Quadratic Lattices with Regularity Properties

Andrew G. Earnest
Southern Illinois University Carbondale

International Conference on the Algebraic and Arithmetic Theory of Quadratic Forms
Puerto Natales, Chile
December 16-21, 2013

Outline of the talk:

Outline of the talk:

- 1 Regular quadratic forms and lattices
    - 1.1 Definitions and basic properties
    - 1.2 Regular ternary lattices
    - 1.3 Regular quaternary lattices

Outline of the talk:

- 1 Regular quadratic forms and lattices
  - 1.1 Definitions and basic properties
  - 1.2 Regular ternary lattices
  - 1.3 Regular quaternary lattices
- 2 Strictly regular quaternary lattices
  (joint work with Ji Young Kim & Nicolas Meyer)
  - 2.1 Statement of results
  - 2.2 Successive minima
  - 2.3 Watson transformations
  - 2.4 Outline of proof of Theorem 1

Outline of the talk:

1 Regular quadratic forms and lattices
  1.1 Definitions and basic properties
  1.2 Regular ternary lattices
  1.3 Regular quaternary lattices
2 Strictly regular quaternary lattices
  (joint work with Ji Young Kim & Nicolas Meyer)
  2.1 Statement of results
  2.2 Successive minima
  2.3 Watson transformations
  2.4 Outline of proof of Theorem 1
3 (n-1)-regular lattices of rank n
  (joint work with Nicolas Meyer)
  3.1 Kitaoka's characteristic submodules
  3.2 Statement of Theorem 2

Outline of the talk:

1 Regular quadratic forms and lattices
  - 1.1 Definitions and basic properties
  - 1.2 Regular ternary lattices
  - 1.3 Regular quaternary lattices

2 Strictly regular quaternary lattices
(joint work with Ji Young Kim & Nicolas Meyer)
  - 2.1 Statement of results
  - 2.2 Successive minima
  - 2.3 Watson transformations
  - 2.4 Outline of proof of Theorem 1

3 (n-1)-regular lattices of rank *n*
(joint work with Nicolas Meyer)
  - 3.1 Kitaoka's characteristic submodules
  - 3.2 Statement of Theorem 2

4 Some open questions

1 Regular quadratic forms and lattices

1.1 Definitions and basic properties

Definition: [L.E. Dickson, *Ann. of Math.*, 1927] A positive definite integral quadratic form f in n variables is said to be regular if for positive integers a the equation

$$f(x_1, \ldots, x_n) = a$$

is solvable in integers $x_1, \ldots, x_n$ whenever it is true that for every positive integer m the congruence

$$f(x_1, \ldots, x_n) \equiv a \pmod{m}$$

is solvable in integers $x_1, \ldots, x_n$.

Lattice formulation:

Let L be a $\mathbb{Z}$-lattice on a positive definite rational quadratic space (V, Q). For a prime p, let L_p denote the local completion of L at p, and let $\mathrm{gen}(L)$ be the genus of L.

Lattice formulation:

Let L be a $\mathbb{Z}$-lattice on a positive definite rational quadratic space (V, Q). For a prime p, let L_p denote the local completion of L at p, and let $\mathrm{gen}(L)$ be the genus of L.

For a positive integer a, write $a \longrightarrow L$ or $a \in Q(L)$ if there exists $v \in L$ such that $Q(v) = a$, and $a \longrightarrow L_p$ if there exists $v \in L_p$ such that $Q(v) = a$. If S is a set of positive integers, then $S \longrightarrow L$ or $S \subseteq Q(L)$ will mean $a \longrightarrow L$ for all $a \in S$. Write $a \longrightarrow \mathrm{gen}(L)$ if there exists $L' \in \mathrm{gen}(L)$ such that $a \longrightarrow L'$.

Lattice formulation:

Let L be a $\mathbb{Z}$-lattice on a positive definite rational quadratic space (V, Q). For a prime p, let L_p denote the local completion of L at p, and let $\text{gen}(L)$ be the genus of L.

For a positive integer a, write $a \longrightarrow L$ or $a \in Q(L)$ if there exists $v \in L$ such that $Q(v) = a$, and $a \longrightarrow L_p$ if there exists $v \in L_p$ such that $Q(v) = a$. If S is a set of positive integers, then $S \longrightarrow L$ or $S \subseteq Q(L)$ will mean $a \longrightarrow L$ for all $a \in S$. Write $a \longrightarrow \text{gen}(L)$ if there exists $L' \in \text{gen}(L)$ such that $a \longrightarrow L'$.

Definition: The lattice L is regular if, for positive integers a, $a \longrightarrow L$ whenever $a \longrightarrow L_p$ for all p.

