TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 345, Number 2, October 1994

THE REPRESENTATION OF BINARY QUADRATIC FORMS BY POSITIVE DEFINITE QUATERNARY QUADRATIC FORMS

A. G. EARNEST

ABSTRACT. A quadratic $\mathbb{Z}$-lattice L of rank n is defined to be k-regular for a positive integer $k \leq n$ if L globally represents all quadratic $\mathbb{Z}$-lattices of rank k which are represented everywhere locally by L. It is shown that there exist only finitely many isometry classes of primitive positive definite quadratic $\mathbb{Z}$-lattices of rank 4 which are 2-regular.

1. INTRODUCTION

A necessary condition for the representation of a positive integer a by a positive definite integral quadratic form $f(x_1, \ldots, x_n)$ (i.e., the existence of $\mathbf{x} \in \mathbb{Z}^n$ such that $f(\mathbf{x}) = a$) is that a be locally represented by f at all p-adic completions (i.e., for each prime p, there exists $\mathbf{x}_p \in \mathbb{Z}_p$ such that $f(\mathbf{x}_p) = a$). Forms for which these local conditions are also sufficient to guarantee global representation were first systematically studied by Dickson [3], who referred to such forms as "regular". For example, forms for which the genus and equivalence class coincide (i.e., forms of class number 1) have this regularity property. Primitive positive definite forms of class number 1 are known to occur in only finitely many equivalence classes, regardless of rank [6]. A similar finiteness result for ternary regular forms follows from a fundamental theorem of Watson [10], who considered the number $E(f)$ of positive integers which are represented everywhere locally, but not globally, by a primitive positive definite ternary form f, and proved that $E(f)$ is asymptotically bounded from below by a power of the discriminant of f. In particular, from this it follows that primitive positive definite ternary regular forms, being those for which $E(f) = 0$, have bounded discriminant and thus occur in only finitely many equivalence classes. In contrast, for any fixed rank $n \geq 4$, it can be shown that there exist infinitely many inequivalent primitive positive definite regular forms. For example, since the form $x_1^2 + x_2^2 + x_3^2 + x_4^2$ is universal, any form which represents this particular form is regular. There is a considerable body of literature devoted to the problem of finding positive definite ternary regular forms (see [4] and the references given there for results of this type).

In this paper, we initiate the study of higher-dimensional analogues of Dickson's regularity condition. The geometric language of quadratic spaces and lat-

Received by the editors September 14, 1993 and, in revised form, February 23, 1994.
1991 *Mathematics Subject Classification.* Primary 11E12, 11E20.
Research partially supported by NSA grants MDA 904-90-H-1016 and MDA 904-92-H-3051.

0002-9947/94 $1.00 + $.25 per page

tices will be adopted throughout the paper, and notation and terminology will follow that of O'Meara's book [8]. The aim of this work is to study the lattices represented by a given $\mathbb{Z}$-lattice L on a positive definite rational quadratic space V. The dimension n of V will initially be arbitrary, but will be specialized to $n = 4$ in §4. A $\mathbb{Z}$-lattice K on a rational quadratic space W is said to be represented by L, denoted $K \rightarrow L$, if there exists an isometry $\sigma : W \rightarrow V$ such that $\sigma(K) \subseteq L$. In the local setting, representation $K_p \rightarrow L_p$ is defined analogously for the p-adic completions of K and L.

Definition 1.1. Let L be a quadratic $\mathbb{Z}$-lattice of rank n, and k a positive integer not exceeding n. Then L will be said to be *k-regular* if L represents all quadratic $\mathbb{Z}$-lattices K of rank k for which $K_p \rightarrow L_p$ for all prime spots p on $\mathbb{Q}$.

Proposition 1.2. *If L is a k-regular lattice, then L is m-regular for all positive integers $m \leq k$.*

Proof. Let M be a $\mathbb{Z}$-lattice of rank m for which $M_p \rightarrow L_p$ holds for all prime spots p on $\mathbb{Q}$. Then there exists L' in the genus of L such that $M \rightarrow L'$ [8, 102:5]. Let $\Sigma \in J_V$ be such that $L' = \Sigma L$, and let K be a sublattice of L' of rank k which contains M. Then for each p, $\Sigma_p^{-1} K_p \subseteq \Sigma_p^{-1} L'_p = L_p$. Thus, $K_p \rightarrow L_p$ holds for all p, and then $K \rightarrow L$ follows from the assumption of k-regularity. So $M \rightarrow L$. □

The main goal of this paper is to prove the finiteness of the number of isometry classes of primitive 2-regular positive definite quaternary $\mathbb{Z}$-lattices (Theorem 4.3). This theorem will be proved by analyzing the successive minima of 2-regular lattices. It will be shown that the 2-regularity condition leads to inequalities of the type $\mu_j \leq C_j D^{\alpha_j}$, where μ_j is the jth successive minimum of the 2-regular lattice L, D is the discriminant of L, C_j is a constant, and $0 < (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) < 1$. Thus $\mu_1\mu_2\mu_3\mu_4 \leq CD^{\beta}$, where C is a constant and $0 < \beta < 1$. But this inequality can be consistent with the elementary inequality $D \leq \mu_1\mu_2\mu_3\mu_4$ for at most finitely many values of D. Hence, primitive 2-regular positive definite quaternary lattices must have bounded discriminant, and the desired finiteness follows.

We note that in the proof outlined in the preceding paragraph the estimates for μ_1, μ_2 and μ_3 are established by using only the 1-regularity of the lattice. Hence, similar estimates can be obtained in a completely analogous way for 1-regular ternary lattices, leading to an alternate proof of the finiteness in the ternary case. The stronger assumption of 2-regularity is required only to obtain a suitable bound for μ_4.

2. Successive minima

Let L be a $\mathbb{Z}$-lattice on the positive definite rational quadratic space (V, Q) of dimension n. We will assume that L is integral, in the sense that $B(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}$ for all $\mathbf{x}, \mathbf{y} \in L$, where B is the symmetric bilinear form on V defined by $B(\mathbf{x}, \mathbf{y}) = \frac{1}{2}[Q(\mathbf{x}+\mathbf{y}) - Q(\mathbf{x}) - Q(\mathbf{y})]$. The next definition and lemma are adapted from [2, Chapter 12].

