R^n$ such that $q(y) = d$.

These notions of Euclidean form and ADC form are the subject of [Cl12]. The jumping-off point was the following result relating the two classes, a generalization of classical work of **A**ubry, **D**avenport and **C**assels.

Theorem 1.3 ([Cl12, Thm. 8]). *A Euclidean form is an ADC form.*

Much of [Cl12] concerns Euclidean and ADC forms over complete discrete valuation rings and Hasse domains. We recall the two main results and two conjectures from [Cl12] that we will address in the present work.

A *Hasse domain* R is either an S-integer ring in a number field or the coordinate ring of a regular, geometrically integral affine algebraic curve over a finite field. Such an R has a natural multiplicative norm: $x \in R^\bullet \mapsto \#R/(x)$. Let Σ_R denote the set of height one primes of R; for each $\mathfrak{p} \in \Sigma_R$, the completed local ring $R_\mathfrak{p}$ is a complete discrete valuation ring (CDVR). Each $R_\mathfrak{p}$ carries a canonical norm, again given by $x \in R_\mathfrak{p} \mapsto \#R_\mathfrak{p}/(x)$. Let K be the field of fractions of R (a global field). Let Σ_K be the set of places of K, and put $S = \Sigma_K \setminus \Sigma_R$.

Theorem 1.4 ([Cl12, Prop. 11, Thm. 19]). *Let $(R, |\cdot|)$ be a normed domain, and let $q_{/R}$ be a quadratic form.*

(a) *If q is Euclidean, then the corresponding quadratic lattice is maximal.*
(b) *If R is a CDVR, then q is Euclidean if and only if the corresponding quadratic lattice is maximal.*

Let R be a Hasse domain, and let $q_{/R}$ be a quadratic form. The *genus* $\mathfrak{g}(q)$ of R is the set of all equivalence classes of quadratic forms q' such that $q \cong_{K_v} q'$ for all $v \in S$ and $q \cong_{R_\mathfrak{p}} q'$ for all $\mathfrak{p} \in \Sigma_R$. A quadratic form q is *regular* if for all $d \in R$, whenever there exists $q' \in \mathfrak{g}(q)$ such that q' represents d, then q represents d. The set $\mathfrak{g}(q)$ is always finite [O'M, Thm. 103:4]; its cardinality is the *class number* of q. Thus a class number one form is necessarily regular. The converse is true in certain cases but not in general, as we will see below.

For $a \in R^\bullet$, we have $\mathfrak{g}(aq) = a\mathfrak{g}(q)$. So q is regular if and only if aq is.

Theorem 1.5 ([Cl12, Thm. 25]). *For a quadratic form q over a Hasse domain R, the following are equivalent:*

(i) *q is an ADC form.*
(ii) *q is regular and* locally ADC: *for all $\mathfrak{p} \in \Sigma_R$, $q_{/R_\mathfrak{p}}$ is ADC.*

Conjecture 1 ([Cl12, Conj. 27]). *For a Hasse domain R, there are finitely many isomorphism classes of anisotropic Euclidean quadratic forms over R.*

Conjecture 2 ([Cl12, Conj. 28]). *Every Euclidean quadratic form over a Hasse domain has class number one.*

1.2. ADC forms over $\mathbb{Z}$. In the first part of the paper we study ADC forms over $\mathbb{Z}$. By Theorem 1.5, this necessitates (i) an understanding of ADC forms over $\mathbb{Z}_p$ for all prime numbers p, and (ii) a classification of regular forms over $\mathbb{Z}$.

We study ADC forms over $\mathbb{Z}_p$ in §2. When p is odd, we give a complete classification; in fact, we work in the context of a complete discrete valuation ring with residue field of finite *odd* order. This local analysis is also applicable to the study and classification of ADC forms over Hasse domains of positive characteristic, though we do not consider this case here.

On the other hand, the study of quadratic forms in the dyadic case—i.e., over the ring of integers of a finite extension of $\mathbb{Q}_2$—is notoriously intricate. Here we confine ourselves to classifying ADC forms over $\mathbb{Z}_2$ in at most three variables.

In §3 these results are applied to the study of ADC forms over $\mathbb{Z}$. In order to get finite classification theorems we need finiteness theorems for regular forms. It is an old and widely believed conjecture that there are infinitely many primes $p \equiv 1 \pmod 4$ such that the ring of integers of $\mathbb{Q}(\sqrt{p})$ is a PID. It follows from Theorem 3.3 that, for each such prime, the form $q(x,y) = x^2 + xy + \frac{1-p}{4}y^2$ is ADC, so there ought to be infinitely many primitive indefinite binary integral ADC forms.

Because of the existence of sign-universal positive integral quaternary forms, for each $n \geq 5$ there are infinitely many sign-universal positive integral n-ary forms, hence infinitely many ADC forms. On the other hand, for each $1 \leq n \leq 4$ there are only finitely many primitive, positive integral ADC n-ary forms. The main result of the first part of the paper is a complete enumeration of such forms, with the proviso that the completeness of our list of primitive positive binary ADC forms is conditional on the Generalized Riemann Hypothesis (GRH). In summary: the *number of d-dimensional primitive positive integral ADC forms* is

1	1
2	764
3	103
4	6436

The unique primitive positive ADC unary form is x^2. Tables of primitive positive ADC binaries and ternaries are given at the end of this paper. The list of sign-universal positive quaternary forms is available at [QUQF].

To prove this enumeration result we make use of work of Voight [Vo07], Jagy–Kaplansky–Schiemann [JKS97] and Bhargava–Hanke [BH]. To complete the classification of positive integral ADC forms we need to deal with imprimitive forms, i.e., forms obtained by scaling a primitive form by a positive integer d. It is easy to see (Proposition 2.3) that this scaling integer d must be squarefree. Even more easily one sees that the unary form dx^2 is ADC when d is squarefree. It turns out that starting in dimension 3 an ADC form over any Hasse domain must be primitive (Theorem 3.5). The imprimitivity issue is most interesting for binary forms: here, for each primitive ADC binary form q there are infinitely many squarefree d such that dq is ADC and infinitely many squarefree d such that dq is not ADC. The class of such d is given by explicit congruence conditions in Theorem 3.4.

1.3. Euclidean forms over $\mathbb{Z}$. Next we consider the problem of classifying positive Euclidean integral quadratic forms. More precisely we reconsider it: it was solved by G. Nebe.

THEOREM 1.6 ([Ne03]). *There are* 70 *positive Euclidean integral forms.*

Notice that Theorem 1.6 verifies Conjecture 1 for positive forms over $\mathbb{Z}$. A direct computation then verifies Conjecture 2 for positive forms over $\mathbb{Z}$.

Nebe approaches the problem from the perspective of lattices in Euclidean space, using root lattices to find all lattices in Euclidean space with covering radius less than $\sqrt{2}$. Our setup so far has been in the language of quadratic forms theory (with the concession that we have only considered *free* quadratic lattices), but for our present work on Euclidean integral forms we would like to make use of both frameworks, so we give in §4 a dictionary between the two. In particular, "Euclideanity" corresponds to "covering radius", and "Euclidean form" corresponds to "covering radius less than $\sqrt{2}$".

REMARK 1.7. In [Ne03], Nebe lists 69 Euclidean integral quadratic forms. The present authors started searching for Euclidean forms in an ad hoc manner before becoming aware of Nebe's work. When we learned of her paper we compared our list of examples to hers: the form

$$q = x_1^2 + x_1x_4 + x_2^2 + x_2x_5 + x_3^2 + x_3x_5 + x_4^2 + x_4x_5 + 2x_5^2,$$

with Euclideanity $E(q) = 13/14$, was missing from her list. Professor Nebe informed us that this form was not included due to an oversight in her casewise analysis.

Such minor slips of computation and tabulation are unfortunately common in results which enumerate all quadratic forms having a certain property. One could ask what changes in the way such computationally intensive work is performed, presented and vetted would be sufficient to eliminate—or, more realistically, signficantly reduce—tabular inaccuracies of this kind. The contemporary mathematical community is only slowly coming to address this question, which is of course beyond the scope of the present work. We bring it up to emphasize the desirability of independent corroboration: multiple research groups performing the same or overlapping computations, ideally by distinct approaches and methods.

One of our main results does corroborate Nebe's work: rather than verifying Conjecture 1 by enumerating all Euclidean forms and then using this enumeration to verify a case of Conjecture 2, we do the reverse: we give an *a priori* proof that a positive integral Euclidean form has class number one (Theorem 6.1). We then use the known classification of class number one positive integral forms in order to compute all positive integral Euclidean forms; in this way we recover Nebe's list.

The classification of class number one positive integral forms is a quite different result from Nebe's; in fact it is a much longer calculation. The *finiteness* of the set of all positive, primitive integral forms of class number one was proven by G. L. Watson. He spent much of the rest of his career attempting to give an enumeration and published several papers on it but died before completing his work [Wa63a]–[Wa88]. A complete enumeration of all class number one *maximal* lattices was recently given by J. P. Hanke [Ha11] (this is sufficient for our purposes in view of Theorem 1.4(a)) and then (with no maximality condition) by D. Lorch and M. Kirschmer [LK13]. The case of binary forms has a different flavor; in recent work, the first author and his collaborators gave a list of 2779 $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of primitive, positive binary forms of class number one. This list is complete *conditional on GRH*: we encountered this phenomenon for ADC binaries above. In this case, however, we can avoid the dependence on GRH by giving a separate treatment of binary Euclidean forms, including indefinite ones.

We are optimistic that our method of proof of Conjecture 2 can be extended to other cases, e.g. to totally positive forms over the ring of integers of a totally real number field. If so, it should be possible to resolve further cases of Conjecture 1: it is a result of Pfeuffer [Pf79] that there are only finitely many class number one totally positive forms as we range over all rings of integers of totally real number fields. In fact, M. Kirschmer has just given an enumeration of the *maximal* such forms [Ki14]. Thus the complete classification of positive Euclidean forms over rings of integers of totally real number fields may be within reach.

2. ADC forms over compact discrete valuation rings. Let K be a field which is complete with respect to a nontrivial discrete valuation v and with *finite* residue field $k \cong \mathbb{F}_q = \mathbb{F}_{p^a}$. Let π be a uniformizing element for v. We assume, as usual, that $\operatorname{char} K \neq 2$. We say that K is *dyadic* if $\operatorname{char} k = 2$ and *nondyadic* otherwise. Let R be the valuation ring of K. Thus R is a compact discrete valuation ring: either the ring of integers of a p-adic number field or a formal power series ring $\mathbb{F}_q[[t]]$.

In this section we will give:

- A full classification of ADC forms over any nondyadic compact DVR.
- A classification of ADC forms in dimensions 2 and 3 over $\mathbb{Z}_2$.

2.1. Primitivity and semiprimitivity. Let R be a domain with fraction field K. Let $q = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j \in R[x]$ be a quadratic form over R. Let $D(q) = \{q(a) \mid a \in R^n\}$, and let $\mathfrak{n}(q) = \langle D(q) \rangle$, the ideal of R generated by $D(q)$. Thus R is ADC if and only if $D(q_{/K}) \cap R = D(q)$.

LEMMA 2.1. *Let* $q = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j \in R[x]$ *be a quadratic form. Let* $a \in R^{\bullet}$.

(a) *We have* $D(aq) = aD(q)$ *and* $\mathfrak{n}(aq) = (a)\mathfrak{n}(q)$.
(b) *If* aq *is ADC, then* q *is ADC.*
(c) *We have* $\mathfrak{n}(q) = \langle a_{ij} \rangle$.
(d) *If* $R \to S$ *is a ring homomorphism, then* $\mathfrak{n}(q_{/S}) = (\mathfrak{n}(q))S$.

Proof. (a) This is clear from the definitions.

(b) If aq is ADC, then

$$aD(q) = D(aq) = D(aq_{/K}) \cap R = aD(q_{/K}) \cap R,$$

so

$$D(q) = D(q_{/K}) \cap \frac{1}{a}R \supset D(q_{/K}) \cap R.$$

Clearly $D(q) \subset D(q_{/K}) \cap R$, so $D(q) = D(q_{/K}) \cap R$.

(c) (Cf. [Wa, p. 4].) Put $J = \langle a_{ij} \rangle$. Then $\mathfrak{n}(q) \subset J$. Conversely, let e_i be the ith standard basis vector of R^n; then $q(e_i) = a_{ii}$ for all $1 \le i \le n$, and $q(e_i + e_j) = a_{ii} + a_{jj} + a_{ij}$ for all $1 \le i \le j \le n$. It follows that $J \subset \mathfrak{n}(q)$.

(d) This is an immediate consequence of (c). ∎

Two quadratic forms q, q' over R are *unit equivalent* if there is $u \in R^{\times}$ such that $q' \cong uq$. As noted in [Cl12], replacing a quadratic form by a unit equivalent form does not disturb whether it is ADC or Euclidean or change its Euclideanity $E(q)$.

REMARK 2.2. In view of these properties, when studying ADC and Euclidean forms it is natural to classify forms up to unit equivalence rather than up to isomorphism, and we will take this convention here. For forms over $\mathbb{Z}$ this amounts to the following: we do not (as usual!) give separate consideration to negative forms, and for indefinite forms we identify f with $-f$ whether they are integrally equivalent or not (a somewhat subtle dichotomy). One must take a little care in the interaction of this convention with Gauss composition of binary forms: cf. Corollary 5.6.

We further observe that $\mathfrak{n}(q) = \mathfrak{n}(q')$ if q and q' are unit equivalent.

We say q is *primitive* if $\mathfrak{n}(q) = R$, and *semiprimitive* if there is no $a \in R^{\bullet} \setminus R^{\times}$ with $\mathfrak{n}(q) \subset a^2 R$.

PROPOSITION 2.3. *Let* R *be a domain; let* $q_{/R}$ *be a nonzero quadratic form.*

(a) *The form* q *is primitive if and only if it is* locally primitive: *for all* $\mathfrak{m} \in \operatorname{MaxSpec} R$, $q_{/R_{\mathfrak{m}}}$ *is primitive.*
(b) *If* R *is a Noetherian domain and* q *is ADC, then* q *is semiprimitive.*
(c) *If* R *is a Dedekind domain and* q *is ADC, then* $\mathfrak{n}(q)$ *is squarefree.*

Proof. (a) An ideal I in a ring R is proper if and only if $I \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of R if and only if $IR_{\mathfrak{m}} \subset \mathfrak{m}R_{\mathfrak{m}} \subsetneq R_{\mathfrak{m}}$ for some maximal ideal $\mathfrak{m}$ of R. The result follows from this and Lemma 2.1(b)&(c).

(b) Suppose that q is ADC but not semiprimitive. Then $\mathfrak{n}(q) \subset a^2R$ for $a \in R^\bullet \setminus R^\times$. By Lemma 2.1(a), there is a quadratic form $q'_{/R}$ with $q = a^2q'$. Since $q'(ax) = a^2q'(x) = q(x)$ and $D((a^2q)_{/K}) = D(q_{/K})$, and since q is ADC, so is q'. Moreover, $q_{/K} \cong q'_{/K}$. Thus if q is ADC, then

$$a^2\mathfrak{n}(q') = \mathfrak{n}(q) = \mathfrak{n}(q_{/K}) \cap R = \mathfrak{n}(q'_{/K}) \cap R = \mathfrak{n}(q').$$

This identity implies

$$(0) \subsetneq \mathfrak{n}(q') \subset \bigcap_{n \geq 1} (a^2)^n,$$

contradicting the Krull Intersection Theorem [Ma, Thm. 8.10].

(c) Combine (b) with [Cl12, Thm. 16]: ADC implies locally ADC. ∎

2.2. Primitive square classes and ADC forms. Let R be a UFD with fraction field K. Let $\iota : R^\bullet/R^{\times 2} \to K^\times/K^{\times 2}$ be the canonical map on square classes. Let Σ_R be the set of height one prime ideals of R, and let $\mathbb{Z}_\Sigma$ be the free abelian group on Σ. Uniqueness of factorization gives a short exact sequence

$$1 \to R^\times \to K^\times \xrightarrow{V} \mathbb{Z}_\Sigma \to 0.$$

Since $\mathbb{Z}_\Sigma$ is free abelian, the sequence splits:

$$K^\times \cong \mathbb{Z}_\Sigma \times R^\times. \tag{3}$$

Passing to square classes, we get a split exact sequence

$$1 \to R^\times/R^{\times 2} \to K^\times/K^{\times 2} \xrightarrow{V} \bigoplus_{\mathfrak{p} \in \Sigma_R} \mathbb{Z}/2\mathbb{Z} \to 1.$$

Since $R^{\times 2} \subset \ker V$, (3) also induces an exact sequence of monoids

$$1 \to R^\times/R^{\times 2} \to R^\bullet/R^{\times 2} \xrightarrow{V_R} \bigoplus_{\mathfrak{p} \in \Sigma} \mathbb{N} \to 0.$$

Let us say that a square class $s \in R^\bullet/R^{\times 2}$ is *primitive* if every component of $V_R(s)$ lies in $\{0, 1\}$. Now we observe:

- For every square class $s \in R$, there is a unique primitive square class s_0 and $x \in R$ such that $s = x^2 s_0$.
- For every square class $S \in K$, there is a unique primitive square class s_0 of R such that $\iota(s_0) = S$. In other words, ι restricts to a bijection from the primitive square classes of R to the square classes of K.

Proposition 2.4. *Let R be a UFD, and let $q_{/R}$ be a quadratic form. Then q is ADC if and only if for every square class of K which is K-repre-*

sented by q, the corresponding primitive square class of R is R-represented by q.