Equivalently: The lattice L is regular if, for positive integers a, $a \longrightarrow L$ whenever $a \longrightarrow \text{gen}(L)$.

A few observations:

- The regular lattices are those for which a local-global principle holds for the representation of integers.
- Every universal lattice is regular.
- Every lattice having class number 1 is regular.
- Regularity is preserved by scaling.
- If a lattice is regular or universal, then so is any lattice in its isometry class. So in counting regular or universal lattices, the count will always refer to the number of isometry classes of primitive lattices with the stated property.

1.2 Regular ternary quadratic forms and lattices

B.W. Jones thesis (1928): There exist 102 diagonal regular ternary quadratic forms.

G.L. Watson thesis (1953): There exist only finitely many regular ternary quadratic forms.

G.L. Watson (1954): Asymptotic growth of the exceptional set with the discriminant.

Jagy, Kaplansky & Schiemann (1997): There are at most 913 regular ternary quadratic forms, of which 119 have class number exceeding 1. (Regularity has not yet been proven for 14 of these forms - see B.-K. Oh, *Acta Arith.*, 2011, and R. Lemke Oliver, preprint, 2013)

1.3 Regular quaternary quadratic forms and lattices

Ramanujan (1917): There exist 54 diagonal universal quaternary quadratic forms.

Bhargava & Hanke (290-Theorem): There exist 6436 universal quaternary lattices.

1.3 Regular quaternary quadratic forms and lattices

Ramanujan (1917): There exist 54 diagonal universal quaternary quadratic forms.

Bhargava & Hanke (290-Theorem): There exist 6436 universal quaternary lattices.

E (1995): There exist infinitely many (nonisometric) regular quaternary lattices.

B.M. Kim (unpublished) has determined all regular diagonal quaternary lattices. The list of these lattices consists of 106 individual lattices and 180 infinite families.

2 Strictly regular quaternary lattices

2.1 Statement of results

2 Strictly regular quaternary lattices

2.1 Statement of results

Definitions: A vector $v \in L$ is primitive in L, denoted $v \overset{*}{\in} L$, if $\{v\}$ can be extended to a basis for L. A positive integer a is primitively represented by L, denoted $a \xrightarrow{*} L$ or $a \in Q^*(L)$, if there exists $v \overset{*}{\in} L$ such that $Q(v) = a$.

2 Strictly regular quaternary lattices

2.1 Statement of results

Definitions: A vector $v \in L$ is primitive in L, denoted $v \overset{*}{\in} L$, if $\{v\}$ can be extended to a basis for L. A positive integer a is primitively represented by L, denoted $a \xrightarrow{*} L$ or $a \in Q^*(L)$, if there exists $v \overset{*}{\in} L$ such that $Q(v) = a$.

Definition: A lattice L is strictly regular if, for positive integers a, $a \xrightarrow{*} L$ whenever $a \xrightarrow{*} L_p$ for all p. (Terminology due to Watson (1976))

Remark: If L is strictly regular, then L is regular.

Theorem 1: *There exist only finitely many strictly regular primitive quaternary lattices.*

Theorem 1: *There exist only finitely many strictly regular primitive quaternary lattices.*

Proposition: *There exist 96 strictly regular diagonal primitive quaternary lattices. Among these lattices, there are 27 strictly universal lattices and 34 lattices of class number 1.*

Theorem 1: *There exist only finitely many strictly regular primitive quaternary lattices.*

Proposition: *There exist 96 strictly regular diagonal primitive quaternary lattices. Among these lattices, there are 27 strictly universal lattices and 34 lattices of class number 1.*

2.2 Successive Minima

For a lattice L of rank n, let $\mu_i(L)$ denote the ith successive minimum of L, for $1 \leq i \leq n$. Then there exists a linearly independent set of vectors $\{v_1, \ldots, v_n\}$ such that $Q(v_i) = \mu_i(L)$ for $1 \leq i \leq n$, and

$$dL \leq \prod_{i=1}^{n} \mu_i(L).$$

It can be proved using character sum estimates that there exists a constant C such that $\mu_i(L) \leq C$ for $1 \leq i \leq 3$ for all regular lattices of rank at least 4.

It can be proved using character sum estimates that there exists a constant C such that $\mu_i(L) \leq C$ for $1 \leq i \leq 3$ for all regular lattices of rank at least 4.