Definition 2.1. For $1 \leq j \leq n$, the *jth minimum of L* is that positive integer μ_j such that

(i) $\dim(\text{span}\{\mathbf{x} \in L : Q(\mathbf{x}) \leq \mu_j\}) \geq j$ and
(ii) $\dim(\text{span}\{\mathbf{x} \in L : Q(\mathbf{x}) < \mu_j\}) < j$.

The values $\mu_1, \ldots, \mu_n$ will be collectively referred to as the "successive minima" of L. The existence of linearly independent vectors $\mathbf{m}_1, \ldots, \mathbf{m}_n \in L$ with $Q(\mathbf{m}_j) = \mu_j$ can be established by induction on the dimension, using the following lemma.

Lemma 2.2. *For some $j \in \{2, \ldots, n\}$, suppose there exist linearly independent vectors $\mathbf{m}_1, \ldots, \mathbf{m}_{j-1} \in L$ such that $Q(\mathbf{m}_i) = \mu_i$ for $i = 1, \ldots, j-1$. If $\mathbf{c} \in L$ satisfies the inequality $Q(\mathbf{c}) < \mu_j$, then $\mathbf{c} \in \text{span}\{\mathbf{m}_1, \ldots, \mathbf{m}_{j-1}\}$.*

Proof. Let l be the smallest subscript such that $Q(\mathbf{c}) < \mu_l$ (so $2 \leq l \leq j$ and $\mu_{l-1} \leq Q(\mathbf{c}) < \mu_l$). If $\mathbf{c} \notin \text{span}\{\mathbf{m}_1, \ldots, \mathbf{m}_{j-1}\}$ then $\mathbf{c} \notin \text{span}\{\mathbf{m}_1, \ldots, \mathbf{m}_{l-1}\}$, and it follows that $\dim(\text{span}\{\mathbf{m}_1, \ldots, \mathbf{m}_{l-1}, \mathbf{c}\}) = l$. But then

$$\dim(\text{span}\{\mathbf{x} \in L : Q(\mathbf{x}) \leq Q(\mathbf{c})\}) \geq l$$

and it follows that $Q(\mathbf{c}) \geq \mu_l$, a contradiction. □

The following proposition gives two fundamental inequalities relating the discriminant of L and the product of its successive minima.

Proposition 2.3. *Let L be a lattice of discriminant D with successive minima $\mu_1, \ldots, \mu_n$. Then there exists a constant C $(= C(n))$ such that*

$$D \leq \mu_1 \cdots \mu_n \leq CD.$$

Proof. The existence of a constant C for which the second inequality holds is a classical result of Minkowski (see, e.g., [2, Chapter 12]). The proof of the first inequality requires only real linear algebra, but we sketch a proof in the present context for completeness. Let $\mathbb{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ be a basis for L, and $M = (B(\mathbf{v}_i, \mathbf{v}_j))$; so $D = \det(M)$. Let $\mathbf{m}_1, \ldots, \mathbf{m}_n$ be linearly independent vectors of L such that $Q(\mathbf{m}_i) = \mu_i$, let $\mathbf{x}_i$ be the coordinate vector (written as a column vector) for $\mathbf{m}_i$ with respect to $\mathbb{B}$, and let $X \in M_n(\mathbb{Z})$ be the matrix with columns $\mathbf{x}_1, \ldots, \mathbf{x}_n$. The matrix $A = X^t M X$ is positive definite and so is orthogonally similar over $\mathbb{R}$ to I_n; thus, there exists $P \in M_n(\mathbb{R})$ such that $A = P^t P$. Write $P = TP_1$ with T orthogonal and P_1 upper triangular, and denote the ijth entry of P_1 by p_{ij}. Then $A = P_1^t P_1$ and the ith diagonal entry of A is seen to be

$$\mu_i = Q(\mathbf{m}_i) = \sum_{j=1}^{i} p_{ji}^2 \geq p_{ii}^2.$$

So

$$\prod_{i=1}^{n} \mu_i \geq \prod_{i=1}^{n} p_{ii}^2 = (\det(P_1))^2 = \det(A) = (\det(X))^2 D.$$

The desired inequality now follows since $\det(X)$ is an integer. □

We close this section with a specialized result which is tailored to its application in the proof of Theorem 4.3.

Lemma 2.4. *Let L be a lattice of rank 4 with successive minima $\mu_1, \ldots, \mu_4$, let $\mathbf{m}_1, \ldots, \mathbf{m}_4$ be linearly independent vectors in L with $Q(\mathbf{m}_i) = \mu_i$, $1 \leq i \leq 4$,*

and let $M = \text{span}\{\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3\} \cap L$. *Let* K *be a binary lattice with successive minima* μ_1', μ_2'. *If* K *is represented by* L, *but not by* M, *then* $\mu_4 \leq \mu_2'$.

Proof. Without loss of generality, we may assume that $K \subseteq L$. Let $\mathbf{m}_1', \mathbf{m}_2' \in K$ be linearly independent vectors such that $Q(\mathbf{m}_1') = \mu_1'$ and $Q(\mathbf{m}_2') = \mu_2'$. Note that $Q(\mathbf{m}_1' \pm \mathbf{m}_2') \geq \mu_2'$ implies that $|B(\mathbf{m}_1', \mathbf{m}_2')| \leq \frac{1}{2}Q(\mathbf{m}_1')$. We first establish that $K = \mathbb{Z}\mathbf{m}_1' + \mathbb{Z}\mathbf{m}_2'$. If not, then there exist $r, s \in \mathbb{Q}$, not both integers, such that $\mathbf{v} = r\mathbf{m}_1' + s\mathbf{m}_2' \in K$ (since $\mathbf{m}_1', \mathbf{m}_2'$ span $\mathbb{Q}K$). Subtracting off integral multiples of $\mathbf{m}_1'$ and $\mathbf{m}_2'$ if necessary, we may assume that $0 \leq r, s \leq \frac{1}{2}$, with not both r and s equal 0. So

$$\begin{aligned} Q(\mathbf{v}) = Q(r\mathbf{m}_1' + s\mathbf{m}_2') &\leq \tfrac{1}{4}Q(\mathbf{m}_1') + \tfrac{1}{4}Q(\mathbf{m}_2') + \tfrac{1}{2}|B(\mathbf{m}_1', \mathbf{m}_2')| \\ &\leq \tfrac{3}{4}Q(\mathbf{m}_2') < Q(\mathbf{m}_2'). \end{aligned}$$

If $s \neq 0$, then $\dim(\text{span}\{\mathbf{m}_1', \mathbf{v}\}) = 2$ and $Q(\mathbf{v}) < \mu_2'$, a contradiction. If $s = 0$, then $\mathbf{v} = r\mathbf{m}_1' \in K$ and $Q(\mathbf{v}) < \mu_1$, again a contradiction. Hence it must be that $K = \mathbb{Z}\mathbf{m}_1' + \mathbb{Z}\mathbf{m}_2'$, as claimed.