Proof. Suppose q is ADC and K-represents a square class S of K. Let $s \in R$ be an element of the corresponding primitive square class of R; since $sS^{-1} \in K^{\times 2}$, q K-represents s; since q is ADC and $s \in R$, q R-represents s.

Suppose that q R-represents every primitive square class in R whose corresponding square class in K is K-represented by q, and let $s \in R^\bullet$ be K-represented by q. We may write $s = x^2 s_0$ with s_0 representing a primitive square class and $u \in R^\times$. By assumption, there is $v \in R^n$ such that $q(v) = s_0$, and thus $q(xv) = x^2 s_0 = s$. ∎

2.3. Preliminary generalities. Let R be a compact DVR with fraction field K, residue field $\mathbb{F}_q$ and uniformizing element π. We define δ to be 0 if R is nondyadic; if R is dyadic, then K is a finite-dimensional $\mathbb{Q}_2$-vector space, and we define $\delta = \dim_{\mathbb{Q}_2} K$.

PROPOSITION 2.5. *Let R be a compact DVR with fraction field K.*

(a) *We have $\# K^\times/K^{\times 2} = 2^{\delta+2}$.*
(b) *Suppose R is nondyadic, and fix any $r \in R^\times \setminus R^{\times 2}$. Then $1, r, \pi, \pi r$ is a set of coset representatives for $K^{\times 2}$ in $K^\times$.*
(c) *A set of coset representatives for $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ is $1, 3, 5, 7, 2, 6, 10, 14$.*

Proof. (a) [L, Thm. VI.2.22]. (b) [L, Thm. VI.2.2]. (c) [L, Cor. VI.2.24]. ∎

PROPOSITION 2.6. *Let R be a compact DVR with fraction field K, and let $q_{/R}$ be an n-ary quadratic form.*

(a) *If $n = 2$ and q is anisotropic, then q K-represents exactly $2^{\delta+1}$ square classes of K (i.e., precisely half of them).*
(b) *If $n = 3$ and q is anisotropic, then q K-represents exactly $2^{\delta+2} - 1$ square classes of K: all except the class of $-\operatorname{disc}(q)$.*
(c) *If $n \geq 4$, then q is K-universal.*

Proof. (a) Suppose first that $q \cong \langle 1, a\rangle$ is a principal form. Since q is anisotropic, $-a$ is not a square in K, and q is the norm form of the quadratic field extension $L = K(\sqrt{-a})$. By local class field theory [Mi, Thm. I.1.1],

$$K^\times/NL^\times \cong \operatorname{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z},$$

so q represents precisely half of the square classes. In general, q is a scalar multiple of a principal form and then it follows from the above that $q(K^\times) \subset K^\times/K^{\times 2}$ is a coset of an index 2 subgroup.

(b) [L, Cor. VI.2.15].

(c) Every quadratic form in at least five variables over K is isotropic [L, Thm. VI.2.12], hence [L, Cor. I.3.5] every form in at least four variables is universal. ∎

Corollary 2.7. *Let $q_{/R}$ be an n-ary ADC form over a compact DVR. If $n \geq 3$, then q is primitive.*

Proof. If $n \geq 4$, then $q_{/R}$ is ADC if and only if it is universal, and universal forms are primitive. Suppose $n = 3$. If q is isotropic, then it is K-universal; since it is ADC, it is universal, hence primitive. Otherwise q is anisotropic so K-represents $2^{\delta+2}-1$ square classes in K. However, if q is not primitive then it does not represent any of the unit square classes, hence it represents at most $2^{\delta+1}$ square classes. ∎

2.4. ADC forms over nondyadic compact DVRs. Let R be a compact DVR with residue field $\mathbb{F}_q$, q odd. Then the canonical map $R^\times/R^{\times 2} \to \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$ is an isomorphism, hence $R^\times/R^{\times 2}$ has order 2. For $x \in R^\times$, define $\left(\frac{x}{q}\right)$ to be 1 if $x \in R^{\times 2}$—or equivalently, if the reduction of x modulo (π) is a square in the finite field $\mathbb{F}_q$—and -1 otherwise.

Lemma 2.8 ([C, §8.3]). *Every quadratic form q over a nondyadic DVR may be diagonalized. It follows that q may be written in the form*

$$q = \bigoplus_{i \in \mathbb{N}} \pi^i J_i(q) \tag{4}$$

with each $J_i(q)$ diagonal and unimodular: $\operatorname{disc}(J_i(q)) \in R^\times$.

The forms $J_i(q)$ are called the *Jordan components* of q, and the decomposition (4) is called the *Jordan splitting*. We will write $d_i(q)$ for $\dim J_i(q)$.

Theorem 2.9. *Let $q_{/R}$ be nondegenerate of dimension $n \geq 1$.*

(a) *If $v(\operatorname{disc}(q)) \leq 1$, then q is Euclidean, hence ADC.*
(b) *Suppose either*
  (i) *$d_0(q) \geq 3$, or*
  (ii) *$d_0(q) = 2$ and $\left(\frac{-\operatorname{disc}(J_0(q))}{q}\right) = 1$.*

  Then q is universal, hence ADC.
(c) *If $d_0(q) = d_1(q) = 0$, then q is not ADC.*
(d) *If $n \geq 3$ and $d_0(q) = 0$, then q is not ADC.*
(e) *If $n \geq 4$ and $d_0(q) = 1$, then q is not ADC.*
(f) *Suppose $n \geq 4$ and $J_0(q)$ is 2-dimensional anisotropic. Then:*
  (i) *If $d_1(q) = 0$, then q is not ADC.*
  (ii) *If $d_1(q) = 1$, then q is ADC if and only if it is universal if and only if $J_0(q) \oplus J_1(q)$ is isotropic.*
  (iii) *If $d_1(q) \geq 2$, then q is universal, hence ADC.*

Proof. (a) If $v(\operatorname{disc}(q)) \leq 1$, then the quadratic lattice of q is maximal. By [Cl12, Thm. 19], q is Euclidean, and thus by [Cl12, Thm. 8], q is ADC.

(b) The hypotheses imply that $J_0(q)$ is isotropic, hence K-universal. By part (a), $J_0(q)$ is ADC and thus universal. It follows that q is universal.

(c) Since $d_0(q) = d_1(q) = 0$, $q = \pi^2 q'$ for some form q'. The form q K-represents some element with valuation 0 or 1, but does not R-represent any such element.

(d) This is a special case of Corollary 2.7.

(e) Since $n \geq 4$, $q = ux_1^2 + \pi q'(x_2, \dots, x_n)$ is K-universal, but R-represents exactly one of the two unit square classes in K.

(f) Since $\dim q \geq 4$, q is K-universal, thus it is ADC if and only if it is R-universal.

(i) Since $q = u_1x_1^2 + u_2x_2^2 + \pi^2 q'(x_3, \dots, x_n)$ and $u_1x_1^2 + u_2x_2^2$ is anisotropic, q does not R-represent π.

(ii) Since $d_1(q) = 1$, $v(\mathrm{disc}(J_0(q) \oplus J_1(q))) = 1$, so by (a), $J_0(q) \oplus J_1(q)$ is ADC. Thus if it is isotropic, it is universal, and hence so is q. Conversely, if $J_0(q) \oplus J_1(q)$ is anisotropic, then it fails to K-represent some element $x \in R$ of valuation 0 or 1, hence $J_0(q) \oplus J_1(q) \oplus \pi^2 q'$ does not R-represent x.

(iii) Since q has $q' = u_1x_1^2 + u_2x_2^2 + \pi u_3x_3^2 + \pi u_4x_4^2$ as a subform, it suffices to show q' is universal. But indeed $u_1x_1^2 + u_2x_2^2$ R-represents 1 and r, and thus $\pi(u_3x_3^2 + u_4x_4^2)$ R-represents π and πr. It follows that q is universal. ∎

Theorem 2.10. *Let $q(x, y) = ax^2 + by^2$ be a nondegenerate binary form over R. We may assume $v(a) \leq v(b)$.*

(a) *If $v(ab) \leq 1$, then q is ADC.*
(b) *If $v(b) \geq 2$, then q is not ADC.*
(c) *If $v(a) = v(b) = 1$, then:*
  (i) *$\pi x^2 + \pi y^2 \cong \pi r x^2 + \pi r y^2$ is ADC if and only if $q \equiv 3 \pmod 4$.*
  (ii) *$\pi x^2 + \pi r y^2$ is ADC if and only if $q \equiv 1 \pmod 4$.*

Proof. (a) A quadratic form q over a nondyadic CDVR with $v(\mathrm{disc}(q)) \in \{0, 1\}$ is maximal, hence ADC.

(b) If $v(b) \geq 2$, then q represents at most one primitive square class so is not ADC.

(c) If $v(a) = v(b) = 1$, then $q = \pi q'$, with $q' = u_1x^2 + u_2y^2$, $u_1, u_2 \in R^\times$. If q' is isotropic, then q is K-universal, but it does not R-represent any unit square class so it is not ADC. If q' is anisotropic then among primitive square classes it represents preciesly the unit square classes 1 and r, so q represents precisely π and πr, hence it is ADC. A binary form q is isotropic if and only if $\left(\frac{-\mathrm{disc}\, q}{q}\right) = 1$, and the result follows. ∎

For future use we record the following special case of Theorem 2.10.

Corollary 2.11. *A primitive binary form $q_{/R}$ is ADC if and only if $v(\mathrm{disc}\, q) \leq 1$.*

THEOREM 2.12. *Let $q(x,y,z) = ax^2 + by^2 + cz^2$ be a nondegenerate ternary form over R. We may assume $v(a) \le v(b) \le v(c)$.*

(a) *If $v(abc) \le 1$, then q is ADC.*
(b) *If $v(a) \ge 1$, then q is not ADC.*
(c) *If $v(c) \ge 2$, then:*
  (i) *If $q \equiv 1 \pmod 4$, then q is ADC if and only if $v(a) = v(b) = 0$ and $ab^{-1} \in R^{\times 2}$.*
  (ii) *If $q \equiv 3 \pmod 4$, then q is ADC if and only if $v(a) = v(b) = 0$ and $ab^{-1} \in R^{\times} \setminus R^{\times 2}$.*
(d) *Suppose $v(a) = 0$, $v(b) = 1$, and $v(c) = 1$. Then:*
  (i) *If $q \equiv 1 \pmod 4$, then q is ADC if and only if $ab^{-1} \in K^{\times} \setminus K^{\times 2}$.*
  (ii) *If $q \equiv 3 \pmod 4$, then q is ADC if and only if $ab^{-1} \in K^{\times 2}$.*

Proof. The key point in what follows is that, by Proposition 2.6, an anisotropic ternary form over K represents precisely three out of the four square classes.

(a) As above, $v(abc) \le 1$ implies q is maximal, hence ADC.

(b) If $v(a) \ge 1$, then q does not represent either of the two unit square classes, but as it K-represents at least one of these, q is not ADC.

(c) If $v(c) \ge 2$, then q represents the same primitive square classes as its subform $ax^2 + by^2$. If $ax^2 + by^2$ is isotropic, it is universal, and then q is universal, hence ADC. If $ax^2 + by^2$ is anisotropic, it K-represents two of the primitive square classes and q K-represents at least three of the primitive square classes, so q is not ADC. This leads immediately to the given conditions.

(d) Since the ADC condition depends only on unit equivalence, we may assume that $a = 1$. The form $q = x^2 + \pi by^2 + \pi cz^2$ does not represent r, so it is not universal. Therefore if q is isotropic, it is not ADC. On the other hand, it represents the three primitive square classes $1, \pi, \pi r$, so if it is anisotropic, it is ADC. As for any form over a field of characteristic different from 2, q is isotropic if and only if $x^2 + \pi by^2$ K-represents $-\pi c$. This happens if and only if $b \equiv -c \pmod{K^{\times 2}}$. If $q \equiv 1 \pmod 4$, this holds if and only if $bc^{-1} \in K^{\times}$; if $q \equiv 3 \pmod 4$, this holds if and only if $bc^{-1} \in K^{\times} \setminus K^{\times 2}$. ∎

2.5. Binary and ternary ADC forms over $\mathbb{Z}_2$

LEMMA 2.13. *Let $q(x,y)_{/\mathbb{Z}_2}$ be a nondegenerate binary quadratic form.*

(a) *The form q is either diagonalizable over $\mathbb{Z}_2$ or $\mathbb{Z}_2$-equivalent to one of $2^a(x^2 + xy + y^2)$ or $2^a xy$ for some $a \in \mathbb{N}$.*
(b) *We have $v(\operatorname{disc} q) \in \{-2\} \cup \mathbb{N}$.*

Proof. (a) [C, Lemma 8.4.1]. (b) This follows immediately. ∎

When dealing with binary forms, there is an alternative normalization of the discriminant: we define the *Discriminant* (note the capitalization!)

$$\Delta(ax^2 + bxy + cy^2) = b^2 - 4ac = -4\operatorname{disc}(ax^2 + bxy + c^2).$$

Thus over $\mathbb{Z}_2$ we have $v(\Delta(q)) = v(\operatorname{disc} q) + 2 \in \{0, 2, 3, \ldots\}$.

THEOREM 2.14. *Let $q(x, y)$ be a nondegenerate binary form over $\mathbb{Z}_2$.*

(a) *If $v(\Delta(q)) = 0$, then q is ADC.*
(b) *Suppose $v(\Delta(q)) = 2$. Then:*
   (i) *If q is primitive, then q is ADC if and only if $\Delta(q) \equiv 12, 20, 28 \pmod{32}$.*
   (ii) *If $q = 2q'$, then q is ADC if and only if $\Delta(q) \equiv 20 \pmod{32}$.*
(c) *If $v(\Delta(q))) = 3$, then q is ADC.*
(d) *If $v(\Delta(q))) = 4$, then q is ADC if and only if $q = 2q'$ with $\Delta(q') \equiv 20 \pmod{32}$.*
(e) *If $v(\Delta(q)) \geq 5$, then q is not ADC.*

Proof. (a) If $v(\operatorname{disc}(q)) = -2$, then by Lemma 2.13(b), q is maximal, hence ADC.

(b) (i) Suppose $v(\operatorname{disc}(q)) = 0$ and q is primitive. By Lemma 2.13(a), $q \cong_{\mathbb{Z}_2} ax^2 + by^2$ with $a, b \in \mathbb{Z}_2^\times$. Because being an ADC form is invariant under unit equivalence, we may assume without loss of generality that $a = 1$, and then we are left with consideration of the forms $x^2 + y^2$, $x^2 + 3y^2$, $x^2 + 5y^2$, $x^2 + 7y^2$. The forms $x^2 + y^2$ and $x^2 + 5y^2$ have discriminant 1 (mod 4) and are thus maximal, hence Euclidean. The form $x^2 + 3y^2$ is a nonmaximal lattice in a $\mathbb{Q}_2$-quadratic space with associated maximal lattice $x^2 + xy + y^2$. By Proposition 2.6, a binary form represents precisely four out of the eight square classes in $\mathbb{Q}_2$. Examining $x^2 + 3y^2$ we see that it $\mathbb{Z}_2$-represents primitive elements of the four unit square classes $1, 3, 5, 7 \pmod 8$ and is thus ADC. The form $x^2 + 7y^2$ is a nonmaximal lattice in the $\mathbb{Q}_2$-quadratic space with associated maximal lattice xy, so in order to be ADC, x^2+7y^2 must be universal. But $x^2+7y^2 \cong_{\mathbb{Z}_2} x^2-y^2$ does not $\mathbb{Z}_2$-represent 2.

(ii) If $v(\operatorname{disc} q) = 0$ and q is not primitive, then by Lemma 2.13(a), either $\operatorname{disc} q \equiv 7 \pmod 8$ and $q \cong 2xy$, or $\operatorname{disc} q \equiv 3 \pmod 8$ and $q \cong 2(x^2+xy+y^2)$. In the former case q is isotropic but not hyperbolic so it is not ADC. In the latter case it follows from our previous analysis that the primitive square classes represented by x^2+xy+y^2 are $1, 3, 5, 7$, so the primitive square classes represented by $2(x^2 + xy + y^2)$ are $2 \cdot 1, 2 \cdot 3, 2 \cdot 5, 2 \cdot 7$. Since an anisotropic binary form $\mathbb{Q}_2$-represents precisely four primitive square classes, it follows that $2(x^2 + xy + y^2)$ is ADC.

(d) Suppose $v(\operatorname{disc} q) = 2$. If q is not diagonalizable then $q = 2^2q'$ so q is not ADC. Thus we may suppose $q = ax^2 + by^2$ with either $(v(a), v(b)) =$

$(0,2)$ or $(v(a), v(b)) = (1,1)$. In the former case q represents only one primitive square class so it is not ADC. In the latter case $q = 2q'$ with $q' = u_1x^2 + u_2y^2$, $u_1, u_2 \in \mathbb{Z}_2^\times$. Then q is ADC if and only if q' is ADC, anisotropic, and represents the four unit square classes. By our previous analysis, this holds if and only if $\operatorname{disc} q' \equiv 3 \pmod 8$.

(e) Suppose $v(\operatorname{disc} q) \geq 3$. Again, if q is not diagonalizable then $q = 2^2q'$, so q is not ADC. If q is diagonalizable and not of the form $2^2q'$, then either $q = u_1x^2 + 2^a u_2 y^2$ with $u_1, u_2 \in \mathbb{Z}_2^\times$ and $a \geq 3$, or $q = 2u_1x^2 + 2^a u_2 y^2$ with $u_1, u_2 \in \mathbb{Z}_2^\times$ and $a \geq 2$. Either way q represents only one primitive square class so it is not ADC. ∎

For future use we record the following special case of Theorem 2.14.