When $n = 4$, we will refer to the primitive sublattice of L generated by $\{v_1, v_2, v_3\}$ as a "leading ternary sublattice " of L. If T is a leading ternary sublattice of the quaternary lattice L then:

- $\mu_i(T) = \mu_i(L)$ for $1 \leq i \leq 3$;
- for $v \in T$, $v \overset{*}{\in} T$ if and only if $v \overset{*}{\in} L$;
- if $v \in L \setminus T$, then $\mu_4(L) \leq Q(v)$.

2.3 Watson transformations

Let L be a positive definite quadratic $\mathbb{Z}$-lattice with $\mathfrak{s}L \subseteq \mathbb{Z}$. We will say that L is primitive if $\mathfrak{s}L = \mathbb{Z}$; L is even if $\mathfrak{n}L \subseteq 2\mathbb{Z}$, and odd otherwise. For a primitive lattice L and positive integer m, define the sublattice

$$\Lambda_m(L) = \{x \in L : Q(x+y) - Q(y) \in m\mathbb{Z} \text{ for all } y \in L\}.$$

For an odd prime p, define $\delta_p(L)$ to be the primitive lattice obtained from $\Lambda_p(L)$ upon scaling by a suitable power of p. For an odd (even, resp.) lattice L, define $\delta_2(L)$ to be the primitive lattice obtained from $\Lambda_2(L)$ ($\Lambda_4(L)$, resp.) upon scaling by a suitable power of 2. [J. Bochnak & B.-K. Oh, *Ann. Inst. Fourier, Grenoble*, 2008]

Lemma: *Let L be a strictly regular primitive quaternary lattice and let p be a prime.*

- *i) If $2\mathbb{Z}_p \not\subseteq Q(L_p)$, then $\delta_p(L)$ is strictly regular;*
- *ii) There exists a nonnegative integer k such that $\delta_p^k(L)$ is strictly regular and $2\mathbb{Z}_p \to \delta_p^k(L)$.*

Lemma: *Let L be a strictly regular primitive quaternary lattice and let p be a prime.*

- *i) If $2\mathbb{Z}_p \not\subseteq Q(L_p)$, then $\delta_p(L)$ is strictly regular;*
- *ii) There exists a nonnegative integer k such that $\delta_p^k(L)$ is strictly regular and $2\mathbb{Z}_p \to \delta_p^k(L)$.*

2.4 Outline of proof of Theorem 1

Suppose on the contrary that there exists an infinite family $\mathcal{R}$ of non-isometric strictly regular primitive quaternary lattices. Since the lattices in $\mathcal{R}$ are regular, the prime divisors of the discriminants of the lattices in $\mathcal{R}$ lie in a fixed finite set [Bochnak & Oh]. So there exists some prime q such that the powers of q dividing the discriminants of lattices in $\mathcal{R}$ are unbounded.

For $L \in \mathcal{R}$ and a prime $p \neq q$, there exists a nonnegative integer k such that the lattice $\delta_p^k(L)$ satisfies the properties

- $\delta_p^k(L)$ is strictly regular;
- $2\mathbb{Z}_p \to \delta_p^k(L)_p$;
- dL and $d(\delta_p^k(L))$ are divisible by the same powers of q.

For $L \in \mathcal{R}$ and a prime $p \neq q$, there exists a nonnegative integer k such that the lattice $\delta_p^k(L)$ satisfies the properties

- $\delta_p^k(L)$ is strictly regular;
- $2\mathbb{Z}_p \to \delta_p^k(L)_p$;
- dL and $d(\delta_p^k(L))$ are divisible by the same powers of q.

So without loss of generality we may assume that for all primes $p \neq q$, $2\mathbb{Z}_p \to L_p$ for all $L \in \mathcal{R}$.

For $L \in \mathcal{R}$ and a prime $p \neq q$, there exists a nonnegative integer k such that the lattice $\delta_p^k(L)$ satisfies the properties

- $\delta_p^k(L)$ is strictly regular;
- $2\mathbb{Z}_p \to \delta_p^k(L)_p$;
- dL and $d(\delta_p^k(L))$ are divisible by the same powers of q.

So without loss of generality we may assume that for all primes $p \neq q$, $2\mathbb{Z}_p \to L_p$ for all $L \in \mathcal{R}$.

For all lattices $L \in \mathcal{R}$, L is regular and so $\mu_i(L)$ is bounded $i = 1, 2, 3$. Consequently only finitely many ternary lattices can occur among the leading ternary sublattices of the lattices in $\mathcal{R}$. So there exists a ternary lattice T which occurs as a leading ternary sublattice of infinitely many lattices in $\mathcal{R}$. Let $W = \mathbb{Q}T$.