Now $K \not\subseteq M$, by assumption. So, since $K = \mathbb{Z}\mathbf{m}_1' + \mathbb{Z}\mathbf{m}_2'$, we must have either $\mathbf{m}_1' \notin M$ or $\mathbf{m}_2' \notin M$. Then $\mu_2' \geq \mu_4$ follows from Lemma 2.2. □

3. Estimation of character sums

The material in this section closely parallels the estimation of character sums in Watson's original paper [10], and indeed the main terms in the estimates remain unchanged. However, detailed proofs of some results are included here, since it is the precise form of the error terms which will play a critical role in later arguments. In this regard, it is the use of the character sum estimate of Burgess [1], rather than that of Pólya [9], which leads to the needed improvement.

The notation in this section is largely independent of that in the rest of the paper. Throughout the section, $\chi_1, \ldots, \chi_r$ will denote a set of Dirichlet characters modulo $k_1, \ldots, k_r$, respectively, $\eta_1, \ldots, \eta_r$ will be values from the set $\{\pm 1\}$, and Γ will be the least common multiple of $k_1, \ldots, k_r$. Our goal here is to estimate the number $S(H)$ of positive integers n less than some value H which satisfy the conditions

$$\chi_i(n) = \eta_i, \quad \text{for } i = 1, \ldots, r \tag{3.1}$$

and

$$\gcd(n, \Delta) = 1, \tag{3.2}$$

where Δ is a positive integer relatively prime to Γ.

An inequality of the form $A \ll B$ will mean that there exists a constant k such that $|A| < kB$. Alternatively we will write $A = B + O(C)$ when $(A - B) \ll C$. Moreover, a statement of the type "$A \ll B^{t+\varepsilon}$" will always mean "for any $\varepsilon > 0$, $A \ll B^{t+\varepsilon}$, where the implied constant depends only on ε". In particular, the symbol ε is used throughout in a generic sense and is not assumed to have the same value at every occurrence.

It will be convenient to introduce some additional notations for the proof of the next result. We will denote the two-element set $\{1, 2\}$ by T and use the notation $\mathbf{e} = (e_1, \ldots, e_r)$ for elements of the product set T^r. For any such $\mathbf{e}$,

$\pi_{\mathbf{e}} = \prod_{i=1}^{r} (\eta_i \chi_i)^{e_i}$ is a Dirichlet character modulo Γ. If $\mathbf{e} = \mathbf{e}_0 = (2, 2, \ldots, 2)$, then $\pi_{\mathbf{e}}$ is the principal character modulo Γ. We will say that $\chi_1, \ldots, \chi_r$ are "independent" if π_e is a nonprincipal character for all $\mathbf{e} \neq \mathbf{e}_0$.

Lemma 3.1. *If $\chi_1, \ldots, \chi_r$ are independent, then*

$$\sum_{\substack{0<n<H \\ (3.1)}} 1 = 2^{-r} \sum_{\substack{0<n<H \\ \gcd(n,\Gamma)=1}} 1 + O(H^{\frac{1}{2}}\Gamma^{\frac{3}{16}+\varepsilon}).$$

Proof. If (3.1) holds for n, then $\pi_e(n) = 1$ for all $\mathbf{e} \in T^r$. On the other hand, if (3.1) fails for n, then there exists j such that either $\chi_j(n) = 0$ (if $\gcd(n, k_j) \neq 1$) or $\eta_j\chi_j(n) = -1$ (if $\gcd(n, k_j) = 1$). If $\chi_j(n) = 0$, then $\pi_{\mathbf{e}}(n) = 0$ for all $\mathbf{e} \in T^r$. If $\eta_j\chi_j(n) = -1$, then $\sum_{\mathbf{e}\in T^r} (\eta_j\chi_j(n))^{e_j} = 0$. So we obtain

$$\sum_{\mathbf{e}\in T^r} \pi_{\mathbf{e}}(n) = \begin{cases} 0 & \text{if (3.1) fails for } n, \\ 2^r & \text{if (3.1) holds for } n. \end{cases}$$

Hence,

$$\begin{aligned} 2^r \sum_{\substack{0<n<H \\ (3.1)}} 1 &= \sum_{0<n<H} \left(\sum_{\mathbf{e}\in T^r} \pi_{\mathbf{e}}(n) \right) = \sum_{\mathbf{e}\in T^r} \left(\sum_{0<n<H} \pi_{\mathbf{e}}(n) \right) \\ &= \sum_{0<n<H} \pi_{\mathbf{e}_0}(n) + \sum_{\substack{\mathbf{e}\in T^r \\ \mathbf{e}\neq\mathbf{e}_0}} \left(\sum_{0<n<H} \pi_{\mathbf{e}}(n) \right) \\ &= \sum_{\substack{0<n<H \\ \gcd(n,\Gamma)=1}} 1 + \sum_{\substack{\mathbf{e}\in T^r \\ \mathbf{e}\neq\mathbf{e}_0}} \left(\sum_{0<n<H} \pi_{\mathbf{e}}(n) \right). \end{aligned}$$

So

$$\left| 2^r \sum_{\substack{0<n<H \\ (3.1)}} 1 - \sum_{\substack{0<n<H \\ \gcd(n,\Gamma)=1}} 1 \right| \leq \sum_{\substack{\mathbf{e}\in T^r \\ \mathbf{e}\neq\mathbf{e}_0}} \left| \sum_{0<n<H} \pi_{\mathbf{e}}(n) \right|.$$