Corollary 2.15. *A primitive binary form $q_{/\mathbb{Z}_2}$ is ADC if and only if*

$$\Delta(q) \equiv 1, 3, 5, 7, 8, 9, 11, 12, 13, 15, 17, 19, 20, 21, 23, 24, 25, 27, 28, 29, 31 \pmod{32}.$$

Lemma 2.16 ([C, Lemma 8.4.1]). *Let $q(x,y,z)$ be a nondegenerate ternary form over $\mathbb{Z}_2$. Then q is $\mathbb{Z}_2$-equivalent to a diagonal form, to $2^a(xy) + 2^b uz^2$ or to $2^a(x^2 + xy + y^2) + 2^b uz^2$ for $a, b \in \mathbb{N}$, $u \in \mathbb{Z}_2^\times$.*

Theorem 2.17. *Let $q = ax^2 + by^2 + cz^2$ be a nondegenerate diagonal ternary form over $\mathbb{Z}_2$; we may assume $v(a) \leq v(b) \leq v(c)$.*

(a) *If $(v(a), v(b), v(c)) \in \{(0,0,0), (0,0,1)\}$, then q is ADC.*
(b) *If $(v(a), v(b), v(c)) \in \{(0,1,1), (0,1,2)\}$, then q is ADC if and only if it is anisotropic.*
(c) *Otherwise q is not ADC.*

Proof. Step 0. Recall that a nondegenerate ternary form q $\mathbb{Q}_2$-represents all eight square classes of $\mathbb{Q}_2$ if it is isotropic, and represents all but $-\operatorname{disc} q$ if it is anisotropic. In particular, q $\mathbb{Q}_2$-represents at least three out of the four unit square classes, so if q is ADC, it must represent at least three of the primitive unit square classes.

Step 1. Suppose $(v(a), v(b), v(c)) \in \{(0,0,0), (0,0,1)\}$ or that q is anisotropic and $(v(a), v(b), v(c)) \in \{(0,1,1), (0,1,2)\}$. We will (unfortunately) show that q is ADC by brute force. Since the ADC condition depends only on the unit equivalence class of q and $v(a) = 0$, we may assume without loss of generality that $a = 1$. Then:

- If $(v(a), v(b), v(c)) = (0,0,0)$, then q is unit equivalent to one of:

$$\langle 1,1,1\rangle, \langle 1,1,3\rangle, \langle 1,1,5\rangle, \langle 1,1,7\rangle, \langle 1,3,3\rangle,$$
$$\langle 1,3,5\rangle, \langle 1,3,7\rangle, \langle 1,5,5\rangle, \langle 1,5,7\rangle, \langle 1,7,7\rangle.$$

We consider a representative example: let $q = x^2 + 5y^2 + 5z^2$. Then q is anisotropic and thus does not $\mathbb{Q}_2$-represent the square class $-\operatorname{disc} q \equiv 7 \pmod{\mathbb{Q}^{\times 2}}$. So, it represents the other seven primitive $\mathbb{Z}_2$-square classes:

$$\begin{aligned}
1 &\cong 1^2 + 5 \cdot 0^2 + 5 \cdot 0^2, \\
2 &\cong 50 \cong 5^2 + 5 \cdot 2^2 + 5 \cdot 1^2, \\
3 &\cong 11 \cong 1^2 + 5 \cdot 1^2 + 5 \cdot 1^2, \\
5 &\cong 0^2 + 5 \cdot 1^2 + 5 \cdot 0^2, \\
6 &\cong 1^2 + 5 \cdot 1^2 + 5 \cdot 0^2, \\
10 &\cong 0^2 + 5 \cdot 1^2 + 5 \cdot 1^2, \\
14 &\cong 2^2 + 5 \cdot 1^2 + 5 \cdot 1^2.
\end{aligned}$$

- If $(v(a), v(b), v(c)) = (0, 0, 1)$, then q is unit equivalent to one of:

$$\begin{gathered}
\langle 1,1,2\rangle,\ \langle 1,1,6\rangle,\ \langle 1,1,10\rangle,\ \langle 1,1,14\rangle,\ \langle 1,3,2\rangle,\ \langle 1,3,6\rangle, \\
\langle 1,3,10\rangle, \langle 1,3,14\rangle,\ \langle 1,5,2\rangle,\ \langle 1,5,6\rangle,\ \langle 1,5,10\rangle,\ \langle 1,5,14\rangle, \\
\langle 1,7,2\rangle,\ \langle 1,7,6\rangle,\ \langle 1,7,10\rangle,\ \langle 1,7,14\rangle.
\end{gathered}$$

We consider a representative example: let $q = x^2 + 7y^2 + 14z^2$. Then q is isotropic and represents all eight primitive $\mathbb{Z}_2$-square classes:

$$\begin{aligned}
1 &\cong 1^2 + 7 \cdot 0^2 + 14 \cdot 0^2, \\
2 &\cong 18 \cong 2^2 + 7 \cdot 0^2 + 14 \cdot 1^2, \\
3 &\cong 11 \cong 2^2 + 7 \cdot 1^2 + 14 \cdot 0^2, \\
5 &\cong 21 \cong 0^2 + 7 \cdot 1^2 + 14 \cdot 1^2, \\
6 &\cong 22 \cong 1^2 + 7 \cdot 1^2 + 14 \cdot 1^2, \\
7 &\cong 0^2 + 7 \cdot 1^2 + 14 \cdot 0^2, \\
10 &\cong 42 \cong 0^2 + 7 \cdot 2^2 + 14 \cdot 1^2, \\
14 &\cong 0^2 + 7 \cdot 0^2 + 14 \cdot 1^2.
\end{aligned}$$

- An anisotropic form with $(v(a), v(b), v(c)) = (0, 1, 1)$ is unit equivalent to one of:

$$\langle 1,2,2\rangle, \langle 1,2,6\rangle, \langle 1,6,14\rangle, \langle 1,10,10\rangle, \langle 1,10,14\rangle.$$

- An anisotropic form with $(v(a), v(b), v(c)) = (0, 1, 1)$ is unit equivalent to one of:

$$\langle 1,2,4\rangle, \langle 1,2,12\rangle, \langle 1,6,12\rangle, \langle 1,6,20\rangle, \langle 1,10,12\rangle, \langle 1,14,12\rangle,\ \langle 1,14,20\rangle.$$

In all cases, the method of proof is the same as above: find $x, y, z \in \mathbb{Z}$ such that $q(x, y, z)$ represents seven of the eight primitive square classes.

It remains to show that none of the other forms is ADC.

Step 2. Suppose $(v(a), v(b), v(c)) = (0, 1, 1)$ and q is isotropic. We may assume $a = 1$ and write $b = 2u_2$, $c = 2u_3$ with $u_2, u_3 \in \mathbb{Z}_2^\times$. If q is isotropic and ADC, it represents each $d \in \{1, 3, 5, 7\}$. Considering the equation $x^2 + 2u_2y^2 + 2u_3z^2 = d$ modulo 8 yields

$$u_2y^2 + u_3z^2 \equiv \frac{d-1}{2} \pmod 4.$$

But no matter what choices of u_2 and u_3 we make, the quadratic form $u_2y^2 + u_3z^2$ modulo 4 takes only two out the three values $\{1, 2, 3\}$, a contradiction.

Step 3. Suppose $(v(a), v(b), v(c)) = (0, 1, 2)$ and q is isotropic. We may assume $a = 1$ and write $b = 2u_2$, $c = 4u_3$ with $u_2, u_3 \in \mathbb{Z}_2^\times$. If q is isotropic and ADC, it represents each $d \in \{2, 6, 10, 14\}$. Suppose $x^2 + 2u_2y^2 + 4u_3z^2 = 2d$; then $v(x) > 0$, so we may write $x = 2X$ and simplify to get $2X^2 + u_2y^2 + 2u_3z^2 = d$. Since $v(d) = 0$ we must have $v(y) = 0$ and thus $y^2 \equiv 1 \pmod 8$, so we get $2X^2 + 2u_3z^2 \equiv d - u_2 \pmod 8$ or

$$X^2 + u_3z^2 \equiv \frac{d-u_2}{2} \pmod 4.$$

For any choice of u_2, u_3, there is a choice of d such that this congruence has no solution, a contradiction.

Step 4. Suppose $v(a) > 0$. Then $q = 2q'$ is not primitive, so it represents no primitive unit square class. Thus q is not ADC.

Step 5. Suppose $v(a) = 0$ and $v(b) \geq 2$, so up to unit equivalence, $q = x^2 + 4by^2 + 4cz^2$. Going modulo 4 shows that q does not $\mathbb{Z}_2$-represent 3 or 7, so is not ADC.

Step 6. Suppose $v(a) = v(b) = 0$, $v(c) \geq 2$, so up to unit equivalence, $q = x^2 + uy^2 + 4cz^2$ for $u \in \mathbb{Z}_2^\times$. The mod 4 reduction of q represents only two of the three classes $\{1, 2, 3\}$ mod 4, and thus fails to $\mathbb{Z}_2$-represent both of $\{1, 5\}$, both of $\{2, 6\}$ or both of $\{3, 7\}$, so it is not ADC.

Step 7. Suppose $v(c) \geq 3$. No diagonal binary form $ax^2 + by^2$ $\mathbb{Z}/8\mathbb{Z}$-represents more than four of the six classes $\{1, 2, 3, 5, 6, 7\}$. From this it follows that $q(x, y, z) = ax^2 + by^2 + cz^2 = d$ has no $\mathbb{Z}_2$-solution for at least two primitive square classes d, so q is not ADC. ∎

Theorem 2.18. *Let $q(x, y, z)$ be a nondiagonalizable ternary form over $\mathbb{Z}_2$.*

(a) *Suppose q is unit equivalent to $2^axy + 2^bz^2$ for $a, b \in \mathbb{N}$. Then q is ADC if and only if $a = 0$ or $(a, b) = (1, 0)$.*
(b) *Suppose q is unit equivalent to $2^a(x^2 + xy + y^2) + 2^bz^2$ for $a, b \in \mathbb{N}$. Then q is ADC if and only if $(a, b) \in \{(0, 0), (1, 0), (0, 1)\}$.*

Proof. (a) If $a = 0$, then q contains the universal form xy as a subform, so it is universal, hence ADC. If $(a, b) = (1, 0)$, then it is easy to verify that $q = 2xy + z^2$ represents all eight primitive square classes. Alternately, by [C, p. 118], $q = 2xy + z^2 \sim x^2 + y^2 + 7z^2$, so q is ADC by Theorem 2.17.

If $a \geq 1$ and $b \geq 1$, then q is not primitive, hence not ADC. If $a \geq 2$ and $b = 0$, then q does not represent any of $2, 6, 10, 14$, so it is not ADC.

(b) If $(a, b) = (0, 0)$, then $v(\operatorname{disc} q) = -2$, so q is maximal, hence ADC. If $(a, b) = (0, 1)$, then $v(\operatorname{disc} q) = -1$, so q is maximal, hence ADC. If $(a, b) = (1, 0)$, then $q = 2(x^2 + xy + y^2) + z^2 \sim_{\mathbb{Q}_2} 2x^2 + 6y^2 + z^2$ is anisotropic, so it does not $\mathbb{Q}_2$-represent the square class $5 \equiv -\operatorname{disc} q \pmod{\mathbb{Q}_2^{\times 2}}$. One verifies directly that it represents the other seven primitive $\mathbb{Z}_2$-square classes.

If a and b are both at least one, then q is not primitive and thus not ADC. If either $a \geq 2$ or $b \geq 2$, then q does not represent any of the four primitive square classes $2, 6, 10, 14$, so it is not ADC. ∎

3. ADC forms over $\mathbb{Z}$

3.1. Unary forms

THEOREM 3.1. *Let R be a UFD or a Hasse domain, $a \in R^\bullet$, and $q(x) = ax^2$. Then R is ADC if and only if a is squarefree.*

Proof. We suppose R is a UFD. Then q is semiprimitive if and only if (a) is *not* contained in any proper ideal of the form (b^2) if and only if a is squarefree. By Proposition 2.3(a) these conditions are necessary for q to be ADC. Conversely, if a is squarefree then $aR^{\times 2}$ is the primitive square class corresponding to $aK^{\times 2}$, so q is ADC by Proposition 2.4. Next we suppose R is a Hasse domain. By Proposition 2.3(c), if q is ADC then $(a) = \mathfrak{n}(q)$ is squarefree. For all $\mathfrak{p} \in \Sigma_R$, $R_\mathfrak{p}$ is a UFD, so by what we have just shown, $q_{/R_\mathfrak{p}}$ is ADC. Thus q is locally ADC; certainly q is regular, so q is ADC. ∎

For the rest of this section all quadratic forms are nondegenerate over $\mathbb{Z}$. The ADC property depends only on the unit equivalence class of a quadratic form. So we need only consider positive forms and indefinite forms.

3.2. Binary forms. Let Δ be a quadratic Discriminant, i.e., an integer which is 0 or 1 modulo 4. If $\Delta > 0$, then we denote by $C(\Delta)$ the set of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of primitive binary forms of Discriminant Δ. If $\Delta < 0$, then we denote by $C(\Delta)$ the set of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of primitive, positive binary forms of Discriminant Δ. Elementary reduction theory shows that in either case $C(\Delta)$ is a finite set. Moreover, in his *Disquisitiones Arithmeticae*, Gauss endowed $C(\Delta)$ with a natural composition law, under which it becomes a finite abelian group, the *class group of Discriminant* Δ. Slightly abusing notation, we write "$q \in C(\Delta)$" to mean: q is a primitive (and positive, if $\Delta < 0$) binary form of discriminant Δ.

For $q = Ax^2 + Bxy + Cy^2 \in C(\Delta)$, the form $\overline{q} = Ax^2 - Bxy + Cy^2$ represents the inverse of q in $C(\Delta)$. A form q such that $[q] = [\overline{q}]$ is called *ambiguous*.

A quadratic discriminant Δ is *idoneal* if $C(\Delta) \cong (\mathbb{Z}/2\mathbb{Z})^a$ for some $a \in \mathbb{N}$—i.e., if every $q \in C(\Delta)$ is ambiguous. A form $q \in C(\Delta)$ is *idoneal* if Δ is idoneal. A quadratic discriminant Δ is *bi-idoneal* if $C(\Delta) \cong \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^a$ for some $a \in \mathbb{N}$. A form $q \in C(\Delta)$ is *idoneal* if Δ is idoneal. A form $q \in C(\Delta)$ is *bi-idoneal* if Δ is bi-idoneal and q is *not* ambiguous.

Though in general a regular form over a Hasse domain may have class number greater than one (we will meet such forms later in this section), an anisotropic binary form q over the ring of integers of a number field which is regular—or even *almost regular*, i.e., represents all but finitely many elements of R which are represented by the genus $\mathfrak{g}(q)$—has class number one [Cl08, Thm. A.3]. (The result is stated when R has characteristic 0 but the argument works so long as the characteristic of R is not 2.) We want a version of this result over $\mathbb{Z}$ which reexpresses the class number one condition in terms of the structure of the class group $C(\Delta)$. While this variant is certainly known to some experts, we have not been able to find it in the literature, so for completeness we indicate a proof.

THEOREM 3.2. *Let q be a primitive, nondegenerate binary quadratic form of nonsquare discriminant Δ. If $\Delta < 0$, we suppose that q is positive. The following are equivalent:*

(i) *q is regular.*
(ii) *q is idoneal or bi-idoneal.*

Proof. STEP 1. Suppose q is regular. It is an easy consequence of the local theory recalled in §2 that the set of prime numbers $p \nmid 2\Delta$ which are represented by q is a union of congruence classes modulo some positive integer N (in fact, the classical theory shows that one may take $N = 4\Delta$). Moreover, q represents infinitely many prime numbers [We82] or [Br54], so q represents a full congruence class of primes.

STEP 2. We claim that an integral binary form which represents a full congruence class of primes must be idoneal or bi-idoneal. This is proved in [ClHPT, Thm. 1] for positive forms. In fact the proof also works in the indefinite case, since the four bulleted "tenets of genus theory" hold also in the indefinite case. (Although references are given to [Cx89], which states these results for positive forms only, the proofs do not use this hypothesis. In fact these results were established in Gauss's *Disquisitiones Arithmeticae*; an accessible account can be found in [F].)

STEP 3. Suppose q is idoneal or bi-idoneal. Then the aforementioned genus theory shows that the only forms which are everywhere locally equivalent to q are q and $\overline{q}$. Since $\overline{q}$ is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to q, q has class number 1 and is thus regular. ∎

THEOREM 3.3. *Let $q(x,y)_{/\mathbb{Z}}$ be a primitive binary quadratic form. Then q is ADC if and only if all of the following hold:*

(i) *q is idoneal or bi-idoneal.*
(ii) *For all odd primes p, $v_p(\Delta(q)) \leq 1$.*
(iii) *$\Delta(q) \equiv 1,3,5,7,8,9,11,12,13,15,17,19,20,21,23,24,25,27,28,29,31 \pmod{32}$.*

Proof. The result is an immediate consequence of Theorems 1.5 and 3.2, Proposition 2.3(a) and Corollaries 2.11 and 2.15. ∎

THEOREM 3.4. *Let $q(x,y)_{/\mathbb{Z}}$ be a nondegenerate binary quadratic form. Suppose $d \in \mathbb{Z}^+$ is such that $q(x,y) = dq'(x,y)$ with $q'(x,y)$ a primitive form. Then q is ADC if and only if all of the following hold:*

(i) *$q'(x,y)$ is ADC.*
(ii) *d is squarefree.*
(iii) *For each odd prime p dividing d, $\big(\Delta(q')/p\big) = -1$.*
(iv) *If $2 \mid d$, then either $\Delta(q') \equiv 20 \pmod{32}$ or $\Delta(q') \equiv 5 \pmod 8$.*

Proof. STEP 1. Conditions (i) and (ii) are necessary for q to be ADC by Lemma 2.1(b) and Proposition 2.3(b). Conversely, if they hold then, by Theorem 1.5, q' is regular, hence $q = aq'$ is regular, so by Theorem 1.5 again q is ADC if and only if $q_{/\mathbb{Z}_p}$ is ADC for all primes p. Under condition (ii), $q_{/\mathbb{Z}_p}$ is unit equivalent to either q' or $\pi q'$ for a uniformizing element π. In the former case $q_{/\mathbb{Z}_p}$ is ADC since q' is. Thus it is enough to check that if $q = \pi q'$ for a primitive ADC form $q'_{/\mathbb{Z}_p}$, then q is locally ADC if and only if condition (iii) holds when p is odd, and if and only if condition (iv) holds when $p = 2$.