So there exists an infinite subfamily $\mathcal{F} \subseteq \mathcal{R}$ such that i) T is isometric to a leading ternary sublattice of L for all $L \in \mathcal{F}$, and ii) the powers of q dividing the discriminants of lattices in $\mathcal{F}$ are unbounded.

So there exists an infinite subfamily $\mathcal{F} \subseteq \mathcal{R}$ such that i) T is isometric to a leading ternary sublattice of L for all $L \in \mathcal{F}$, and ii) the powers of q dividing the discriminants of lattices in $\mathcal{F}$ are unbounded.

Claim: W_q is anisotropic.

So there exists an infinite subfamily $\mathcal{F} \subseteq \mathcal{R}$ such that i) T is isometric to a leading ternary sublattice of L for all $L \in \mathcal{F}$, and ii) the powers of q dividing the discriminants of lattices in $\mathcal{F}$ are unbounded.

Claim: W_q is anisotropic.

On the contrary, suppose that W_q is isotropic. Then there exists some $t \in \mathbb{N}$ such that $q^{2t}\mathbb{Z}_q \longrightarrow T_q$. By a computation of Hasse symbols, there exists a prime q' such that $W_{q'}$ is anisotropic. Then there exists an even positive integer b such that $b(\mathbb{Q}_{q'}^{\times})^2 \cap Q(W_{q'}) = \emptyset$. For any $L \in \mathcal{F}$, $q^{2t}b \longrightarrow L_p$ for all p; since L is regular, it follows that $q^{2t}b \longrightarrow L$. But $q^{2t}b \not\longrightarrow T$, and it would follow that $\mu_4(L) \leq q^{2t}b$ for all $L \in \mathcal{F}$, leading to a contradiction since the powers of q dividing the discriminants of the lattices in L are unbounded.

Lemma: There exists $\ell = \ell(T, q) \in \mathbb{N}$ such that $Q^*(T_q) \cap q^\ell \mathbb{Z}_q = \emptyset$.

The proof of the lemma follows by considering various possibilities for a Jordan splitting of T_q and using the Local Square Theorem.

Lemma: There exists $\ell = \ell(T, q) \in \mathbb{N}$ such that $Q^*(T_q) \cap q^\ell \mathbb{Z}_q = \emptyset$.

The proof of the lemma follows by considering various possibilities for a Jordan splitting of T_q and using the Local Square Theorem.

Completion of proof of Theorem 1:

Let $v \overset{*}{\in} T$ be such that $q \nmid Q(v)$ and denote $Q(v) = a$. Let $k \in \mathbb{N}$ be such that $2k \geq \ell$.

Lemma: There exists $\ell = \ell(T, q) \in \mathbb{N}$ such that $Q^*(T_q) \cap q^\ell \mathbb{Z}_q = \emptyset$.

The proof of the lemma follows by considering various possibilities for a Jordan splitting of T_q and using the Local Square Theorem.

Completion of proof of Theorem 1:

Let $v \overset{*}{\in} T$ be such that $q \nmid Q(v)$ and denote $Q(v) = a$. Let $k \in \mathbb{N}$ be such that $2k \geq \ell$.

If $L \in \mathcal{F}$ and $\mathrm{ord}_q dL$ is sufficiently large relative to k and $\mathrm{ord}_q dT$, it can be shown that L_q has a Jordan splitting in a basis $\{x_1, \ldots, x_4\}$ in which

$$\mathrm{ord}_q Q(x_4) \geq 2k + 3 \quad \text{and} \quad B(x_i, x_4) = 0 \text{ for } i = 1, 2, 3.$$

Write $v = \sum_{i=1}^{4} a_i x_i$ with $a_i \in \mathbb{Z}_q$ and consider $v' = v - a_4 x_4 \in L_q$. Then

$$Q(v') \equiv a \pmod{q^{2k+3}\mathbb{Z}_q}$$

and it follows that there exists $\xi \in \mathbb{Z}_q^\times$ such that

$$a = \xi^2 Q(v') = Q(\xi v').$$

Let $w = q^k \xi v' + x_4 \overset{*}{\in} L_q$. Then

$$Q(w) \equiv q^{2k} a \pmod{q^{2k+3}\mathbb{Z}_q}$$

and so there exists $\lambda \in \mathbb{Z}_q^\times$ such that

$$q^{2k} a = \lambda^2 Q(w) = Q(\lambda w).$$

Hence, $q^{2k} a \xrightarrow{*} L_q$.

Also, $q^k v \overset{*}{\in} L_p$ for all $p \neq q$. Hence, $q^{2k} a \xrightarrow{*} L_p$ for all p.