For each $\mathbf{e} \neq \mathbf{e}_0$, $\pi_{\mathbf{e}}$ is a nonprincipal character modulo Γ, and it follows from [1, Theorem 2] that

$$\left| \sum_{0<n<H} \pi_{\mathbf{e}}(n) \right| \ll H^{\frac{1}{2}}\Gamma^{\frac{3}{16}+\varepsilon}.$$

Hence,

$$\left| 2^r \sum_{\substack{0<n<H \\ (3.1)}} 1 - \sum_{\substack{0<n<H \\ \gcd(n,\Gamma)=1}} 1 \right| \ll 2^{r-1} H^{\frac{1}{2}}\Gamma^{\frac{3}{16}+\varepsilon},$$

and the desired result follows. □

Proceeding exactly as in the proof of Lemma 4 in [10], the following estimate for $S(H)$ can now be derived from Lemma 3.1.

Proposition 3.2. *If $\chi_1, \ldots, \chi_r$ are independent, then*

$$S(H) = 2^{-r} \frac{\phi(\Gamma\Delta)}{\Gamma\Delta} H + O\left(H^{\frac{1}{2}}\Gamma^{\frac{3}{16}+\varepsilon}\Delta^{\varepsilon} \right),$$

where ϕ denotes Euler's phi-function.

The main use of this result in later arguments will be to obtain an upper bound, in terms of the magnitudes of Γ and Δ, for the smallest positive integer h for which conditions (3.1) and (3.2) hold. In terms of the sums $S(H)$, h can be characterized as $\min\{H \in \mathbb{N} : S(H) > 0\}$.

Corollary 3.3. *Suppose that* $\chi_1, \ldots, \chi_r$ *are independent and* $r \leq \omega(\Gamma) + 1$, *where* $\omega(\Gamma)$ *denotes the number of distinct prime divisors of* Γ. *Then* $h \ll \Gamma^{\frac{3}{8}+\varepsilon}\Delta^{\varepsilon}$.

Proof. By Proposition 3.2, there exists a positive constant C such that, for all H,

$$S(H) \geq 2^{-r}\frac{\phi(\Gamma\Delta)}{\Gamma\Delta}H - CH^{\frac{1}{2}}\Gamma^{\frac{3}{16}+\varepsilon}\Delta^{\varepsilon}.$$

It follows that $S(H) > 0$ whenever

$$\sqrt{H} > 2^{r}C\frac{\Gamma\Delta}{\phi(\Gamma\Delta)}\Gamma^{\frac{3}{16}+\varepsilon}\Delta^{\varepsilon}.$$

Furthermore, $2^r \ll 2^{\omega(\Gamma)} \leq \tau(\Gamma) \ll \Gamma^{\varepsilon}$, where $\tau(\Gamma)$ denotes the number of positive divisors of Γ, and $\frac{\Gamma\Delta}{\phi(\Gamma\Delta)} \ll (\Gamma\Delta)^{\varepsilon}$ (e.g., see [5]). The desired inequality $h \ll \Gamma^{\frac{3}{8}+\varepsilon}\Delta^{\varepsilon}$ follows. □

The following minor refinement of Corollary 3.3 will also be needed.

Corollary 3.4. *Let* n_0 *satisfy* (3.1) *and* (3.2), *and let* $h_0 = \min\{n \in \mathbb{N}:$ (3.1) *and* (3.2) *hold, and* $n \neq \lambda^2 n_0$ *for any* $\lambda \in \mathbb{N}\}$. *Then, under the assumptions of Corollary* 3.3, $h_0 \ll \Gamma^{\frac{3}{8}+\varepsilon}\Delta^{\varepsilon}$.

Proof. Let

$$S_0(H) = \sum_{\substack{0<n<H \\ (3.1),(3.2) \\ n\neq\lambda^2 n_0}} 1.$$

Then

$$S_0(H) = S(H) - \sum_{1<\lambda<\sqrt{H}/n_0} 1 = S(H) - \left[\!\left[\frac{\sqrt{H}}{n_0}\right]\!\right].$$

As

$$\left[\!\left[\frac{\sqrt{H}}{n_0}\right]\!\right] = O(H^{\frac{1}{2}})$$

we obtain from Proposition 3.2

$$S_0(H) = 2^{-r}\frac{\phi(\Gamma\Delta)}{\Gamma\Delta}H + O(H^{\frac{1}{2}}\Gamma^{\frac{3}{16}+\varepsilon}\Delta^{\varepsilon}).$$

The proof now follows as for Corollary 3.3. □

4. Representation by quaternary lattices

Let (V, Q) be a positive definite rational quadratic space of dimension 4 and let L be a $\mathbb{Z}$-lattice on V of scale $\mathbb{Z}$ and discriminant D. Such a lattice L is said to be even (odd, respectively) if its norm ideal nL is $2\mathbb{Z}$ ($\mathbb{Z}$, respectively). Write $D = \prod D_p$, where $D_p = p^{\operatorname{ord}_p D}$ and the product is taken