STEP 2. Suppose p is odd. By Theorem 2.10, $q_{/\mathbb{Z}_p}$ is ADC if and only if ($\operatorname{disc} q' \in \mathbb{Z}_p^{\times 2}$ and $p \equiv 3 \pmod 4$) or ($\operatorname{disc} q' \in \mathbb{Z}_p^{\times} \setminus \mathbb{Z}_p^{\times 2}$ and $p \equiv 1 \pmod 4$). If $p \equiv 3 \pmod 4$ then $\big(\frac{-1}{p}\big) = -1$, so $\big(\frac{\Delta(q')}{p}\big) = \big(\frac{-4 \operatorname{disc} q}{p}\big) = -1$. If $p \equiv 1 \pmod 4$ then $\big(\frac{-1}{p}\big) = 1$, so again $\big(\frac{\Delta(q')}{p}\big) = \big(\frac{-4 \operatorname{disc} q'}{p}\big) = -1$.

STEP 3. Suppose $p = 2$.

CASE 1: $v_2(\Delta(q')) = 0$, so $v_2(\Delta(q)) = 2$. Then by Theorem 2.14(b)(ii), $q = 2q'$ is ADC if and only if $\Delta(q) \equiv 20 \pmod{32}$ if and only if $\Delta(q') \equiv 5 \pmod 8$.

CASE 2: $v_2(\Delta(q')) = 2$, so $v_2(\Delta(q)) = 4$. By Theorem 2.14(d), q is ADC if and only if $\Delta(q') \equiv 20 \pmod{32}$.

Case 3: $v_2(\Delta(q')) \geq 3$, so $v_2(\Delta(q)) \geq 5$. By Theorem 2.14(e), $q_{/\mathbb{Z}_2}$ is not ADC. ∎

3.3. Ternary forms

Theorem 3.5. *For $n \geq 3$, an n-ary ADC form over a Hasse domain R is primitive.*

Proof. Let $q_{/R}$ be an n-ary ADC form with $n \geq 3$. By Corollary 2.7, q is locally primitive, so by Proposition 2.3(a), q is primitive. ∎

Theorem 3.6. *There are* 103 *positive ADC ternary forms $q_{/\mathbb{Z}}$.*

Proof. Let q be a positive ternary ADC form. By Theorem 1.5, q is regular, whereas by Theorem 3.5, q is primitive. We now use the main result of [JKS97], which gives a list of 913 forms among which all primitive, positive, regular integral ternary forms must lie. For each of these forms, we check whether it is locally ADC using Theorems 2.12, 2.17 and 2.18; Theorem 2.12 implies that if a prime p does not divide $2 \operatorname{disc} q$, then q is necessarily ADC, so that for each form there are only finitely many primes to check. (For each such odd prime we do have to diagonalize q over $\mathbb{Z}_p$, and for $p = 2$ we need to either diagonalize q or put it in the normal form of Theorem 2.18, so there is some nontrivial—though routine—computation to do.) We are left with a list of 103 forms.

The [JKS97] enumeration includes regularity proofs of all but 22 of the 913 forms. The remaining 22 forms are strongly suspected to be regular but the regularity was not proved in [JKS97]. (Some, but not yet all, of these 22 forms have since been shown to be regular.) But we got lucky: none of these 22 forms is locally ADC. ∎

Remark 3.7. In contrast to the binary case (but similarly to the quaternary case and beyond), positive integral ADC ternary forms need not have class number one: eight of them have class number two.

3.4. Quaternary forms

Theorem 3.8. *There are* 6436 *positive ADC quaternary forms $q_{/\mathbb{Z}}$.*

Proof. A form q over a Hasse domain R in at least four variables is ADC if and only if it is sign-universal. Fortunately for us, the classification of sign-universal positive quaternary forms $q_{/\mathbb{Z}}$ has recently been completed by Bhargava and Hanke [BH]. ∎

3.5. Beyond quaternary forms. It seems hopeless to classify positive sign-universal forms in five or more variables. Certainly there are infinitely many such primitive forms, e.g. $x_1^2 + \cdots + x_{n-1}^2 + Dx_n^2$. More generally, any form with a sign-universal subform is obviously sign-universal, and this makes the problem difficult. However, using the following result we may verify whether a given form is ADC.

THEOREM 3.9 (Bhargava–Hanke [BH]). *A positive quadratic form $q_{/\mathbb{Z}}$ is sign-universal if and only if it $\mathbb{Z}$-represents every positive integer less than or equal to* 290.

4. From quadratic forms to lattices

4.1. Voronoi cells. Let (X, d) be a metric space, and let $\Lambda \subset X$. For $P \neq P' \in X$, put

$$H(P, P') = \{x \in X \mid d(x, P) \leq d(x, P')\}.$$

We define the *Voronoi cell*

$$V(\Lambda, P) = \bigcap_{P' \in \Lambda \setminus \{P\}} H(P, P'),$$

i.e., the locus of points which are as close to P as to any other point of Λ.

Let $q(x) = q(x_1, \ldots, x_n)$ be a positive quadratic form on $\mathbb{R}^n$. We associate with it the inner product $\langle x, y \rangle = q(x + y) - q(x) - q(y)$. Note that we are not dividing by 2 as is often done, hence $\langle x, x \rangle = 2q(x)$. This convention has the effect that if $q(x) \in \mathbb{Z}[x]$, then $\langle \mathbb{Z}^n, \mathbb{Z}^n \rangle \subset \mathbb{Z}^n$. Now

$$d(x, y) = \sqrt{\langle x - y, x - y \rangle} = \sqrt{2q(x - y)}$$

is a metric on $\mathbb{R}^n$. Since all positive bilinear forms are $\mathrm{GL}_n(\mathbb{R})$-equivalent, d differs from the standard Euclidean metric by a linear change of variables. For $P, P' \in \mathbb{R}^n$,

$$\begin{aligned} H(P, P') &= \{x \in \mathbb{R}^n \mid \langle x - P, x - P \rangle \leq \langle x - P', x - P' \rangle\} \\ &= \{x \in \mathbb{R}^n \mid 2\langle x, P' - P \rangle \leq \langle P', P' \rangle - \langle P, P \rangle\}. \end{aligned}$$

In particular each $H(P, P')$ is a convex subset, hence for any $\Lambda \subset \mathbb{R}^n$, the Voronoi cells $V(\Lambda, P)$ are convex. Now take $\Lambda \subset \mathbb{R}^n$ to be a full lattice, i.e., the $\mathbb{Z}$-span of an $\mathbb{R}$-linearly independent set $v_1, \ldots, v_n$. Let

$$\mathcal{R} = \{\alpha_1 v_1 + \cdots + \alpha_n v_n \mid \alpha_i \in [0, 1]\}$$

be the associated fundamental parallelepiped, and let d be its diameter. Then every $x \in \mathbb{R}^n$ has distance at most d from some point of Λ, and it follows that $V(\Lambda) = V(\Lambda, 0)$ is contained in the closed ball of radius d. Thus the intersection $\bigcap_{P' \in \Lambda^\bullet} H(0, P')$ can be replaced by a finite intersection: all but finitely many of the hyperplanes will be too far away for the intersection condition to be nonvacuous. A *set of Voronoi vectors* for Λ is a finite subset $S \subset \Lambda^\bullet$ such that

$$V(\Lambda) = \bigcap_{P' \in S} H(0, P').$$

This description makes it clear that the Voronoi cell $V(\Lambda)$ is a *convex polytope*; since $-\Lambda^\bullet = \Lambda^\bullet$, $V(\Lambda)$ is symmetric about the origin. Moreover, if $q \in \mathbb{Q}[x]$ and $\Lambda \subset \mathbb{Q}^n$ then all the defining hyperplanes are rational and thus $V(\Lambda)$ is a *rational polytope*: the convex hull of a finite subset of $\mathbb{Q}^n$.

For each $P \in \Lambda^\bullet$, the Voronoi cell $V(\Lambda, P)$ equals $P + V(\Lambda)$, and thus the Voronoi cells give a periodic polytopal tiling of $\mathbb{R}^d$. We define the *holes* of Λ (with respect to q) to be the vertices of $V(\Lambda, P)$, and the *deep holes* to be the holes x for which $d(0, x)$ is maximized. This maximal value is called the *covering radius* and denoted by R. The covering radius is thus the least radius r such that the ball $B(0, r)$ contains the Voronoi cell $V(\Lambda)$, hence $R \le d$.

4.2. The Euclideanity and the covering radius. From our discussion of Voronoi cells we infer the following result.

Proposition 4.1. *Let q be a positive integral quadratic form. Let*

$$E(q) = \sup_{y \in \mathbb{Q}^n} \inf_{x \in \mathbb{Z}^n} |q(x - y)|$$

be its Euclideanity. Let $\Lambda = \mathbb{Z}^n$ and endow $\mathbb{R}^n$ with the inner product

$$\langle x, y \rangle = q(x + y) - q(x) - q(y).$$

Let $V(\Lambda)$ be the Voronoi cell and R the covering radius of $(\langle\, ,\rangle, \Lambda)$.

(a) *As y ranges over all elements of $\mathbb{R}^n$, the quantity $\inf_{x \in \mathbb{Z}^n} q(x - y)$ attains a maximum value at a rational vector $y \in \mathbb{Q}^n$.*
(b) *We have $E(q) = R^2/2$.*
(c) *The form q is Euclidean if and only if $E(q) < 1$ if and only if $R < \sqrt{2}$.*

Proof. As y ranges over elements of $\mathbb{R}^n$,

$$\inf_{x \in \mathbb{Z}^n} |q(x - y)| = \inf_{x \in \mathbb{Z}^n} \frac{1}{2} \langle x - y, x - y \rangle$$

attains its maximum at a deep hole of Λ, which by the above discussion exists and lies in $\mathbb{Q}^n$. This gives part (a). Parts (b) and (c) follow. ∎

5. Euclidean binary integral quadratic forms

5.1. The covering radius of a planar lattice

Theorem 5.1. *Let $q(x, y) = ax^2 + bxy + cy^2$ be a positive real quadratic form which is* Minkowski-reduced: $0 \le b \le a \le c$. *Let $\langle x, y \rangle = q(x + y) - q(x) - q(y)$ be the associated positive bilinear form and $d(x, y) = \sqrt{2q(x - y)}$ be the associated metric.*

(a) *The covering radius of* $\mathbb{Z}^2$ *with respect to* d *is*

$$R = \sqrt{\frac{2ac(a-b+c)}{4ac-b^2}}.$$

(b) *If* $a, b, c \in \mathbb{Z}$, *then the Euclideanity of* E *is*

$$E(q) = \frac{(ac)(a-b+c)}{4ac-b^2} \geq \frac{c}{4}.$$

Proof. (a) CASE 1: $b = 0$. It is immediate that $E(q) = (a+c)/4$ (a more general case—stil immediate—was recorded as [Cl12, Ex. 2.2]). By way of comparison with the following case, we record the geometry of the situation: the vertices of the Voronoi cell for $(\mathbb{R}^n, d, \mathbb{Z}^2)$ are $\left(\frac{1}{2}, \frac{1}{2}\right)$, $\left(-\frac{1}{2}, \frac{1}{2}\right)$, $\left(-\frac{1}{2}, -\frac{1}{2}\right)$, $\left(\frac{1}{2}, -\frac{1}{2}\right)$. These are all deep holes, so the covering radius is

$$R = \sqrt{2q\left(\frac{1}{2}, \frac{1}{2}\right)} = \sqrt{\frac{a+c}{2}}.$$

(b) CASE 2: $b > 0$. For $x = (x_1, x_2)$, $y = (y_1, y_2) \in \mathbb{R}^2$, let

$$d_0(x,y) = \sqrt{(x_1-x_2)^2 + (y_1-y_2)^2}, \qquad q_0(x) = d_0^2/2,$$

$$T = \frac{2ac-ab}{\sqrt{(2a)(4ac-b^2)}}, \qquad U = \frac{2ac-b^2+ab}{\sqrt{(2a)(4ac-b^2)}},$$

$$v = (\sqrt{2a}, 0), \qquad w = \left(\frac{b}{\sqrt{2a}}, T+U\right).$$

Then the map $\Phi : (\mathbb{R}^2, d) \to (\mathbb{R}^2, d_0)$ given by

$$(x,y) \mapsto \left(\sqrt{2a}\, x + \frac{b}{\sqrt{2a}} y, (T+U)y\right)$$

is an isometry. Let

$$\Lambda = \Phi(\mathbb{Z}^2) = \mathbb{Z}v + \mathbb{Z}w.$$

Thus the covering radius of $(\mathbb{R}^2, d, \mathbb{Z}^2)$ is the same as the covering radius of $(\mathbb{R}^2, d_0, \Lambda)$, so it suffices to compute the latter. Since the ordered basis (v, w) of Λ is Minkowski-reduced, $q_0(v)$ and $q_0(w)$ are the first and second successive minima of Λ, and then it is a classical fact (elementary, but nontrivial; see [Aa, pp. 119–122] for a careful discussion) that $S = \{v, w, w-v, -v, -w, v-w\}$ is a set of Voronoi vectors in the sense of §4.1, so that the Voronoi cell

$$V(\Lambda) = \bigcap_{P' \in S} H(0, P')$$

is a hexagon, with vertices the *holes*

$$\pm\left(\sqrt{\frac{a}{2}}, T\right), \pm\left(\frac{b-a}{\sqrt{2a}}, U\right), \pm\left(-\sqrt{\frac{a}{2}}, T\right).$$

Evaluating q_0 at each of these holes we get

$$R=\sqrt{\frac{2ac(a-b+c)}{4ac-b^2}},$$

so all the holes are deep holes and R is the covering radius.

(b) By Proposition 4.1 we have

$$\begin{aligned}E(q)&=\frac{R^2}{2}=\frac{(ac)(a-b+c)}{4ac-b^2}=\frac{ac^2-abc+a^2c}{ac-b^2}\\&\geq\frac{(ac^2-b^2c/4)+(a^2c-abc)}{4ac-b^2}=\frac{c}{4}+\frac{ac(a-b)}{4ac-b^2}\geq\frac{c}{4}.\ \blacksquare\end{aligned}$$

COROLLARY 5.2.

(a) *The complete list of positive binary Euclidean integral forms is:*

$$\begin{aligned}
q_1&=x^2+xy+xy^2, & E&=1/3;\\
q_2&=x^2+y^2, & E&=1/2;\\
q_3&=x^2+xy+2y^2, & E&=4/7;\\
q_4&=2x^2+2xy+2y^2, & E&=2/3;\\
q_5&=x^2+2y^2, & E&=3/4;\\
q_6&=2x^2+xy+2y^2, & E&=4/5;\\
q_7&=x^2+xy+3y^2, & E&=9/11;\\
q_8&=2x^2+2xy+3y^2, & E&=9/10.
\end{aligned}$$

(b) *Every positive binary Eulidean quadratic form $q_{/\mathbb{Z}}$ has class number one.*

Proof. (a) Let q be a positive integral binary quadratic form. Then q is $\mathrm{GL}_2(\mathbb{Z})$-equivalent to a (unique) form $ax^2+bxy+cy^2$ with $0\leq b\leq a\leq c$ and $b^2-4ac>0$. By Proposition 4.1, E is Euclidean if and only if $E(q)<1$. By Theorem 5.1, $E(q)\geq c/4$, so if q is Euclidean we must have $1\leq c\leq 3$. This gives us a list of 16 triples (a,b,c) on which to check whether

$$\frac{(ac)(a-b+c)}{4ac-b^2}<1.$$

Doing so, we arrive at the list given in the statement of the result.

(b) Since scaling a quadratic form does not change its class number, q_4 will have class number 1 if and only if q_1 does. Let $q=Ax^2+Bxy+Cy^2$ be a primitive positive integral binary form of discriminant Δ. Then, as we recalled in Theorem 3.2 above, q has class number one if and only if it is idoneal or bi-idoneal. For q_1, q_2, q_3, q_5 and q_7, the Discriminants are -3, -4, -7, -8 and -11, and $\#C(\Delta)=1$. For q_6 and q_8 the Discriminants are -15 and -20, and $\#C(\Delta)=2$. Thus every form is idoneal. $\blacksquare$

REMARK 5.3. Observe that the Euclidean forms above are all idoneal. Moreover the class group $C(\Delta(q))$ is either trivial or has order 2, and the former holds if and only if q represents 1. These extra conditions are explained by work of Lenstra which we discuss next.