Since L is strictly regular, it follows that $q^{2k} a \xrightarrow{*} L$. But $q^{2k} a \overset{*}{\not\rightarrow} T$, since $2k \geq \ell$. It would then follow that

$$\mu_4(L) \leq q^{2k} a, \text{ for all } L \in \mathcal{F},$$

which is impossible since the discriminants of the lattices in $\mathcal{F}$ are unbounded. This completes the proof of Theorem 1.

3 (n-1)-regular lattices of rank n

3.1 Kitaoka's characteristic submodules

3 (n-1)-regular lattices of rank n

3.1 Kitaoka's characteristic submodules

Theorem: [Kitaoka, *Nagoya Math. J.*, 1978] *Let L be a lattice of rank n in a nondegenerate quadratic space over* $\mathbb{Q}$*; then L has a submodule M of rank (n-1) and* $dM \neq 0$ *which is a direct summand of L as a module and satisfies the following condition:*

Let L' *be a lattice in some nondegenerate quadratic space* U' *over* $\mathbb{Q}$ *with* $dL' = dL$*,* $\operatorname{rank} L' = n$ *and* $t_p(L') \geq t_p(L)$ *for all primes p; if* $M \to L'$*, then* $L' \cong L$*.*

3 (n-1)-regular lattices of rank n

3.1 Kitaoka's characteristic submodules

Theorem: [Kitaoka, *Nagoya Math. J.*, 1978] *Let L be a lattice of rank n in a nondegenerate quadratic space over $\mathbb{Q}$; then L has a submodule M of rank (n-1) and $dM \neq 0$ which is a direct summand of L as a module and satisfies the following condition:*

Let L' be a lattice in some nondegenerate quadratic space U' over $\mathbb{Q}$ with $dL' = dL$, $\operatorname{rank} L' = n$ and $t_p(L') \geq t_p(L)$ for all primes p; if $M \to L'$, then $L' \cong L$.

Definition: Let L be a lattice of rank n and let $k \leq n$ be a positive integer. The lattice L is k-regular if for lattices K of rank k, $K \to L$ whenever $K \to \operatorname{gen}(L)$.

Corollary: *If L is an $(n\text{-}1)$-regular lattice of rank n, then the class number of L is one.*

Corollary: *If L is an (n-1)-regular lattice of rank n, then the class number of L is one.*

3.2 Statement of Theorem 2

Corollary: *If L is an (n-1)-regular lattice of rank n, then the class number of L is one.*

3.2 Statement of Theorem 2

The definition of k-regularity can be carried over verbatim to the case of an $\mathfrak{o}$-lattice on a totally definite quadratic space over a totally real algebraic number field F, where $\mathfrak{o}$ is the ring of integers of F.

Corollary: *If L is an (n-1)-regular lattice of rank n, then the class number of L is one.*

3.2 Statement of Theorem 2

The definition of k-regularity can be carried over verbatim to the case of an $\mathfrak{o}$-lattice on a totally definite quadratic space over a totally real algebraic number field F, where $\mathfrak{o}$ is the ring of integers of F.

Theorem 2: *If L is an (n-1)-regular definite lattice of rank* $n \geq 2$ *over the ring of integers of any totally real number field, then the class number of L is one.*

Note: The case $n = 2$ in this theorem is a consequence of a result in Chan & Icaza, *Bull. London Math. Soc.*, 2008.

4 Some further questions

4 Some further questions

- Does the result of Theorem 1 generalize to definite quaternary lattices over the rings of integers of totally real number fields? (The finiteness result for regular ternary lattices is generalized to this context in Chan & Icaza, *Bull. London Math. Soc.*, 2008.)

4 Some further questions

- Does the result of Theorem 1 generalize to definite quaternary lattices over the rings of integers of totally real number fields? (The finiteness result for regular ternary lattices is generalized to this context in Chan & Icaza, *Bull. London Math. Soc.*, 2008.)

- Are there other positive integers k and n for which there exist infinitely many k-regular lattices of rank n, but only finitely many that are strictly k-regular? (A next interesting case to investigate seems to be the case of strictly 2-regular lattices of rank 6.)

4 Some further questions

- Does the result of Theorem 1 generalize to definite quaternary lattices over the rings of integers of totally real number fields? (The finiteness result for regular ternary lattices is generalized to this context in Chan & Icaza, *Bull. London Math. Soc.*, 2008.)
- Are there other positive integers k and n for which there exist infinitely many k-regular lattices of rank n, but only finitely many that are strictly k-regular? (A next interesting case to investigate seems to be the case of strictly 2-regular lattices of rank 6.)
- Do there exist any (n-2)-regular lattices of rank n with class number exceeding one, for any $n \geq 4$?

Thank You!!