over all primes p. To distinguish between orthogonal splittings of lattices and spaces, it will be convenient to use the notation $\langle \alpha_1, \ldots, \alpha_n \rangle$ for the former and $[\alpha_1, \ldots, \alpha_n]$ for the latter. For each odd prime p, L_p has a splitting of the type $L_p \cong \langle \alpha_p, p^{r_p}\beta_p \rangle \perp L_p'$, where $\alpha_p, \beta_p \in \mathscr{U}_p$, r_p is a nonnegative integer, and $sL_p' \subseteq p^{r_p}\mathbb{Z}_p$. Let T_1 (T_2, respectively) denote the set of odd primes p for which $r_p \geq 1$ ($r_p = 0$ and $sL_p' \subseteq p\mathbb{Z}_p$, respectively), and let $T = T_1 \cup T_2 \cup \{2\}$. For $p \in T_1$, we have $p^{3r_p} \leq D_p$ and so $p^{r_p} \leq D_p^{\frac{1}{3}}$; for $p \in T_2$, $p^2 | D$ implies that $p \leq D_p^{\frac{1}{2}}$. For the prime 2, there are two possible types of splittings to consider. If $nL_2 = 2\mathbb{Z}_2$, let $r_2 = 0$. On the other hand, if $nL_2 = \mathbb{Z}_2$ then there is a splitting $L_2 = \mathbb{Z}_2\mathbf{x} \perp L_2'$ with $Q(\mathbf{x}) \in \mathscr{U}_2$ and $sL_2' \subseteq \mathbb{Z}_2$; in this case, let r_2 denote that nonnegative integer such that $nL_2' = 2^{r_2}\mathbb{Z}_2$. Note that $sL_2' \subseteq 2^{r_2-1}\mathbb{Z}_2$, and it follows that $vL_2' \subseteq 2^{3(r_2-1)}\mathbb{Z}_2$; thus, $3(r_2 - 1) \leq \operatorname{ord}_2 dL_2 = \operatorname{ord}_2 D$ and $2^{r_2} \leq (8D_2)^{\frac{1}{3}}$. Let Ω denote the product $\prod_{p \in T} p^{r_p}$. From the above inequalities it follows that $\Omega \leq (8\prod_{p \in T} D_p)^{\frac{1}{3}} \leq (8D)^{\frac{1}{3}}$.

Lemma 4.1. *For each $p \in T$, there exists a binary $\mathbb{Z}_p$-lattice $N(p) \subseteq L_p$ such that $sN(p) = \mathbb{Z}_p$ and $\operatorname{ord}_p dN(p) = r_p$.*

Proof. For odd $p \in T$, simply take $N(p) \subseteq L_p$ such that $N(p) \cong \langle \alpha_p, p^{r_p}\beta_p \rangle$. So we consider further only $p = 2$. To analyze the splitting of L_2, it is helpful to first summarize some facts regarding the splitting of lattices over $\mathbb{Z}_2$ (for details and proofs, see [8, §93]). If K is a $\mathbb{Z}_2$-lattice with scale $2^j\mathbb{Z}_2$, then any Jordan splitting of K contains a $2^j\mathbb{Z}_2$-modular component M. Moreover, $nK = 2^j\mathbb{Z}_2$ holds if and only if $nM = 2^j\mathbb{Z}_2$, which in turn holds if and only if M has an orthogonal basis. Otherwise, M (and hence K) is split by a plane isometric to $2^jA(2, b)$ for either $b = 0$ or $b = 2$. Returning now to the situation at hand, we see that if $nL_2 = 2\mathbb{Z}_2$ then L_2 is split by a binary unimodular sublattice $N(2)$ as desired. In case $nL_2 = \mathbb{Z}_2$, consider further the splitting $L_2 = \mathbb{Z}_2\mathbf{x} \perp L_2'$ with $Q(\mathbf{x}) \in \mathscr{U}_2$ and $sL_2' \subseteq \mathbb{Z}_2$. If $nL_2' = sL_2'$, then $L_2' = \mathbb{Z}_2\mathbf{y} \perp L_2''$ for some $\mathbf{y} \in L_2'$ with $\operatorname{ord}_2 Q(\mathbf{y}) = r_2$. If $nL_2' = 2sL_2'$, then L_2' is split by a plane $\mathbb{Z}_2\mathbf{y} + \mathbb{Z}_2\mathbf{w}$ with $\operatorname{ord}_2 Q(\mathbf{y}) = r_2$. In either case, $N(2) = \mathbb{Z}_2\mathbf{x} \perp \mathbb{Z}_2\mathbf{y}$ has the required properties. □

For the remainder of the section, for each $p \in T$ fix a lattice $N(p)$ satisfying the conditions in Lemma 4.1, and let $\delta_p \in \mathbb{Z}_p$ be such that $dN(p) = \delta_p$.

Proposition 4.2. *Let q and q' be primes not dividing D. If n is a positive integer such that $qq'n\Omega \cong \delta_p$ for all $p \in T$ and $\gcd(n, 2qq'D) = 1$, then there exists a binary $\mathbb{Z}$-lattice K $(= K(n, q, q'))$ such that*

(i) $dK = qq'n\Omega$,
(ii) $S_q(\mathbb{Q}K) = +1$,
(iii) $\mathbb{Q}K \rightarrowtail V$, *and*
(iv) $K_p \rightarrowtail L_p$ *for all p in the set S of all nonarchimedean prime spots on $\mathbb{Q}$.*

Proof. For simplicity, we write Θ $(= \Theta(n, q, q'))$ for the product $qq'n\Omega$. For $p \neq q, q'$, let $U(p)$ denote a binary space over $\mathbb{Q}_p$ such that

$$U(p) \cong \begin{cases} \mathbb{Q}_p N(p) & \text{if } p \in T, \\ [1, \Theta] & \text{if } p \notin T \cup \{q, q'\}. \end{cases}$$

Since $\Theta \notin -\dot{\mathbb{Q}}_q^2$ and $\Theta \notin -\dot{\mathbb{Q}}_{q'}^2$, there exist binary spaces $U(q)$ and $U(q')$ over $\mathbb{Q}_q$ and $\mathbb{Q}_{q'}$, respectively, with $dU(q) = \Theta$, $dU(q') = \Theta$, $S_q U(q) = +1$ and $S_{q'} U(q') = \prod_{p \neq q'} S_p U(p)$ [8, 63:23]. Note that Θ is a positive integer such that $dU(p) = \Theta$ holds for all p (for $p \in T$ this follows from the assumption that $qq'n\Omega \cong \delta_p$). Since $S_p U(p) = +1$ holds for almost all p and $\prod_p S_p U(p) = +1$, there exists a global binary space W over $\mathbb{Q}$ for which $W_p \cong U(p)$ for all p [8, 72:1].