5.2. Euclidean rings and Euclidean ideal classes. For a nonsquare integer D which is 0 or 1 modulo 4, let $R_D = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right]$ be the quadratic order of discriminant D, and let $K = \mathbb{Q}(\sqrt{D})$ be its fraction field. Denote by $x \mapsto \overline{x}$ the nontrivial field automorphism of K and by $N : x \mapsto x\overline{x}$ the norm map from K to $\mathbb{Q}$. We put $|x| = |N(x)|$. Denote by $\operatorname{Pic} R_D$ the Picard group of R_D, i.e., invertible R_D ideals modulo principal ideals. Denote by $\operatorname{Pic}^+ R_D$ the narrow Picard group of R_D, i.e., invertible R_D ideals modulo principal ideals with totally positive generators.

A quadratic form is *nonnegative* if it is either positive or indefinite.

THEOREM 5.4 ([Co93, Thms. 5.2.8, 5.2.9]).

(a) *Suppose $D < 0$. Then the mappings*

$$\Phi : ax^2 + bxy + cy^2 \mapsto a\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z},$$
$$\Psi : \mathfrak{a} \mapsto \frac{|x\omega_1 - y\omega_2|}{|\mathfrak{a}|},$$

where $\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with

$$\frac{\omega_2\overline{\omega}_1 - \omega_1\overline{\omega}_2}{\sqrt{D}} > 0,$$

induce mutually inverse bijections from the set of $\mathrm{SL}_2(\mathbb{Z})$*-isomorphism classes of primitive, positive integral binary quadratic forms of Discriminant D to* $\operatorname{Pic} R_D = \operatorname{Pic}^+ R_D$.

(b) *Suppose $D > 0$. Then the mappings*

$$\Phi : ax^2 + bxy + cy^2 \mapsto \left(a\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\right)\alpha,$$

where α is any element of $K^\times$ such that $\operatorname{sign}(N(\alpha)) = \operatorname{sign}(\alpha)$, *and*

$$\Psi : \mathfrak{a} \mapsto \frac{N(x\omega_1 - y\omega_2)}{N(\mathfrak{a})},$$

where $\alpha = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with

$$\frac{\omega_2\overline{\omega}_1 - \omega_1\overline{\omega}_2}{\sqrt{D}} > 0,$$

induce mutually inverse bijections from the set of $\mathrm{SL}_2(\mathbb{Z})$*-isomorphism classes of primitive, indefinite integral binary quadratic forms of Discriminant D to* $\operatorname{Pic}^+ R_D$.

REMARK 5.5. The correspondence of Theorem 5.4 carries principal quadratic forms (those integrally representing 1) to principal fractional ideals.

COROLLARY 5.6. *Let D be a quadratic discriminant. As $\mathfrak{a}$ runs through a full set of representatives for* $\operatorname{Pic} R_D$*, every primitive, nonnegative integral binary form of discriminant D is unit equivalent to at least one form $\Psi(\mathfrak{a})$.*

Proof. The only nontrivial aspect of this is replacing the narrow Picard group by the Picard group when $D > 0$. If $\operatorname{Pic} R_D = \operatorname{Pic}^+ R_D$, there is nothing to show; otherwise $\operatorname{Pic} R_D$ is the quotient of $\operatorname{Pic}^+ R_D$ by an involution whose action on the quadratic forms side carries $ax^2 + bxy + cy^2$ to $-ax^2 + bxy - cy^2$ [F, p. 127]. Since the latter form is unit equivalent to the former one, the result follows. ∎

We can reduce the classification of Euclidean binary quadratic forms over $\mathbb{Z}$ to work of Lenstra on *Euclidean ideals.* First observe that because Euclidean forms give maximal lattices, in the above results we may restrict to *fundamental* discriminants D, so that the quadratic order R_D of discriminant D is simply the ring of integers in the quadratic field $\mathbb{Q}(\sqrt{D})$. Thus R_D is a Dedekind domain with ideal norm given by $|I| = |N(I)| = \# R_D/I$.

Let $(R, |\cdot|)$ be an ideal normed Dedekind domain with fraction field K. A nonzero fractional R-ideal $\mathfrak{a}$ is *Euclidean* if for all $v \in K$, there is $w \in \mathfrak{a}$ such that $|v - w| < |\mathfrak{a}|$. The following result is now immediate.

THEOREM 5.7. *Let D be a fundamental quadratic discriminant, and let R_D be the quadratic ring of discriminant D, with ideal norm*

$$|I| = |N(I)| = \# R_D/I.$$

(a) *For an invertible ideal $\mathfrak{a}$ of R_D, the following are equivalent:*
   (i) *The ideal $\mathfrak{a}$ is Euclidean.*
   (ii) *The integral binary quadratic form $\Psi(\mathfrak{a}) = N(x\omega_1 - y\omega_2)/N(\mathfrak{a})$ is Euclidean.*

(b) *The conditions of part* (a) *depend only on the image of $\mathfrak{a}$ in* $\operatorname{Pic} R_D$.

Using Remark 5.5 we see that Theorem 5.7 induces a bijective correspondence between Euclidean quadratic rings and principal Euclidean binary forms. This suggests attacking the classification problem on the other side of the correspondence, i.e., by classifying Euclidean quadratic rings. Our previous results specialize to give the well-known classification of Euclidean imaginary quadratic rings.

PROPOSITION 5.8.

(a) *Let Δ be a negative integer which is* 0 *or* 1 *modulo* 4*, and let q_Δ be the norm form of the quadratic order of discriminant Δ. Then:*
   (i) *If $\Delta \equiv 0 \pmod 4$, then $E(q_\Delta) = \frac{|\Delta|+4}{16}$.*
   (ii) *If $\Delta \equiv 1 \pmod 4$, then $E(q_\Delta) = \frac{(|\Delta|+1)^2}{16|\Delta|}$.*

(b) *The principal positive binary Euclidean quadratic forms $q_{/\mathbb{Z}}$ are q_1, q_2, q_3, q_5 and q_7 of Corollary* 5.2.

Proof. (a) If $\Delta \equiv 0 \pmod 4$, then the quadratic order of Discriminant Δ is $\mathbb{Z}\left[\frac{\Delta}{2}\right]$ and its norm form is $q_\Delta(x,y) = x^2 - \frac{\Delta}{4}y^2$. If $\Delta \equiv 1 \pmod 4$, then the quadratic order of Discriminant Δ is $\mathbb{Z}\left[\frac{1+\sqrt{\Delta}}{2}\right]$ and its norm form is $q_\Delta(x,y) = x^2 + xy + \left(\frac{1-\Delta}{4}\right)y^2$. These forms are positive and Minkowski-reduced, so Theorem 5.1 applies to compute their Euclideanities.

(b) This follows immediately. ∎

Of course Proposition 5.8(b) simply repeats a special case of Corollary 5.2. But the link to Euclidean *rings* explains the phenomenon that beyond simply being idoneal or bi-idoneal, for these forms $C(\Delta(q))$ is trivial.

The classification of Euclidean real quadratic rings is more difficult; it was initiated by Wantzel in 1848 and completed by Barnes and Swinnerton-Dyer in 1952 [BSD52]. We recommend [Le95] as a source for this and related results.

Theorem 5.9. *The real quadratic* (*norm-*)*Euclidean rings are precisely those of discriminant D for*

$$D \in \{5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 41, 44, 57, 73, 76\}.$$

(a) *The principal, anisotropic indefinite binary Euclidean forms $q_{/\mathbb{Z}}$ are*

$$\begin{aligned}
q_9 &= x^2 + xy - y^2, & E &= 1/4;\\
q_{10} &= x^2 + xy - 3y^2, & E &= 1/3;\\
q_{11} &= x^2 - 2y^2, & E &= 1/2;\\
q_{12} &= x^2 - 3y^2, & E &= 1/2;\\
q_{13} &= x^2 + xy - 4y^2, & E &= 1/2;\\
q_{14} &= x^2 - 7y^2, & E &= 9/14;\\
q_{15} &= x^2 + xy - 8y^2, & E &= 29/44;\\
q_{16} &= x^2 + xy - 5y^2, & E &= 5/7;\\
q_{17} &= x^2 + xy - 10y^2, & E &= 23/32;\\
q_{18} &= x^2 + xy - 18y^2, & E &= 1541/2136;\\
q_{19} &= x^2 + xy - 14y^2, & E &= 14/19;\\
q_{20} &= x^2 - 6y^2, & E &= 3/4;\\
q_{21} &= x^2 + xy - 9y^2, & E &= 3/4;\\
q_{22} &= x^2 + xy - 7y^2, & E &= 4/5;\\
q_{23} &= x^2 - 11y^2, & E &= 19/22;\\
q_{24} &= x^2 - 19y^2, & E &= 170/171.
\end{aligned}$$

(b) *The Euclidean forms which are obtained as imprimitive multiples of the forms of part* (a) *are*

$$\begin{aligned} q_{25} &= 2(x^2+xy-y^2), & E &= 1/2; \\ q_{26} &= 3(x^2+xy-y^2), & E &= 3/4; \\ q_{27} &= 2(x^2+xy-3y^2), & E &= 2/3. \end{aligned}$$

Proof. (a) See [Le95, Thm. 4.4] and [Lz].

(b) Whenever we have a primitive integral form with $E(q) \leq 1/n$ for some $n \in \mathbb{Z}^+$, since for $d \in \mathbb{Z}^+$ we have $E(dq) = dE(q)$, the forms dq with $1 \leq d < n$ are Euclidean. If $E(q) = 1/n$, then nq is Euclidean if and only if the supremum is not attained if and only if the critical set $C(q)$ is empty. As mentioned above, this is conjectured (but not yet known) never to occur for integral binary quadratic forms. Thus for the first five forms in part (a) we need to make use of Lezowski's tables [Lz], which record a finite, nonempty critical set $C(q)$ in every case. ∎

Lenstra further showed that the ring of integers R_D of a quadratic field admits at most one Euclidean ideal class, and if a nonprincipal Euclidean ideal class exists then $\# \operatorname{Pic} R_D = 2$. Using these facts he classified all Euclidean ideal classes in quadratic rings. To deal with imprimitive forms we also need to know the Euclideanities, which were computed by P. Lezowski.

THEOREM 5.10 (Lenstra [Ls79], Lezowski [Lz]). *The quadratic ring R_D admits a nonprincipal Euclidean ideal class if and only if $D \in \{-20, -15, 40, 60, 85\}$.*

The corresponding positive nonprincipal Euclidean binary forms $q_{/\mathbb{Z}}$ are

$$\begin{aligned} q_8 &= 2x^2+2xy+3y^2, & E &= 9/10; \\ q_9 &= 2x^2+xy+2y^2, & E &= 4/5. \end{aligned}$$

The corresponding indefinite nonprincipal Euclidean binary forms $q_{/\mathbb{Z}}$ are

$$\begin{aligned} q_{28} &= 2x^2-5y^2, & E &= 3/4; \\ q_{29} &= 3x^2-5y^2, & E &= 5/6; \\ q_{30} &= 3x^2-7xy-3y^2, & E &= 15/17. \end{aligned}$$

In summary:

THEOREM 5.11. *There are* 30 *anisotropic Euclidean binary forms $q_{/\mathbb{Z}}$.*

6. Positive Euclidean integral forms have class number one

6.1. The theorem. As promised in §1, we now present a proof that all positive Euclidean integral quadratic forms have class number one. Of course one proof is obtained simply by calculating the class numbers of the $69+1$ Euclidean forms listed in [Ne03], and this is what we did first. In searching for an a priori proof, the second author contacted N. Elkies and R. Borcherds. Borcherds indicated that this fell under the general methodology that Conway used in dealing with the Leech lattice, and suggested the book by W. Ebeling [Eb]. Prof. Elkies suggested that we contact D. Allcock, who was a student of Borcherds. Allcock was quite firm that the Lorentzian method was the proper path. Finally, in §4.5 of the second edition of [Eb], the second author found a detailed rendition of Conway's argument and was able to adapt it to the present circumstance. We are pleased to be able to offer this simple version of a technique which has hitherto been associated primarily with the Leech lattice and finite simple groups, and for which other possible applications have been known to only a few specialists.

THEOREM 6.1. *Every positive Euclidean form $q_{/\mathbb{Z}}$ has class number one.*

We will need a preliminary result characterizing the genus of an integral quadratic form in terms of *Lorentzian lattices*. This result is alluded to in the seminal work [CS] but not proved there, so for completeness we give a proof in §6.2. The proof of Theorem 6.1 is given in §6.3.

6.2. Lorentzian characterization of the genus. Let $q(x)$ be an integral quadratic form. We remind the reader of our convention that the associated bilinear form is $\langle x, y\rangle = q(x+y) - q(x) - q(y)$. This results in a bilinear $\mathbb{Z}$-lattice which is *even* in the sense that $\langle x, x\rangle \in 2\mathbb{Z}$ for all $x \in \mathbb{Z}^n$.

LEMMA 6.2 ([O'M, IX, 92:3, 93:14]). *Let R be a complete DVR of characteristic different from 2, and let f, g be nondegenerate quadratic forms over R. If $f \oplus \mathbb{H} \cong g \oplus \mathbb{H}$, then $f \cong g$.*

THEOREM 6.3. *Let f and g be nondegenerate integral quadratic forms. The following are equivalent:*

(i) *f and g are in the same genus.*
(ii) *$f \oplus \mathbb{H}$ and $g \oplus \mathbb{H}$ are integrally equivalent.*

Proof. (i)⇒(ii). STEP 1. We claim $f \oplus \mathbb{H}$ and $g \oplus \mathbb{H}$ lie in the same *spinor genus*. This follows quickly from the results of [C, §11.3], which the interested reader will now wish to consult for notation. Especially, the Corollary to Lemma 11.3.6 of [C] reads: "If we show $U_p \subset \theta(\Lambda_p)$ for all [prime numbers] p, then the genus of Λ consists of a single spinor genus." Identifying integral forms with their corresponding lattices, put $\Lambda = f \oplus \mathbb{H}$. By the remark immediately preceding [C, Lemma 11.3.8] we have, for all prime numbers p, $\theta(\Lambda_p) \supset \theta(\mathbb{H}_p)$. Further, by [C, Lemmas 11.3.7 and 11.3.8] , $\theta(\mathbb{H}_p) \supset U_p$. Therefore $U_p \subset \theta(\Lambda_p)$ for all p.

STEP 2. Since $(f \oplus \mathbb{H}) \otimes \mathbb{Q}$ is nondegenerate, indefinite and of dimension at least 3, by Eichler's Theorem [Ei52] its spinor genus consists of a single class.

(ii)⇒(i). Suppose $f \oplus \mathbb{H} \cong_{\mathbb{Z}} g \oplus \mathbb{H}$. Then $f \oplus \mathbb{H} \cong_{\mathbb{R}} g \oplus \mathbb{H}$, so by Witt Cancellation $f \cong_{\mathbb{R}} g$. Moreover, for any prime number p, $f \oplus \mathbb{H} \cong_{\mathbb{Z}_p} g \oplus \mathbb{H}$, so $f \cong_{\mathbb{Z}_p} g$ by Lemma 6.2. Thus $\mathfrak{g}(f) = \mathfrak{g}(g)$. ∎

Remark 6.4. The statement of Theorem 6.3 appears in [CS, p. 378]: "[M]uch of the importance of the genus ... arises from the fact that two forms f and g are in the same genus if and only if $f \oplus \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$ and $g \oplus \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$ are integrally equivalent. This follows from properties of the spinor genus." (In terms of our setup, the authors are speaking about the even bilinear lattices associated to integral quadratic forms.) But so far as we know the literature does not contain a proof. The above argument was supplied by A. Kumar at our request [K].

6.3. The proof. Let q be a positive integral Euclidean form. Let Λ be the even positive lattice corresponding to q, so Λ has covering radius less than $\sqrt{2}$. Consider the *Lorentzian lattice* $L = \Lambda \oplus U$ corresponding to the indefinite integral form $q \oplus \mathbb{H}$. We may represent elements of L as triples (λ, m, n) with $\lambda \in \Lambda$, $m, n \in \mathbb{Z}$. Denoting the induced bilinear form $(x, y) \mapsto q(x+y) - q(x) - q(y)$ on Λ simply as $x \cdot y$, the induced bilinear form on L is

$$(\lambda_1, m_1, n_1) \cdot (\lambda_2, m_2, n_2) = \lambda_1 \cdot \lambda_2 + m_1 n_2 + m_2 n_1.$$

Let $\ell \in L$ be a primitive isotropic vector. The bilinear form on L induces a well-defined bilinear form on the lattice

$$E(\ell) = \ell^{\perp}/\langle \ell \rangle.$$

We claim that $E(\ell) \otimes \mathbb{Q} \cong \Lambda \otimes \mathbb{Q}$. Indeed, since ℓ is an isotropic vector in the nondegenerate quadratic space $L \otimes \mathbb{Q}$, there is an isomorphism $\Phi : L \otimes \mathbb{Q} \to \mathbb{H} \oplus V'$ with $\Phi(\ell) = e_2$. By Witt Cancellation, $V' \cong \Lambda \otimes \mathbb{Q}$, so in particular V' is positive. We have $\ell^{\perp} = \Phi^{-1}(e_2^{\perp}) = \langle e_2 \rangle \oplus V'$ and thus

$$\ell^{\perp}/\langle \ell \rangle \cong (e_2 \oplus V')/\langle e_2 \rangle \cong V' \cong \Lambda \otimes \mathbb{Q}.$$

In particular, $E(\ell)$ is positive. Further, the $\mathbb{Z}$-isomorphism class of $E(\ell)$ depends only on the $(\operatorname{Aut} L)$-orbit of ℓ.