Next we will show that $W_p \rightarrowtail V_p$ holds for all p. Such a representation is guaranteed to exist unless $dV_p = -dW_p$ and $V_p \not\cong W_p \perp H$, where H is a hyperbolic plane [8, 63:21]. First, for $p \in T$, $W_p \rightarrowtail V_p$ follows from the fact that $W_p \cong \mathbb{Q}_p N(p)$ and $\mathbb{Q}_p N(p) \subseteq V_p$. Next, if $p|D$ but $p \notin T$, then L_p has a ternary unimodular Jordan component L_p'. As $\Theta \in \mathscr{U}_p$, it follows from [8, 92:1a] that $L_p' \cong \langle 1, \Theta, \Theta u \rangle$ for some $u \in \mathscr{U}_p$; so $W_p \rightarrowtail V_p$. Now consider those primes p for which $p \nmid 2D$. If $\operatorname{ord}_p \Theta$ is odd (note that this includes the cases $p = q, q'$), then $dV_p = -dW_p$ does not hold and we are assured that $W_p \rightarrowtail V_p$. If $\operatorname{ord}_p \Theta$ is even, then $S_p(W_p \perp H) = S_p([1, \Theta, 1, -1]) = 1 = S_p V_p$, the last equality holding since $L_p \cong \langle 1, 1, 1, D \rangle$ with $D \in \mathscr{U}_p$ [8, 92:1]. So again $W_p \rightarrowtail V_p$. Finally, for the infinite spot p, $W_p \rightarrowtail V_p$ holds since $\Theta > 0$ and thus W_p is positive definite. We have now completed the verification that $W_p \rightarrowtail V_p$ holds for all p. It follows from the Hasse-Minkowski Theorem that $W \rightarrowtail V$.

Now we turn to the construction of a lattice K on W having the required properties. Note first that there exist $\mathbf{x}, \mathbf{y} \in W$ such that $W = \mathbb{Q}\mathbf{x} \perp \mathbb{Q}\mathbf{y}$ and $Q(\mathbf{x})Q(\mathbf{y}) = \Theta$. For the lattice $M = \mathbb{Z}\mathbf{x} \perp \mathbb{Z}\mathbf{y}$, $sM_p = \mathbb{Z}_p$ holds for all primes p outside some finite set Σ. We proceed to define local lattices $J(p)$ for each $p \in S$. For each $p \notin \Sigma \cup T$, let $J(p) = M_p$. For $p \in T$, let $J(p)$ be a lattice on W_p isometric to the lattice $N(p)$. For $p \in \Sigma \setminus (T \cup \{q, q'\})$, let $J(p)$ be a lattice on W_p isometric to $\langle 1, \Theta \rangle$. If $q \in \Sigma$, proceed as follows to define $J(q)$. Since $\operatorname{ord}_q dW_q = 1$, W_q represents an element $\alpha \in \mathbb{Q}_q$ with $\operatorname{ord}_q \alpha$ even. So there exists some $\mathbf{w} \in W_q$ such that $Q(\mathbf{w}) \in \mathscr{U}_q$, and W_q has a splitting $W_q = \mathbb{Q}_q\mathbf{w} \perp \mathbb{Q}_q\mathbf{z}$ with $Q(\mathbf{z}) \in q\mathscr{U}_q$; let $J(q) = \mathbb{Z}_q\mathbf{w} \perp \mathbb{Z}_q\mathbf{z}$. Finally, if $q' \in \Sigma$, obtain a lattice $J(q')$ exactly as described for $J(q)$. So for all $p \in S$ we have now defined local lattices $J(p)$ on W_p with the properties that $dJ(p) = \Theta$ and $sJ(p) = \mathbb{Z}_p$. Moreover, $J(p) = M_p$ for almost all p. So there exists a $\mathbb{Z}$-lattice K on W such that $K_p = J(p)$ for all $p \in S$ [8, 81:14]. In particular, $sK = \mathbb{Z}$ and $dK = \Theta$.

To complete the proof, it remains to show that $K_p \rightarrowtail L_p$ for all $p \in S$ or, equivalently, that $J(p) \rightarrowtail L_p$ for all $p \in S$. For $p \in T$ this follows immediately from the definition of $J(p)$. For $p|D$, $p \notin T$, $J(p) \rightarrowtail L_p$ follows from [8, 92:1a] (since $dJ(p) \in \mathscr{U}_p$ and L_p has a ternary unimodular Jordan component). Finally, for $p \nmid 2D$, L_p is unimodular and $sK_p = \mathbb{Z}_p$; so [7, Theorem 1] reduces the representation problem to the corresponding problem for the spaces spanned by the two lattices. As $W_p \rightarrowtail V_p$ has already been established, it again follows that $K_p \rightarrowtail L_p$, and the proof is now complete. □

Theorem 4.3. *There exist only finitely many inequivalent 2-regular primitive positive definite quaternary lattices.*

Proof. Let L be a 2-regular primitive positive definite quaternary lattice. We continue the notations for the local splittings of L established in the first paragraph of this section. For each $p \in T_1 \cup T_2$, define Ψ_p to be the character modulo p defined by the Legendre symbol $(\frac{*}{p})$ and define $\nu_p \in \{\pm 1\}$ by

$$\nu_p = \begin{cases} (\alpha_p, p)_p & \text{if } L \text{ is odd,} \\ (\frac{2}{p})(\alpha_p, p)_p & \text{if } L \text{ is even,} \end{cases}$$

where $(\alpha_p, p)_p$ denotes the Hilbert symbol. To handle the prime 2, we need to introduce two characters. Let Ψ_{-1} and Ψ_2 be the characters modulo 8 defined by the Jacobi symbols $(\frac{-1}{*})$ and $(\frac{2}{*})$, respectively. If $nL_2 = \mathbb{Z}_2$ ($nL_2 = 2\mathbb{Z}_2$, respectively) then there exists $\mathbf{x} \in L_2$ such that $Q(\mathbf{x}) \in \mathcal{U}_2$ ($Q(\mathbf{x}) \in 2\mathcal{U}_2$, respectively); let $\xi \in \{1, 3, 5, 7\}$ be such that $Q(\mathbf{x}) \in \xi\mathcal{U}_2^2$ ($Q(\mathbf{x}) \in 2\xi\mathcal{U}_2^2$, respectively). For odd integers k, the values of $\Psi_{-1}(k)$ and $\Psi_2(k)$ determine the congruence class of k modulo 8. So there exist $\nu_{-1}, \nu_2 \in \{\pm 1\}$ such that $\Psi_{-1}(k) = \nu_{-1}$ and $\Psi_2(k) = \nu_2$ hold if and only if $k \equiv \xi \pmod 8$.

Now suppose that k is a positive integer satisfying

$$\Psi_p(k) = \nu_p \quad \text{for all } p \in T_1 \cup \{-1, 2\} \tag{4.1}$$

and

$$\gcd(k, D) = 1. \tag{4.2}$$

If L is odd (even, respectively), then the condition (4.1) guarantees that k ($2k$, respectively) is represented by L_p for all $p \in T_1 \cup \{2\}$. For the primes $p \in T_2$, L_p has a binary unimodular Jordan component and thus (4.2) guarantees that L_p represents both k and $2k$ [8, 92:1b]. For those primes p outside T, L_p has a unimodular Jordan component which is at least ternary and again L_p represents both k and $2k$ [8, 92:1b]. Hence, L locally represents all integers k (if L is odd) or all integers of the form $2k$ (if L is even) for which (4.1) and (4.2) hold. Since L is 2-regular (and hence regular), it follows that L globally represents all such integers.

Let μ_1 be the minimum of L. Applying Corollary 3.3 with characters $\{\Psi_p : p \in T_1 \cup \{-1, 2\}\}$, specified values $\{\nu_p : p \in T_1 \cup \{-1, 2\}\}$ and Δ the product of all primes dividing D but not in $T_1 \cup \{2\}$, we obtain

$$\mu_1 \ll \left(8 \prod_{p \in T_1} p\right)^{\frac{3}{8}+\varepsilon} \Delta^{\varepsilon}$$

and, since $2\prod_{p \in T_1} p \le \Omega \le (8D)^{\frac{1}{3}}$, this yields

$$\mu_1 \ll D^{\frac{1}{8}+\varepsilon}. \tag{4.3}$$

Now let $\mathbf{m}_1 \in L$ be such that $Q(\mathbf{m}_1) = \mu_1$. If $n \in Q(L)$ and $n \neq \gamma^2\mu_1$ for any $\gamma \in \mathbb{Z}$, then $\dim(\operatorname{span}\{\mathbf{x} \in L : Q(\mathbf{x}) \le n\}) \ge 2$ and it follows that the second minimum μ_2 of L satisfies $\mu_2 \le n$. Applying Corollary 3.4 with characters, specified values and Δ as above and $n_0 = \mu_1$, we obtain

$$\mu_2 \ll D^{\frac{1}{8}+\varepsilon}. \tag{4.4}$$

Let $\mathbf{m}_1, \mathbf{m}_2$ be linearly independent vectors in L such that $Q(\mathbf{m}_i) = \mu_i$ for $i = 1, 2$, and let $G = \operatorname{span}\{\mathbf{m}_1, \mathbf{m}_2\} \cap L$. The successive minima of the binary lattice G are μ_1 and μ_2. So $dG \le \mu_1\mu_2$ by Proposition 2.3, and it

follows from (4.3) and (4.4) that $dG \ll D^{\frac{1}{4}+\varepsilon}$. Let f be the smallest prime not dividing $2D$ for which $(\frac{-dG}{f}) = -1$. To estimate the size of f, apply Corollary 3.3 in the case that $r = 1$, the only character is the character modulo $8dG$, defined by the Jacobi symbol $(\frac{-dG}{*})$, the corresponding value of η is -1, and Δ is the product of the odd prime divisors of D which do not divide dG. This yields $f \ll dG^{\frac{3}{8}+\varepsilon}\Delta^{\varepsilon}$ which, combined with the estimate for dG above, gives $f \ll D^{\frac{3}{32}+\varepsilon}$. Next, let m be the smallest positive integer for which $\gcd(m, fD) = 1$ and $\Psi_p(m) = \Psi_p(f)\nu_p$ holds for $p \in T_1 \cup \{-1, 2\}$. Arguing as in the preceding paragraph (with ν_p replaced by $\Psi_p(f)\nu_p$ and the Δ used there replaced by $f\Delta$), we obtain $m \ll D^{\frac{1}{8}+\varepsilon}$. Since the conditions (4.1) and (4.2) hold for $k = fm$, either fm or $2fm$ is represented by L. However, neither fm nor $2fm$ is represented by G. To see this for fm, compare the Hasse symbols at f of the spaces $[fm, fmdG]$ and $\mathbb{Q}G$. On the one hand, $S_f(\mathbb{Q}G) = +1$ since $f \nmid dG$. But $S_f([fm, fmdG])$ is easily computed to be $(\frac{-dG}{f}) = -1$, using the conditions $f \nmid dG$ and $f \nmid m$. The verification for $2fm$ is identical. Thus, there exists $\mathbf{y} \in L$ such that $Q(\mathbf{y}) \leq 2fm$ and $\mathbf{y} \notin G$. So $\dim(\operatorname{span}\{\mathbf{x} \in L : Q(\mathbf{x}) \leq 2fm\}) \geq 3$, and it follows that the third minimum μ_3 of L satisfies

$$\mu_3 \ll D^{\frac{7}{32}+\varepsilon}. \tag{4.5}$$

Now let $\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3$ be linearly independent vectors of L with $Q(\mathbf{m}_i) = \mu_i$ for $i = 1, 2, 3$, and let $M = \operatorname{span}\{\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3\} \cap L$. The successive minima of the ternary lattice M are μ_1, μ_2 and μ_3. So $dM \leq \mu_1\mu_2\mu_3$ by Proposition 2.3 and it follows from (4.3)–(4.5) that $dM \ll D^{\frac{15}{32}+\varepsilon}$. Let q be the smallest prime not dividing $2D$ for which $(\frac{dM}{q}) = -1$. Arguing as for f in the preceding paragraph yields $q \ll D^{\frac{15}{32}\cdot\frac{3}{8}+\varepsilon} = D^{\frac{45}{256}+\varepsilon}$. Let q' be the smallest prime not dividing $2qD$. Then $q' \ll D^{\varepsilon}$ follows from Corollary 3.3 (applied in the case that there are no character conditions). Let n be the smallest positive integer for which $qq'n\Omega \cong \delta_p$ holds for all $p \in T$ and $\gcd(n, 2qq'D) = 1$. For each $p \in T$, $\delta_p(qq'\Omega)^{-1} \in \mathscr{U}_p$ and $qq'n\Omega \cong \delta_p$ is equivalent to $n \in \delta_p(qq'\Omega)^{-1}\mathscr{U}_p^2$. So there exist σ_{-1} and $\{\sigma_p : p \in T\}$ in $\{\pm 1\}$ such that the conditions $\Psi_{-1}(n) = \sigma_{-1}$ and $\Psi_p(n) = \sigma_p$ hold for all $p \in T$ if and only if $qq'n\Omega \cong \delta_p$ holds for all $p \in T$. Applying Corollary 3.3 with characters $\{\Psi_p : p \in T \cup \{-1\}\}$, specified values $\{\sigma_p : p \in T \cup \{-1\}\}$ and Δ equal to the product of all prime divisors of $qq'D$ which do not lie in T, we obtain $n \ll \Gamma^{\frac{3}{8}+\varepsilon}\Delta^{\varepsilon}$, where $\Gamma = 8\prod_{p\in T} p$. Now $\prod_{p\in T_1} p \leq \prod_{p\in T_1} p^{r_p} \leq \prod_{p\in T_1} D_p^{\frac{1}{3}}$ and $\prod_{p\in T_2} p \leq \prod_{p\in T_2} D_p^{\frac{1}{2}}$. So