Suppose Λ' is a positive even lattice in the same genus as Λ. By Theorem 6.3 there is an isomorphism $\Phi : \Lambda' \oplus U \to \Lambda \oplus U$, and then $\Lambda' \cong E(\Phi(e_2))$. Thus to prove Theorem 6.1 it suffices to show that for every primitive isotropic vector $\ell \in L$, there is $\Phi \in \operatorname{Aut} L$ such that $\Phi \ell = \pm e_2 = \pm(0,0,1)$: then $\pm\Phi\ell = e_2 = (0,0,1)$ and

$$\Lambda' \cong E(\ell) \cong E(e_2) \cong \Lambda.$$

We will show this by performing a sequence of *reflections* in special root vectors of L. For $\lambda \in \Lambda$, we define

$$\tilde{\lambda} = \left(\lambda, 1, 1 - \frac{\lambda \cdot \lambda}{2}\right) \in L.$$

Then $\tilde{\lambda}$ is a *root*, i.e., $\tilde{\lambda} \cdot \tilde{\lambda} = 2$. Recall that for an anisotropic vector v in a quadratic space (V, q) over a field K of characteristic different from 2 we can build an isometry of V, *reflection through* v:

$$s_v : x \mapsto x - \left(\frac{2x \cdot v}{v \cdot v}\right) v.$$

For an anisotropic vector v in a quadratic $\mathbb{Z}$-lattice, s_v need not be integrally defined, but it is if $v \cdot v = 2$. Thus each $\lambda \in \Lambda$ yields a reflection $s_{\tilde{\lambda}}$.

Let $z = (\xi, a, b)$ be a primitive isotropic vector, so

$$-2ab = \xi^2.$$

• Since z is primitive isotropic, if one of a, b is 0, then (since Λ is anisotropic), $\xi = 0$ and the other of a, b is ± 1.

• Suppose $|b| < |a|$. Then

$$z \cdot \tilde{0} = (\xi, a, b) \cdot (0, 1, 1) = a + b,$$
$$s_{\tilde{0}}(z) = z - (z \cdot \tilde{0})\tilde{0} = (\xi, -b, -a).$$

• Therefore we may assume $|a| \leq |b|$. If $a = 0$, then as above $b = \pm 1$ so $\pm z = (0, 0, 1)$ and we are done. Hence we may assume $a \neq 0$. By replacing z with $-z$ if necessary we may assume $a > 0$. Since $b = -\xi^2/2a$ and $2a^2 \leq |2ab| = \xi^2$, we see that $(\xi/a)^2 \geq 2$. By the Euclidean condition, there is $\lambda \in \Lambda \setminus \{0\}$ with

$$(\xi/a - \lambda)^2 < 2.$$

Put

$$\begin{aligned} a' &= \frac{a}{2}(\xi/a - \lambda)^2, \\ b' &= b - (a - a')(1 - \lambda^2/2) = -\xi^2/2a - (a - a')(1 - \lambda^2/2). \end{aligned} \tag{5}$$

Then

$$z \cdot \tilde{\lambda} = (\xi, a, b) \cdot (\lambda, 1, 1 - \lambda^2/2) = a - a',$$

so $a' \in \mathbb{Z}$. Finally, put

$$z' = s_{\tilde{\lambda}}(z) = (\xi - (a - a')\lambda, a', b') = (\xi', a', b'),$$

say. If $a' = 0$, then $s_{\tilde{\lambda}}(z) = (0, 0, \pm 1)$, and we are done. So we may assume $a' \neq 0$. Then (5) gives $|a'| < |a|$ and $a' > 0$; it follows that $0 < a - a' < a$. Since $-2ab = \xi^2$, we have $b < 0$; and since

$$-2a'b' = (\xi - (a - a')\lambda)^2,$$

it follows that $b' < 0$. Since $\lambda^2 \geq 2$, we have $1 - \lambda^2/2 \leq 0$, and thus

$$(a - a')(1 - \lambda^2/2) \leq 0.$$

Since

$$b' = b - (a - a')(1 - \lambda^2/2),$$

we conclude $|b'| \leq |b|$. Therefore we find that $z = (\xi, a, b)$ lies in the same $(\mathrm{Aut}\, L)$-orbit as $z' = (\xi', a', b')$ with $|a'| + |b'| < |a| + |b|$. Continuing in this way, we eventually generate an element $z_k = (\xi_k, a_k, b_k)$ in the $(\mathrm{Aut}\, L)$-orbit of z with $a_k b_k = 0$ and thus $\pm z_k = (0, 0, 1)$. ■

6.4. The positive Euclidean integral forms reclassified. As mentioned above, in view of Theorem 6.1 we get a new proof of Theorem 1.6 by running through the Lorch–Kirschmer list of primitive, positive class number one integral quadratic forms available at

www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/index.html#Watson

and computing their Euclideanities. This was done using the MAGMA computer algebra package, which has a command for computing the covering radius of a lattice in Euclidean space, implementing an algorithm of G. Nebe. These computations take positive time (as measured by MAGMA) starting with five variables. For instance, the 67th Euclidean lattice is the E_8 root lattice, for which MAGMA took 399 seconds to compute the covering radius. (Exact formulas for covering radii of root lattices are known, but since we have to compute covering radii of many nonroot lattices as well, it was simpler not to make use of them.) Covering radii computations become prohibitively slow starting with nine variables: a direct MAGMA computation of the covering radius of the nine- and ten-dimensional class number one lattices did not terminate, so instead we took advantage of the fact that these forms are given as $q_1 \oplus q_2$ with $\dim q_i \leq 8$ and used (2) to reduce to smaller-dimensional cases. The computations took a bit under a day.

A version of the Lorch–Kirschmer list with Euclideanities is available at

www.math.uga.edu/~pete/Class.Number.One.With.Euclideanities.txt

From this list we extract the 67 primitive positive class number one Euclidean integral forms. In precisely two cases we have $E(q) < 1/2$: namely $E(x^2) = 1/4$ and $E(x^2 + xy + y^2) = 1/3$. As discussed in the proof of Theorem 5.9(b), this leads to three more Euclidean forms, $2x^2$, $3x^2$ and $2(x^2 + xy + y^2)$. The binary forms on this list are precisely those of Corollary 5.2, removing the dependence on the Generalized Riemann Hypothesis. Our list of 70 Euclidean forms coincides with the list of [Ne03] augmented with the form of Remark 1.7. The forms are recorded in Table 3 below.

6.5. Remark on the sharpness of Conjecture 2. As mentioned in the introduction to [Ne03], it is also of interest to classify integral lattices Λ in Euclidean n-space with covering radius $R = \sqrt{2}$.

This classification is not yet complete, but Nebe's method yields several lattices with covering radius $\sqrt{2}$ and class number greater than one. A more dramatic example is the *Leech lattice* Λ_L, which has covering radius $\sqrt{2}$ [CPS82], whereas a positive integral form of class number one has at most 10 variables [Wa63a]. In fact, Niemeier [Ni73] showed that there are precisely 24 even unimodular lattices of dimension 24. It follows from the Lorentzian characterization of the genus and the fact that any two indefinite unimodular lattices of the same signature and type (i.e., even or odd) are isomorphic [S, §V.2.2] that the genus of Λ_L consists of all 24 even unimodular lattices of dimension 24; thus the class number of Λ_L is 24.

Acknowledgments. Although the work of this paper has a unifying theme—integral quadratic forms—it required a diverse array of tools, some of them lying outside the union of our comfort zones. Many mathematicians generously contributed their time and expertise to help us. We are grateful to Daniel Allcock, Richard Borcherds, Wai-Kiu Chan, Noam D. Elkies, Larry Gerstein, Jonathan P. Hanke, Abhinav Kumar, Franz Lemmermeyer, Pierre Lezowski, Ted Shifrin and David Speyer for their assistance.

We thank Jacob Hicks for his substantial computational aid.

The first author was partially supported by National Science Foundation grant DMS-0701771.

Table 1. Primitive positive ADC binaries: $(A, B, C) = Ax^2 + Bxy + Cy^2$

$(1,1,1)$	$(1,0,1)$	$(1,1,2)$	$(1,0,2)$	$(1,1,3)$	$(1,0,3)$
$(1,1,4)$	$(2,1,2)$	$(1,1,5)$	$(1,0,5)$	$(2,2,3)$	$(1,0,6)$
$(2,0,3)$	$(1,1,9)$	$(3,1,3)$	$(2,1,5)$	$(1,0,10)$	$(2,0,5)$
$(1,1,11)$	$(1,1,13)$	$(3,3,5)$	$(1,0,13)$	$(2,2,7)$	$(2,1,7)$
$(3,2,5)$	$(1,1,17)$	$(3,2,6)$	$(1,0,21)$	$(2,2,11)$	$(3,0,7)$
$(5,4,5)$	$(1,0,22)$	$(2,0,11)$	$(1,1,23)$	$(5,3,5)$	$(1,1,29)$
$(5,5,7)$	$(1,0,30)$	$(2,0,15)$	$(3,0,10)$	$(5,0,6)$	$(1,1,31)$
$(3,3,11)$	$(1,0,33)$	$(2,2,17)$	$(3,0,11)$	$(6,6,7)$	$(5,2,7)$
$(1,0,37)$	$(2,2,19)$	$(3,1,13)$	$(1,1,41)$	$(1,0,42)$	$(2,0,21)$
$(3,0,14)$	$(6,0,7)$	$(5,4,10)$	$(1,1,47)$	$(7,3,7)$	$(1,1,49)$
$(3,3,17)$	$(5,5,11)$	$(7,1,7)$	$(3,1,17)$	$(5,1,11)$	$(1,0,57)$
$(2,2,29)$	$(3,0,19)$	$(6,6,11)$	$(1,0,58)$	$(2,0,29)$	$(1,1,59)$
$(5,5,13)$	$(5,1,13)$	$(3,2,22)$	$(6,2,11)$	$(5,4,14)$	$(7,4,10)$
$(1,1,67)$	$(3,3,23)$	$(5,2,14)$	$(7,2,10)$	$(1,0,70)$	$(2,0,35)$
$(5,0,14)$	$(7,0,10)$	$(5,3,15)$	$(7,4,11)$	$(3,2,26)$	$(6,2,13)$

Table 1 (cont.). Primitive positive ADC binaries: $(A, B, C) = Ax^2 + Bxy + Cy^2$

$(1,0,78)$	$(2,0,39)$	$(3,0,26)$	$(6,0,13)$	$(3,1,27)$	$(7,6,13)$
$(1,0,85)$	$(2,2,43)$	$(5,0,17)$	$(10,10,11)$	$(7,3,13)$	$(1,0,93)$
$(2,2,47)$	$(3,0,31)$	$(6,6,17)$	$(7,2,14)$	$(1,1,101)$	$(11,9,11)$
$(1,0,102)$	$(2,0,51)$	$(3,0,34)$	$(6,0,17)$	$(1,0,105)$	$(2,2,53)$
$(3,0,35)$	$(5,0,21)$	$(6,6,19)$	$(7,0,15)$	$(10,10,13)$	$(11,8,11)$
$(1,1,107)$	$(7,7,17)$	$(1,1,109)$	$(3,3,37)$	$(5,5,23)$	$(11,7,11)$
$(5,2,23)$	$(10,8,13)$	$(1,1,121)$	$(3,3,41)$	$(7,7,19)$	$(11,1,11)$
$(1,0,130)$	$(2,0,65)$	$(5,0,26)$	$(10,0,13)$	$(1,0,133)$	$(2,2,67)$
$(7,0,19)$	$(13,12,13)$	$(7,6,21)$	$(11,8,14)$	$(1,1,139)$	$(3,3,47)$
$(5,5,29)$	$(13,11,13)$	$(5,4,29)$	$(10,6,15)$	$(11,2,13)$	$(7,6,22)$
$(11,6,14)$	$(1,1,149)$	$(5,5,31)$	$(7,7,23)$	$(13,9,13)$	$(5,2,31)$
$(10,8,17)$	$(1,1,157)$	$(3,3,53)$	$(11,11,17)$	$(13,7,13)$	$(5,3,33)$
$(11,3,15)$	$(1,0,165)$	$(2,2,83)$	$(3,0,55)$	$(5,0,33)$	$(6,6,29)$
$(10,10,19)$	$(11,0,15)$	$(13,4,13)$	$(11,9,17)$	$(1,0,177)$	$(2,2,89)$
$(3,0,59)$	$(6,6,31)$	$(1,1,179)$	$(5,5,37)$	$(11,11,19)$	$(13,13,17)$
$(11,5,17)$	$(1,0,190)$	$(2,0,95)$	$(5,0,38)$	$(10,0,19)$	$(13,11,17)$
$(11,8,19)$	$(1,1,199)$	$(3,3,67)$	$(5,5,41)$	$(15,15,17)$	$(11,4,19)$
$(13,8,17)$	$(1,0,210)$	$(2,0,105)$	$(3,0,70)$	$(5,0,42)$	$(6,0,35)$
$(7,0,30)$	$(10,0,21)$	$(14,0,15)$	$(7,4,31)$	$(14,10,17)$	$(11,10,22)$
$(13,4,17)$	$(7,3,33)$	$(11,3,21)$	$(11,4,22)$	$(13,6,19)$	$(7,5,35)$
$(11,5,23)$	$(13,1,19)$	$(11,3,23)$	$(1,0,253)$	$(2,2,127)$	$(11,0,23)$
$(17,12,17)$	$(7,3,37)$	$(7,2,37)$	$(14,12,21)$	$(7,2,38)$	$(14,2,19)$
$(1,0,273)$	$(2,2,137)$	$(3,0,91)$	$(6,6,47)$	$(7,0,39)$	$(13,0,21)$
$(14,14,23)$	$(17,8,17)$	$(11,4,26)$	$(13,4,22)$	$(5,3,57)$	$(15,3,19)$
$(7,6,42)$	$(11,2,26)$	$(13,2,22)$	$(14,6,21)$	$(1,1,289)$	$(3,3,97)$
$(5,5,59)$	$(7,7,43)$	$(11,11,29)$	$(15,15,23)$	$(17,1,17)$	$(19,17,19)$
$(5,4,61)$	$(10,6,31)$	$(11,7,29)$	$(11,6,29)$	$(17,16,22)$	$(17,7,19)$
$(13,8,26)$	$(17,2,19)$	$(1,0,330)$	$(2,0,165)$	$(3,0,110)$	$(5,0,66)$
$(6,0,55)$	$(10,0,33)$	$(11,0,30)$	$(15,0,22)$	$(1,0,345)$	$(2,2,173)$
$(3,0,115)$	$(5,0,69)$	$(6,6,59)$	$(10,10,37)$	$(15,0,23)$	$(19,8,19)$
$(13,11,29)$	$(5,3,71)$	$(1,0,357)$	$(2,2,179)$	$(3,0,119)$	$(6,6,61)$
$(7,0,51)$	$(14,14,29)$	$(17,0,21)$	$(19,4,19)$	$(1,1,359)$	$(5,5,73)$
$(7,7,53)$	$(19,3,19)$	$(11,3,33)$	$(17,11,23)$	$(13,1,29)$	$(1,0,385)$
$(2,2,193)$	$(5,0,77)$	$(7,0,55)$	$(10,10,41)$	$(11,0,35)$	$(14,14,31)$
$(22,22,23)$	$(17,3,23)$	$(7,6,57)$	$(14,8,29)$	$(17,2,23)$	$(19,6,21)$
$(11,9,39)$	$(13,9,33)$	$(5,1,83)$	$(15,9,29)$	$(7,6,61)$	$(14,8,31)$
$(5,2,86)$	$(10,2,43)$	$(15,12,31)$	$(17,16,29)$	$(13,4,34)$	$(17,4,26)$
$(11,6,41)$	$(22,16,23)$	$(5,3,89)$	$(13,7,35)$	$(13,12,37)$	$(19,14,26)$

Table 1 (cont.). Primitive positive ADC binaries: $(A, B, C) = Ax^2 + Bxy + Cy^2$

$(1,0,462)$	$(2,0,231)$	$(3,0,154)$	$(6,0,77)$	$(7,0,66)$	$(11,0,42)$
$(14,0,33)$	$(21,0,22)$	$(7,4,67)$	$(13,8,37)$	$(14,10,35)$	$(21,18,26)$
$(13,9,39)$	$(17,5,29)$	$(13,6,39)$	$(23,20,26)$	$(1,1,499)$	$(3,3,167)$
$(5,5,101)$	$(7,7,73)$	$(15,15,37)$	$(19,19,31)$	$(21,21,29)$	$(23,11,23)$
$(11,2,46)$	$(22,2,23)$	$(7,3,73)$	$(19,13,29)$	$(7,2,73)$	$(13,12,42)$
$(14,12,39)$	$(21,12,26)$	$(11,1,47)$	$(19,17,31)$	$(5,1,107)$	$(15,9,37)$
$(11,9,51)$	$(17,9,33)$	$(17,10,34)$	$(19,12,31)$	$(5,4,113)$	$(10,6,57)$
$(15,6,38)$	$(19,6,30)$	$(7,4,82)$	$(14,4,41)$	$(17,10,35)$	$(21,18,31)$
$(7,4,86)$	$(14,4,43)$	$(5,2,122)$	$(10,2,61)$	$(15,12,43)$	$(23,18,30)$
$(5,3,123)$	$(15,3,41)$	$(11,4,59)$	$(17,2,38)$	$(19,2,34)$	$(22,18,33)$
$(19,16,38)$	$(23,6,29)$	$(17,11,41)$	$(23,1,29)$	$(7,1,97)$	$(21,15,35)$
$(13,1,53)$	$(17,13,43)$	$(11,10,65)$	$(13,10,55)$	$(22,12,33)$	$(26,16,29)$
$(19,10,38)$	$(23,8,31)$	$(13,10,59)$	$(26,16,31)$	$(1,1,751)$	$(3,3,251)$
$(7,7,109)$	$(11,11,71)$	$(13,13,61)$	$(21,21,41)$	$(29,19,29)$	$(31,29,31)$
$(11,4,71)$	$(13,8,61)$	$(22,18,39)$	$(26,18,33)$	$(19,18,46)$	$(23,18,38)$
$(11,8,74)$	$(17,2,47)$	$(22,8,37)$	$(31,30,33)$	$(11,6,74)$	$(13,2,62)$
$(22,6,37)$	$(26,2,31)$	$(17,15,51)$	$(19,5,43)$	$(1,1,829)$	$(3,3,277)$
$(5,5,167)$	$(13,13,67)$	$(15,15,59)$	$(17,17,53)$	$(29,7,29)$	$(31,23,31)$
$(13,5,65)$	$(23,7,37)$	$(17,6,51)$	$(19,8,46)$	$(23,8,38)$	$(31,28,34)$
$(13,2,67)$	$(19,4,46)$	$(23,4,38)$	$(26,24,39)$	$(13,9,69)$	$(23,9,39)$
$(11,8,83)$	$(17,4,53)$	$(22,14,43)$	$(33,30,34)$	$(11,10,85)$	$(17,10,55)$
$(22,12,43)$	$(31,24,34)$	$(13,1,73)$	$(17,9,57)$	$(19,9,51)$	$(29,27,39)$
$(7,6,138)$	$(14,6,69)$	$(21,6,46)$	$(23,6,42)$	$(13,6,78)$	$(17,14,62)$
$(26,6,39)$	$(31,14,34)$	$(17,5,61)$	$(29,13,37)$	$(17,6,62)$	$(23,12,47)$
$(29,24,41)$	$(31,6,34)$	$(13,2,82)$	$(23,8,47)$	$(26,2,41)$	$(31,24,39)$
$(19,3,57)$	$(23,1,47)$	$(7,2,158)$	$(14,2,79)$	$(19,8,59)$	$(35,30,38)$
$(11,2,101)$	$(19,14,61)$	$(22,20,55)$	$(33,24,38)$	$(11,6,102)$	$(17,6,66)$
$(22,6,51)$	$(33,6,34)$	$(13,6,87)$	$(26,20,47)$	$(29,6,39)$	$(31,10,37)$
$(13,3,87)$	$(19,11,61)$	$(23,19,53)$	$(29,3,39)$	$(11,10,110)$	$(22,10,55)$
$(29,4,41)$	$(33,12,37)$	$(19,3,67)$	$(31,1,41)$	$(7,3,183)$	$(17,11,77)$
$(21,3,61)$	$(35,25,41)$	$(13,12,102)$	$(17,12,78)$	$(26,12,51)$	$(34,12,39)$
$(11,7,119)$	$(17,7,77)$	$(29,27,51)$	$(33,15,41)$	$(19,6,69)$	$(23,6,57)$
$(37,34,43)$	$(38,32,41)$	$(13,10,106)$	$(23,4,59)$	$(26,10,53)$	$(39,36,43)$
$(1,0,1365)$	$(2,2,683)$	$(3,0,455)$	$(5,0,273)$	$(6,6,229)$	$(7,0,195)$
$(10,10,139)$	$(13,0,105)$	$(14,14,101)$	$(15,0,91)$	$(21,0,65)$	$(26,26,59)$
$(30,30,53)$	$(35,0,39)$	$(37,4,37)$	$(42,42,43)$	$(19,9,73)$	$(31,19,47)$
$(11,3,141)$	$(31,25,55)$	$(33,3,47)$	$(37,13,43)$	$(19,1,83)$	$(23,15,71)$
$(11,2,146)$	$(22,2,73)$	$(31,20,55)$	$(33,24,53)$	$(11,8,151)$	$(17,4,97)$

Table 1 (cont.). Primitive positive ADC binaries: $(A, B, C) = Ax^2 + Bxy + Cy^2$

$(22, 14, 77)$	$(34, 30, 55)$	$(17, 16, 101)$	$(23, 14, 74)$	$(34, 18, 51)$	$(37, 14, 46)$
$(23, 10, 74)$	$(29, 22, 62)$	$(31, 22, 58)$	$(37, 10, 46)$	$(19, 18, 94)$	$(29, 16, 61)$
$(37, 32, 53)$	$(38, 18, 47)$	$(11, 7, 161)$	$(23, 7, 77)$	$(31, 23, 61)$	$(33, 15, 55)$
$(13, 6, 138)$	$(19, 2, 94)$	$(23, 6, 78)$	$(26, 6, 69)$	$(29, 20, 65)$	$(37, 36, 57)$
$(38, 2, 47)$	$(39, 6, 46)$	$(13, 11, 143)$	$(29, 15, 65)$	$(31, 1, 59)$	$(37, 23, 53)$
$(7, 5, 265)$	$(21, 9, 89)$	$(31, 13, 61)$	$(35, 5, 53)$	$(19, 14, 101)$	$(23, 8, 82)$
$(38, 24, 53)$	$(41, 8, 46)$	$(17, 12, 113)$	$(23, 2, 82)$	$(34, 22, 59)$	$(41, 2, 46)$
$(7, 1, 277)$	$(19, 15, 105)$	$(21, 15, 95)$	$(35, 15, 57)$	$(19, 17, 109)$	$(23, 3, 87)$
$(29, 3, 69)$	$(37, 21, 57)$	$(17, 4, 118)$	$(29, 24, 74)$	$(34, 4, 59)$	$(37, 24, 58)$
$(19, 2, 106)$	$(31, 16, 67)$	$(38, 2, 53)$	$(41, 36, 57)$	$(17, 15, 129)$	$(23, 3, 93)$
$(31, 3, 69)$	$(43, 15, 51)$	$(7, 4, 307)$	$(14, 10, 155)$	$(21, 18, 106)$	$(29, 2, 74)$
$(31, 10, 70)$	$(35, 10, 62)$	$(37, 2, 58)$	$(42, 18, 53)$	$(13, 2, 167)$	$(26, 24, 89)$
$(29, 22, 79)$	$(43, 36, 58)$	$(19, 5, 115)$	$(23, 5, 95)$	$(41, 31, 59)$	$(43, 33, 57)$
$(11, 3, 201)$	$(33, 3, 67)$	$(41, 29, 59)$	$(43, 25, 55)$	$(13, 8, 173)$	$(19, 6, 118)$
$(26, 18, 89)$	$(38, 6, 59)$	$(13, 4, 178)$	$(17, 12, 138)$	$(23, 12, 102)$	$(26, 4, 89)$
$(34, 12, 69)$	$(37, 26, 67)$	$(39, 30, 65)$	$(46, 12, 51)$	$(29, 15, 87)$	$(37, 7, 67)$
$(43, 25, 61)$	$(47, 35, 59)$	$(11, 6, 249)$	$(19, 10, 145)$	$(22, 16, 127)$	$(29, 10, 95)$
$(33, 6, 83)$	$(38, 28, 77)$	$(55, 50, 61)$	$(57, 48, 58)$	$(37, 2, 74)$	$(41, 32, 73)$
$(43, 24, 67)$	$(47, 12, 59)$	$(13, 3, 213)$	$(37, 25, 79)$	$(39, 3, 71)$	$(47, 5, 59)$
$(17, 7, 173)$	$(29, 1, 101)$	$(43, 29, 73)$	$(51, 27, 61)$	$(13, 12, 237)$	$(17, 14, 182)$
$(26, 14, 119)$	$(34, 14, 91)$	$(37, 20, 85)$	$(39, 12, 79)$	$(51, 48, 71)$	$(53, 40, 65)$
$(11, 7, 301)$	$(43, 7, 77)$	$(47, 23, 73)$	$(55, 15, 61)$	$(11, 8, 326)$	$(22, 8, 163)$
$(23, 16, 158)$	$(33, 30, 115)$	$(46, 16, 79)$	$(47, 14, 77)$	$(55, 30, 69)$	$(59, 36, 66)$
$(23, 7, 161)$	$(47, 29, 83)$	$(53, 17, 71)$	$(59, 39, 69)$	$(17, 2, 218)$	$(29, 12, 129)$
$(34, 2, 109)$	$(43, 12, 87)$	$(47, 28, 83)$	$(51, 36, 79)$	$(58, 46, 73)$	$(59, 44, 71)$
$(29, 27, 149)$	$(37, 13, 113)$	$(41, 3, 101)$	$(47, 41, 97)$	$(17, 16, 257)$	$(29, 8, 149)$
$(31, 4, 139)$	$(34, 18, 129)$	$(43, 18, 102)$	$(51, 18, 86)$	$(58, 50, 85)$	$(62, 58, 83)$
$(17, 14, 287)$	$(29, 20, 170)$	$(34, 20, 145)$	$(41, 14, 119)$	$(51, 48, 106)$	$(53, 48, 102)$
$(58, 20, 85)$	$(73, 68, 82)$	$(13, 4, 373)$	$(23, 20, 215)$	$(26, 22, 191)$	$(39, 30, 130)$
$(43, 20, 115)$	$(46, 26, 109)$	$(65, 30, 78)$	$(69, 66, 86)$	$(19, 7, 259)$	$(31, 9, 159)$
$(37, 7, 133)$	$(41, 39, 129)$	$(43, 39, 123)$	$(53, 9, 93)$	$(57, 45, 95)$	$(59, 37, 89)$
$(19, 14, 266)$	$(23, 6, 218)$	$(37, 16, 137)$	$(38, 14, 133)$	$(46, 6, 109)$	$(47, 40, 115)$
$(61, 54, 94)$	$(74, 58, 79)$	$(17, 15, 465)$	$(31, 15, 255)$	$(43, 9, 183)$	$(47, 1, 167)$
$(51, 15, 155)$	$(61, 9, 129)$	$(71, 49, 119)$	$(85, 15, 93)$	$(11, 3, 771)$	$(33, 3, 257)$
$(41, 19, 209)$	$(55, 25, 157)$	$(61, 1, 139)$	$(67, 11, 127)$	$(77, 63, 123)$	$(79, 23, 109)$
$(23, 1, 443)$	$(31, 17, 331)$	$(41, 9, 249)$	$(43, 3, 237)$	$(69, 45, 155)$	$(79, 3, 129)$
$(83, 9, 123)$	$(93, 45, 115)$				

Table 2. Positive ADC ternaries:
$(A,B,C,D,E,F) = Ax^2 + Bxy + Cxz + Dy^2 + Eyz + Fz^2$

#	(A,B,C,D,E,F)	Class number	Euclideanity
1	$(1,1,1,1,1,1)$	1	1/2
2	$(1,1,0,1,0,1)$	1	7/12
3	$(1,0,0,1,0,1)$	1	3/4
4	$(1,1,1,1,1,2)$	1	3/4
5	$(1,1,0,1,0,2)$	1	5/6
6	$(1,0,1,1,1,2)$	1	2/3
7	$(1,0,1,1,0,2)$	1	23/28
8	$(1,0,0,1,0,2)$	1	1
9	$(1,1,0,1,0,3)$	1	13/12
10	$(1,0,1,1,1,3)$	1	9/10
11	$(1,1,1,2,2,2)$	1	4/5
12	$(1,0,1,1,0,3)$	2	47/44
13	$(1,0,0,1,0,3)$	1	5/4
14	$(1,1,1,2,1,2)$	1	1
15	$(1,0,0,2,2,2)$	1	11/12
16	$(1,1,0,2,1,2)$	1	47/52
17	$(1,1,1,1,1,5)$	1	3/2
18	$(1,0,1,1,0,4)$	1	79/60
19	$(1,0,0,2,1,2)$	2	21/20
20	$(1,0,0,2,0,2)$	1	5/4
21	$(1,1,1,2,2,3)$	2	71/68
22	$(1,0,1,2,2,3)$	1	1
23	$(2,2,2,2,1,2)$	1	7/8
24	$(1,0,0,1,0,5)$	1	7/4
25	$(1,1,0,2,1,3)$	1	23/20
26	$(1,0,0,2,2,3)$	1	23/20
27	$(1,1,0,2,0,3)$	2	37/28
28	$(1,0,1,2,1,3)$	1	95/84
29	$(1,0,1,2,0,3)$	1	29/22
30	$(1,0,0,1,0,6)$	1	2
31	$(1,0,0,2,0,3)$	1	3/2
32	$(1,1,1,2,2,4)$	1	31/24
33	$(2,1,1,2,-1,2)$	1	19/20
34	$(2,2,2,2,2,3)$	1	5/4
35	$(1,1,0,1,0,10)$	1	17/6

Table 2 (cont.). Positive ADC ternaries:
$(A, B, C, D, E, F) = Ax^2 + Bxy + Cxz + Dy^2 + Eyz + Fz^2$

#	(A, B, C, D, E, F)	Class number	Euclideanity
36	$(1, 1, 1, 3, 1, 3)$	1	$3/2$
37	$(1, 0, 0, 2, 0, 4)$	1	$7/4$
38	$(1, 1, 1, 2, 1, 5)$	1	$7/4$
39	$(1, 0, 0, 2, 2, 5)$	1	$59/36$
40	$(1, 0, 0, 3, 0, 3)$	1	$7/2$
41	$(1, 0, 1, 3, 3, 4)$	1	$4/3$
42	$(1, 0, 0, 2, 0, 5)$	1	2
43	$(1, 0, 1, 1, 1, 11)$	1	$121/42$
44	$(1, 0, 0, 2, 2, 6)$	1	$83/44$
45	$(2, 1, 0, 2, 0, 3)$	1	$31/20$
46	$(1, 1, 1, 3, 3, 5)$	1	$37/23$
47	$(1, 0, 0, 2, 0, 6)$	1	$9/4$
48	$(1, 1, 0, 2, 0, 7)$	1	$65/28$
49	$(1, 1, 1, 4, 3, 4)$	1	$8/5$
50	$(1, 0, 0, 3, 2, 5)$	1	$65/28$
51	$(2, 2, 0, 2, 0, 5)$	1	$23/6$
52	$(2, 2, 0, 3, 0, 3)$	1	$33/20$
53	$(1, 0, 0, 3, 3, 6)$	2	$55/28$
54	$(1, 0, 1, 2, 0, 9)$	1	$197/35$
55	$(2, 1, 1, 2, 1, 5)$	1	2
56	$(2, 0, 0, 3, 0, 3)$	1	2
57	$(1, 1, 0, 4, 0, 5)$	2	$139/60$
58	$(1, 1, 1, 5, 4, 5)$	1	$25/13$
59	$(1, 0, 0, 1, 0, 21)$	1	$23/4$
60	$(1, 1, 0, 1, 0, 30)$	1	$47/6$
61	$(2, 2, 0, 3, 2, 5)$	1	$171/92$
62	$(2, 0, 1, 3, 3, 5)$	1	$79/44$
63	$(2, 1, 1, 2, -1, 7)$	1	$11/5$
64	$(2, 2, 0, 3, 0, 5)$	1	$43/20$
65	$(2, 0, 0, 3, 2, 5)$	1	$59/28$
66	$(1, 0, 0, 3, 0, 10)$	1	$7/2$
67	$(1, 1, 0, 3, 0, 11)$	2	$157/44$
68	$(3, 0, 3, 3, 3, 5)$	1	$25/14$
69	$(1, 0, 0, 2, 2, 18)$	1	$683/140$
70	$(3, 1, 2, 3, -2, 5)$	1	$51/28$
71	$(2, 0, 0, 5, 5, 5)$	1	$13/6$
72	$(2, 0, 2, 3, 0, 7)$	1	$137/52$

Table 2 (cont.). Positive ADC ternaries:
$(A, B, C, D, E, F) = Ax^2 + Bxy + Cxz + Dy^2 + Eyz + Fz^2$

#	(A, B, C, D, E, F)	Class number	Euclideanity
73	$(2, 1, 1, 5, -3, 5)$	1	107/52
74	$(2, 2, 0, 2, 0, 15)$	1	53/12
75	$(1, 0, 0, 5, 0, 10)$	1	4
76	$(2, 0, 2, 3, 3, 11)$	1	121/39
77	$(2, 0, 0, 5, 0, 6)$	1	13/4
78	$(3, 0, 0, 3, 0, 7)$	1	13/4
79	$(3, 3, 2, 5, 1, 6)$	2	183/68
80	$(5, 4, 3, 5, -3, 5)$	1	17/8
81	$(1, 0, 0, 10, 10, 10)$	1	43/12
82	$(3, 1, 0, 3, 0, 10)$	1	53/14
83	$(1, 0, 0, 3, 0, 30)$	1	17/2
84	$(5, 5, 0, 5, 0, 6)$	1	19/6
85	$(1, 0, 0, 6, 6, 21)$	1	307/52
86	$(3, 1, 0, 3, 0, 14)$	1	67/14
87	$(3, 0, 0, 7, 0, 7)$	1	17/4
88	$(2, 0, 0, 5, 0, 15)$	1	11/2
89	$(5, 0, 0, 6, 2, 6)$	1	107/28
90	$(2, 0, 0, 6, 0, 15)$	1	23/4
91	$(2, 2, 2, 11, 1, 11)$	1	43/8
92	$(3, 0, 0, 10, 10, 10)$	1	49/12
93	$(6, 2, 0, 6, 0, 7)$	1	121/28
94	$(1, 0, 1, 13, 13, 23)$	1	529/78
95	$(1, 0, 0, 10, 0, 30)$	1	41/4
96	$(1, 0, 0, 21, 0, 21)$	1	43/4
97	$(5, 0, 0, 6, 0, 15)$	1	13/2
98	$(2, 2, 0, 7, 0, 39)$	1	605/52
99	$(1, 1, 0, 9, 0, 70)$	1	1387/70
100	$(3, 3, 3, 17, 7, 17)$	1	289/39
101	$(3, 0, 0, 10, 0, 30)$	1	43/4
102	$(2, 2, 0, 18, 0, 35)$	1	1873/140
103	$(6, 0, 6, 13, 0, 21)$	1	463/52

In the following table, we specify an integral quadratic form $q(x_1, \ldots, x_n)$ by giving a vector in $\mathbb{Z}^{(n)(n+1)/2}$, the coefficients on and below the main diagonal—in the order $a_{11},\ a_{21},\ a_{22},\ a_{31}, \ldots, a_{nn}$—of the Gram matrix M_q of q, i.e., the symmetric matrix such that if x is the column vector $(x_1, \ldots, x_n)$, then $q(x_1, \ldots, x_n) = x^T M_q x$.