$$\begin{aligned}\Gamma^{\frac{3}{8}}\Omega &= 8^{\frac{3}{8}}\Big(\prod_{p\in T_1} p\Big)^{\frac{3}{8}}\Big(\prod_{p\in T_2} p\Big)^{\frac{3}{8}} 2^{r_2}\Big(\prod_{p\in T_1} p^{r_p}\Big)\\ &\ll D_2^{\frac{1}{3}}\Big(\prod_{p\in T_1} D_p^{\frac{11}{24}}\Big)\Big(\prod_{p\in T_2} D_p^{\frac{3}{16}}\Big) \leq D^{\frac{11}{24}}.\end{aligned}$$

Thus,

$$qq'n\Omega \ll D^{\frac{45}{256}+\frac{11}{24}+\varepsilon} = D^{\frac{487}{768}+\varepsilon}. \tag{4.6}$$

By Proposition 4.2, there exists a binary $\mathbb{Z}$-lattice K $(= K(n, q, q'))$ such that $dK = qq'n\Omega$, $S_q(\mathbb{Q}K) = +1$ and $K_p \rightarrowtail L_p$ for all p. Since L is

2-regular, the last condition implies that $K \rightarrowtail L$. However, K is not represented by the ternary sublattice M. To see this, compare the Hasse symbols at q of $\mathbb{Q}M$ and $\mathbb{Q}K \perp [dK \cdot dM]$. On the one hand, $S_q(\mathbb{Q}M) = +1$ since $q \nmid dM$. On the other hand, $S_q(\mathbb{Q}K \perp [dK \cdot dM]) = S_q(\mathbb{Q}K) \cdot (dK \cdot dM, -1)_q (dK, dK \cdot dM)_q$ by [8, 58:3], $S_q(\mathbb{Q}K) = +1$ by the construction of K, $(dK \cdot dM, -1)_q = (dK, -1)_q = (q, -1)_q$ since $q \nmid q' n \Omega dM$, and $(dK, dK \cdot dM)_q = (dK, -dM)_q = (q, -dM)_q$. So

$$S_q(\mathbb{Q}K \perp [dK \cdot dM]) = (q, dM)_q = \left(\frac{dM}{q}\right) = -1 \neq S_q(\mathbb{Q}M).$$

Let μ_1', μ_2' be the successive minima of K. Then $\mu_1 \leq \mu_1'$ and, by Lemma 2.4, $\mu_4 \leq \mu_2'$, where μ_4 is the fourth successive minimum of L. So $\mu_1\mu_2\mu_3\mu_4 \leq \mu_1'\mu_2'\mu_2\mu_3$, and, by Proposition 2.3, $\mu_1'\mu_2' \ll dK = qq'n\Omega$. Combining (4.4)–(4.6) yields

$$\mu_1\mu_2\mu_3\mu_4 \ll D^{\frac{1}{8}+\frac{7}{32}+\frac{487}{768}+\varepsilon} = D^{\frac{751}{768}+\varepsilon}. \tag{4.7}$$

For ε sufficiently small that $\frac{751}{768} + \varepsilon < 1$, (4.7) is consistent with the inequality $D \leq \mu_1\mu_2\mu_3\mu_4$ from Proposition 2.3 for only finitely many values of the discriminant D. Thus, we conclude that the discriminant of a 2-regular primitive positive definite quaternary lattice must be bounded. Hence, such forms can lie in only finitely many equivalence classes. □

Acknowledgements

Work on this paper was initiated while the author was a visitor at the Ohio State Mathematical Research Institute. The author would like to take this opportunity to express his gratitude for the support and hospitality of the Institute, and his thanks to John Hsia for many helpful conversations relating to this research.

References

1. D. A. Burgess, *On character sums and L-series,* II, Proc. London Math. Soc. (3) **13** (1963,), 524–536.
2. J. W. S. Cassels, *Rational quadratic forms*, Academic Press, New York, 1978.
3. L. E. Dickson, *Ternary quadratic forms and congruences*, Ann. of Math. **28** (1927), 333–341.
4. J. S. Hsia, *Regular positive ternary quadratic forms*, Mathematika **28** (1981), 231–238.
5. W. J. LeVeque, *Fundamentals of number theory*, Addison-Wesley, Reading, MA, 1977.
6. W. Magnus, *Über die Anzahl der einem Geschlecht enthaltenen Klassen von positiv-definiten quadratischen Formen*, Math. Ann. **114** (1937), 465–475; **115** (1938), 643–644.
7. O. T. O'Meara, *The integral representations of quadratic forms over local fields*, Amer. J. Math. **80** (1958), 843–878.
8. ——, *Introduction to quadratic forms*, Springer-Verlag, New York, 1963.
9. G. Pólya, *Über die Verteilung der quadratischen Reste und Nichtreste*, Nachr. Wiss. Göttingen Math.-Phys. Kl. (1918), 21–29.
10. G. L. Watson, *The representation of integers by positive ternary quadratic forms*, Mathematika **1** (1954), 104–110.

Department of Mathematics, Southern Illinois University, Carbondale, Illinois 62901–4408