Table 3. Positive Euclidean forms

Lower Gram coefficients	Euclid-eanity
$[1]$	$1/4$
$[2]$	$1/2$
$[3]$	$3/4$
$[1, 1/2, 1]$	$1/3$
$[1, 0, 1]$	$1/2$
$[1, 1/2, 2]$	$4/7$
$[2, 1, 2]$	$2/3$
$[1, 0, 2]$	$3/4$
$[2, 1/2, 2]$	$4/5$
$[1, 1/2, 3]$	$9/11$
$[2, 1, 3]$	$9/10$
$[1, 1/2, 1, -1/2, 0, 1]$	$1/2$
$[1, 1/2, 1, 0, 0, 1]$	$7/12$
$[1, 0, 1, -1/2, 1/2, 2]$	$2/3$
$[1, 1/2, 1, 1/2, 1/2, 2]$	$3/4$
$[1, 0, 1, 0, 0, 1]$	$3/4$
$[1, -1/1, 2, 1/2, -1, 2]$	$4/5$
$[1, 0, 1, 1/2, 0, 2]$	$23/28$
$[1, 1/2, 1, 0, 0, 2]$	$5/6$
$[2, -1/2, 2, -1, -1/2, 2]$	$7/8$
$[1, 0, 1, -1/2, 1/2, 3]$	$9/10$
$[1, 1/2, 2, 0, 1/2, 2]$	$47/52$
$[1, 0, 2, 0, 1, 2]$	$11/12$
$[2, 1/2, 2, 1/2, -1/2, 2]$	$19/20$
$[1, 0, 1, 0, 0, 1, 1/2, 1/2, 1/2, 1]$	$1/2$
$[1, 1/2, 1, 0, 0, 1, 1/2, 0, 1/2, 1]$	$3/5$
$[1, 1/2, 1, 0, 0, 1, 0, 0, 1/2, 1]$	$2/3$
$[1, 0, 1, 0, 1/2, 1, 0, -1/2, 0, 1]$	$3/4$
$[1, 1/2, 1, 1/2, 0, 1, 1/2, 0, 0, 2]$	$3/4$
$[1, 0, 1, 0, 0, 1, 1/2, 1/2, 1/2, 2]$	$4/5$
$[1, 1/2, 1, 1/2, 0, 2, 1/2, 1/2, 1, 2]$	$4/5$
$[1, 1/2, 1, 0, 0, 1, 1/2, 0, 1/2, 2]$	$14/17$
$[1, 0, 1, 0, 0, 1, 1/2, 0, 0, 1]$	$5/6$
$[1, 1/2, 1, 1/2, 0, 1, 0, 1/2, 0, 2]$	$11/13$
$[1, 1/2, 1, 0, 0, 1, 0, 0, 1/2, 2]$	$19/21$
$[1, 0, 1, 1/2, 1/2, 2, 1/2, 0, 1, 2]$	$10/11$
$[1, 0, 1, 0, 0, 1, 0, -1/2, -1/2, 2]$	$11/12$

Table 3 (cont.). Positive Euclidean forms

Lower Gram coefficients	Euclid-eanity
[1, 1/2, 1, 1/2, 0, 2, 0, 1/2, 1/2, 2]	13/14
[1, 1/2, 2, 0, 1, 2, 0, 1/2, 1, 2]	29/30
[1, 1/2, 1, 1/2, 1/2, 1, 1/2, 1/2, 1/2, 1, −1/2, 0, −1/2, −1/2, 1]	5/8
[1, 0, 1, 0, 0, 1, 1/2, 1/2, 0, 1, 0, 1/2, 1/2, 0, 1]	3/4
[1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1/2, 1/2, 1/2, 1]	3/4
[1, 1/2, 1, −1/2, 0, 1, 0, 0, 0, 1, −1/2, −1/2, 1/2, −1/2, 2]	33/40
[1, 1/2, 1, −1/2, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1/2, 1]	5/6
[1, 0, 1, 0, 0, 1, 1/2, 0, 0, 1, 0, 0, 1/2, 1/2, 1]	17/20
[1, 1/2, 1, 0, 0, 1, 1/2, 0, 1/2, 1, 0, 0, 0, 1/2, 2]	6/7
[1, 1/2, 1, 1/2, 1/2, 1, −1/2, 0, −1/2, 1, −1/2, −1/2, −1/2, 1/2, 2]	7/8
[1, 0, 1, 0, 0, 1, 1/2, 0, 0, 1, 0, 1/2, 0, 0, 1]	11/12
[1, 0, 1, 0, 1/2, 1, 0, 0, 0, 1, −1/2, −1/2, 0, 1/2, 2]	13/14
[1, 0, 1, 0, 0, 1, 1/2, 1/2, 0, 1, 0, 1/2, 1/2, 0, 2]	41/44
[1, 1/2, 1, 1/2, 0, 1, 0, 1/2, 0, 2, 0, 0, 1/2, 1, 2]	19/20
[1, −1/2, 1, 0, −1/2, 1, 0, 0, −1/2, 1, 0, 0, 0, −1/2, 1, 0, 0, −1/2, 0, 0, 1]	2/3
[1, 0, 1, 1/2, −1/2, 1, 0, 0, −1/2, 1, 0, 0, 0, −1/2, 1, 0, 0, 0, 0, −1/2, 1]	3/4
[1, 0, 1, 0, 0, 1, 1/2, 1/2, 1/2, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1/2, 1]	5/6
[1, −1/2, 1, 0, −1/2, 1, 0, 0, −1/2, 1, 0, 0, 0, −1/2, 1, 0, 0, 0, 0, −1/2, 1]	6/7
[1, −1/2, 1, −1/2, 1/2, 1, 1/2, 0, 0, 1, 1/2, 0, 0, 1/2, 1, −1/2, 1/2, 0, 0, −1/2, 2]	13/15
[1, 0, 1, 0, 1/2, 1, 0, 1/2, 1/2, 1, 0, 1/2, 1/2, 1/2, 1, 0, −1/2, 0, −1/2, −1/2, 1]	7/8
[1, 1/2, 1, 1/2, 1/2, 1, 1/2, 0, 0, 1, 1/2, 1/2, 0, 1/2, 1, 1/2, 0, 1/2, 0, 0, 2]	10/11
[1, 1/2, 1, 0, 0, 1, 1/2, 0, 1/2, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1/2, 1]	14/15
[1, −1/2, 1, 1/2, 0, 1, 1/2, −1/2, 1/2, 1, 0, 0, 0, 0, 1, −1/2, 1/2, −1/2, −1/2, −1/2, 2]	19/20
[1, 0, 1, 0, 1/2, 1, 0, 1/2, 0, 1, 0, −1/2, 0, −1/2, 1, 1/2, −1/2, −1/2, −1/2, 1/2, 2]	22/23
[1, −1/2, 1, 0, −1/2, 1, 0, 0, −1/2, 1, 0, 0, 0, −1/2, 1, 0, 0, 0, 0, −1/2, 1, 0, 0, 0, −1/2, 0, 0, 1]	3/4
[1, 1/2, 1, 1/2, 1/2, 1, 1/2, 1/2, 1/2, 1, −1/2, 0, −1/2, 1/2, 1, . . .]	7/8
[. . . 1/2, 1/2, 1/2, 1/2, −1/2, 1, 1/2, 1/2, 1/2, 1/2, −1/2, 1/2, 1]	
[1, −1/2, 1, 0, −1/2, 1, 0, 0, −1/2, 1, 0, 0, 0, −1/2, 1, 0, 0, −1/2, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1]	11/12
[1, 1/2, 1, 1/2, 0, 1, 1/2, 1/2, 0, 1, −1/2, −1/2, −1/2, . . .]	19/20
[. . . , −1/2, 1, −1/2, −1/2, 0, −1/2, 1/2, 1, 1/2, 0, 0, 1/2, 0, 0, 2]	
[1, 1/2, 1, 1/2, 1/2, 1, 0, 0, 0, 1, 0, 0, 0, 1/2, 1, −1/2, −1/2 . . .]	23/24
[. . . , −1/2, 0, 0, 1, −1/2, 0, −1/2, 0, 0, 1/2, 1]	
[1, 1/2, 1, 1/2, 1/2, 1, 1/2, 0, 0, 1, 1/2, 1/2, 0, 0, 1, 1/2, 1/2, 0, 0, 1/2, . . .]	1/2
[. . . 1, 1/2, 0, 1/2, 0, 0, 0, 1, 1/2, 1/2, 0, 1/2, 1/2, 1/2, 0, 1]	
[1, −1/2, 1, −1/2, 1/2, 1, −1/2, 1/2, 1/2, 1, 1/2, −1/2, 0, 0, 1, 1/2, −1/2, 0, . . .]	4/6
[. . . , −1/2, 1/2, 1, 1/2, 0, −1/2, −1/2, 0, 0, 1, −1/2, 1/2, 0, 0, −1/2, −1/2, 0, 2]	
[1, 1/2, 1, 1/2, 1/2, 1, 1/2, 0, 0, 1, 1/2, 1/2, 0, 0, 1, 1/2, 1/2, 0, 0, 1/2, 1 . . .]	3/4
[. . . 1/2, 0, 1/2, 0, 0, 0, 1, 1/2, 1/2, 0, 1/2, 1/2, 1/2, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1]	
[1, 1/2, 1, 1/2, 1/2, 1, 1/2, 0, 0, 1, 1/2, 1/2, 0, 0, 1, 1/2, 1/2, 0, 0, 1/2, 1, 1/2, 0, 1/2, 0, . . .]	5/6
[. . . 0, 0, 1, 1/2, 1/2, 0, 1/2, 1/2, 1/2, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1/2, 1]	

References

[Aa] J. M. Aarts, *Plane and Solid Geometry*, Springer, New York, 2008.

[BSD52] E. S. Barnes and H. P. F. Swinnerton-Dyer, *The inhomogeneous minima of binary quadratic forms. I*, Acta Math. 87 (1952), 259–323.

[BH] M. Bhargava and J. Hanke, *Universal quadratic forms and the 290-Theorem*, preprint.

[Br54] W. E. Briggs, *An elementary proof of a theorem about the representation of primes by quadratic forms*, Canad. J. Math. 6 (1954), 353–363.

[C] J. W. S. Cassels, *Rational Quadratic Forms*, London Math. Soc. Monogr. 13, Academic Press, London, 1978.

[CI08] W. K. Chan and M. I. Icaza, *Positive definite almost regular ternary quadratic forms over totally real number fields*, Bull. London Math. Soc. 40 (2008), 1025–1037.

[Cl12] P. L. Clark, *Euclidean quadratic forms and ADC forms I*, Acta Arith. 154 (2012), 137–159.

[ClHPT] P. L. Clark, J. Hicks, H. Parshall and K. Thompson, *GoNI: Primes represented by binary quadratic forms*, Integers 13 (2013), A37, 18 pp.

[Co93] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. 138, Springer, Berlin, 1993.

[CPS82] J. H. Conway, R. H. Parker and N. J. A. Sloane, *The covering radius of the Leech lattice*, Proc. Roy. Soc. London Ser. A 380 (1982), 261–290.

[CS] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups*, Springer, New York, 1988.

[Cx89] D. A. Cox, *Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory and Complex Multiplication*, Wiley, New York, 1989.

[Eb] W. Ebeling, *Lattices and Codes*, 3rd ed., Adv. Lectures Math., Springer Spektrum, Wiesbaden, 2013.

[Ei52] M. Eichler, *Die Ähnlichkeitsklassen indefiniter Gitter*, Math. Z. 55 (1952), 216–252.

[F] D. E. Flath, *Introduction to Number Theory*, Wiley, New York, 1989.

[Ge08] L. J. Gerstein, *Basic Quadratic Forms*, Grad. Stud. Math. 90, Amer. Math. Soc., Providence, RI, 2008.

[Ha11] J. P. Hanke, *Enumerating maximal definite quadratic forms of bounded class number over $\mathbb{Z}$ in $n \geq 3$ variables*, arXiv:1110.1876 (2011).

[JKS97] W. C. Jagy, I. Kaplansky and A. Schiemann, *There are 913 regular ternary forms*, Mathematika 44 (1997), 332–341.

[Ki14] M. Kirschmer, *One-class genera of maximal integral quadratic forms*, J. Number Theory 136 (2014), 375–393.

[Kn82] M. Kneser, *Composition of binary quadratic forms*, J. Number Theory 15 (1982), 406–413.

[K] A. Kumar, http://mathoverflow.net/questions/70666.

[L] T. Y. Lam, *Introduction to Quadratic Forms over Fields*, Grad. Stud. Math. 67. Amer. Math. Soc., Providence, RI, 2005.

[Le95] F. Lemmermeyer, *The Euclidean algorithm in algebraic number fields*, Expo. Math. 13 (1995), 385–416.

[Ls79] H. W. Lenstra, Jr., *Euclidean ideal classes*, in: Journées Arithmétiques de Luminy (Luminy, 1978), Astérisque 61 (1979), 121–131.

[Lz] P. Lezowski, online tables of Euclidean number fields, http://www.math.u-bordeaux1.fr/~plezowsk/tables/index.php.

[Lz12] P. Lezowski, *Examples of norm-Euclidean ideal classes*, Int. J. Number Theory 8 (2012), 1315–1333.

[LK13] D. Lorch and M. Kirschmer, *Single-class genera of positive integral lattices*, LMS J. Comput. Math. 16 (2013), 172–186.

[Ma] H. Matsumura, *Commutative Ring Theory*, Cambridge Univ. Press, Cambridge, 1986.

[Mi] J. M. Milne, *Class Field Theory*, http://www.jmilne.org/math/CourseNotes/CFT.pdf.

[Ne03] G. Nebe, *Even lattices with covering radius* $<\sqrt{2}$, Beiträge Algebra Geom. 44 (2003), 229–234.

[Ni73] H.-V. Niemeier, *Definite quadratische Formen der Dimension 24 und Diskriminante 1*, J. Number Theory 5 (1973), 142–178.

[O'M] O. T. O'Meara, *Introduction to Quadratic Forms*, Classics Math., Springer, Berlin, 2000.

[Pf79] H. Pfeuffer, *On a conjecture about class numbers of totally positive quadratic forms in totally real algebraic number fields*, J. Number Theory 11 (1979), 188–196.

[QUQF] List of the 6436 quaternary universal quadratic forms, http://web.kobepharma-u.ac.jp/~math/note/uqf.txt.

[S] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, New York, 1973.

[Vo07] J. Voight, *Quadratic forms that represent almost the same primes*, Math. Comp. 76 (2007), 1589–1617.

[Wa] G. L. Watson, *Integral Quadratic Forms*, Cambridge Tracts in Math. Math. Phys. 51, Cambridge Univ. Press, New York, 1960.

[Wa63a] G. L. Watson, *The class-number of a positive quadratic form*, Proc. London Math. Soc. (3) 13 (1963), 549–576.

[Wa63b] G. L. Watson, *Positive quadratic forms with small class-numbers*, Proc. London Math. Soc. (3) 13 (1963), 577–592.

[Wa63c] G. L. Watson, *One-class genera of positive quadratic forms*, J. London Math. Soc. 38 (1963), 387–392.

[Wa72] G. L. Watson, *One-class genera of positive ternary quadratic forms*, Mathematika 19 (1972), 96–104.

[Wa74a] G. L. Watson, *One-class genera of positive quadratic forms in at least five variables*, Acta Arith. 26 (1974/75), 309–327.

[Wa74b] G. L. Watson, *One-class genera of positive quaternary quadratic forms*, in: Collection of Articles Dedicated to Carl Ludwig Siegel on the Occasion of his Seventy-Fifth Birthday, V, Acta Arith. 24 (1973/74), 461–475.

[Wa75] G. L. Watson, *One-class genera of positive ternary quadratic forms. II*, Mathematika 22 (1975), 1–11.

[Wa78] G. L. Watson, *One-class genera of positive quadratic forms in nine and ten variables*, Mathematika 25 (1978), 57–67.

[Wa82] G. L. Watson, *One-class genera of positive quadratic forms in eight variables*, J. London Math. Soc. (2) 26 (1982), 227–244.

[Wa84] G. L. Watson, *One-class genera of positive quadratic forms in seven variables*, Proc. London Math. Soc. (3) 48 (1984), 175–192.

[Wa88] G. L. Watson, *One-class genera of positive quadratic forms in six variables*, unfinished draft, 1988.

[We82] H. Weber, *Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist*, Math. Ann. 20 (1882), 301–329.

Pete L. Clark
Department of Mathematics
Boyd Graduate Studies Research Center
University of Georgia
Athens, GA 30602-7403, U.S.A.
E-mail: pete@math.uga.edu

William C. Jagy
P.O. Box 2146
Berkeley, CA 94702-0146, U.S.A.
E-mail: wcjagy@gmail.com

Received on 30.11.2013
and in revised form on 18.4.2014 (7663)