Bull. Aust. Math. Soc. **103** (2021), 50–61
doi:10.1017/S0004972720000325

CLASSIFICATION OF THE SUBLATTICES OF A LATTICE

CHUANMING ZONG

(Received 17 February 2020; accepted 24 February 2020; first published online 13 April 2020)

Abstract

In 1945–1946, C. L. Siegel proved that an n-dimensional lattice Λ of determinant $\det(\Lambda)$ has at most m^{n^2} different sublattices of determinant $m \cdot \det(\Lambda)$. In 1997, the exact number of the different sublattices of index m was determined by Baake. We present a systematic treatment for counting the sublattices and derive a formula for the number of the sublattice classes under unimodular equivalence.

2010 *Mathematics subject classification*: primary 11H06; secondary 20E07, 52C05, 52C07.
Keywords and phrases: lattice, sublattice.

1. Introduction

Let $\mathbb{Z}$ denote the set of all integers and let $\mathbb{E}^n$ denote the n-dimensional Euclidean space. If $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$ are n independent vectors in $\mathbb{E}^n$, then the discrete set

$$\Lambda = \Big\{ \sum z_i \mathbf{a}_i : z_i \in \mathbb{Z} \Big\}$$

is called an *n-dimensional lattice* generated by the *basis* $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$. If the basis vectors are expressed as $\mathbf{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in})$, then the absolute value of the determinant of

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

is called the *determinant* of Λ. Usually, it is written as $\det(\Lambda)$. In fact,

$$\det(\Lambda) = \mathrm{vol}(P),$$

where P is the parallelepiped defined by

$$P = \Big\{ \sum \lambda_i \mathbf{a}_i : 0 \le \lambda_i \le 1 \Big\}.$$

This work is supported by the National Natural Science Foundation of China (NSFC11921001) and the National Key Research and Development Program of China (2018YFA0704701).

A subset Λ^* of Λ is called a *sublattice* if it is also an n-dimensional lattice. If $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ is a basis of Λ^*, where $\mathbf{b}_i = (b_{i1}, b_{i2}, \dots, b_{in})$, then

$$\mathbf{b}_i = d_{i1}\mathbf{a}_1 + d_{i2}\mathbf{a}_2 + \cdots + d_{in}\mathbf{a}_n, \quad d_{ij} \in \mathbb{Z}.$$

Let B denote the $n \times n$ matrix with elements b_{ij} and let D denote the $n \times n$ matrix with elements d_{ij}. Then

$$B = DA$$

and therefore

$$\det(\Lambda^*) = m \cdot \det(\Lambda),$$

where m is the absolute value of the determinant of D. Usually m is defined as $[\Lambda : \Lambda^*]$ and is called the *index* of Λ^* in Λ.

The structures and representations of sublattices have been studied by many authors including Minkowski, Siegel, Cassels, Hlawka, Rogers, Schmidt and Gruber. Many results and their applications can be found in classic references such as [6, 11, 12, 17, 22]. Particular sublattices have been studied in [3–5, 7, 8, 19, 20].

Let Λ be an n-dimensional lattice and m a positive integer. Let $f_n(m)$ denote the number of different sublattices of Λ with index m and let $g_n(m)$ denote the number of different sublattice classes of Λ with index m under unimodular equivalence.

Clearly, an n-dimensional lattice is both a *free abelian group* and a *free module* over $\mathbb{Z}$. Counting the *subgroups* of a group is a classic topic in algebra (see the classic books [15, 21] and papers such as [9, 13]). However, the particular lattice case was neglected and explicit formulae for $f_n(m)$ were achieved only in 1997.

In 1945–1946, Siegel gave a series of lectures on geometry of numbers at New York University. His lecture notes [22] contained the first upper bound for $f_n(m)$, namely

$$f_n(m) \le m^{n^2}. \tag{1.1}$$

Since the lecture notes were published only in 1989, this result and many others were neglected. In 1959, Cassels [6] presented some basic results about the structures of the bases of the sublattices. In 1997, Baake [2] deduced the following formula based on a recursion,

$$f_n(m) = \sum_{d_1 d_2 \dots d_n = m} d_1^0 d_2^1 \dots d_n^{n-1}. \tag{1.2}$$

Remark 1.1. The formula (1.2) may be much older since its generating function is a product of zeta functions. Let Λ be an n-dimensional lattice and define

$$\zeta_\Lambda(s) = \sum_{m=1}^{\infty} \frac{f_n(m)}{m^s}.$$

Lubotzky and Segal [15] presented six proofs for

$$\zeta_\Lambda(s) = \zeta(s)\zeta(s-1)\cdots\zeta(s-n+1).$$

Nevertheless, the formula for $f_n(m)$ was not given there and no earlier reference has been located.

https://doi.org/10.1017/S0004972720000325 Published online by Cambridge University Press

Clearly, both Cassels and Baake were unaware of Siegel's work. Assume that

$$m = p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell},$$

where the p_i are prime numbers. Baake's formula was simplified by Gruber [10] as

$$f_n(m) = \prod_{i=1}^{\ell} \prod_{j=1}^{\alpha_\ell} \frac{p_i^{j+n-1} - 1}{p_i^j - 1} = \prod_{i=1}^{\ell} \prod_{j=1}^{n-1} \frac{p_i^{j+\alpha_i} - 1}{p_i^j - 1}.$$

In particular, when p is a prime, it is interesting to notice that

$$f_n(p) = 1 + p + \cdots + p^{n-1}$$

and

$$f_2(p^\ell) = 1 + p + \cdots + p^\ell.$$

Let k be a positive integer and let $p_n(k)$ denote the number of partitions of k into n parts. In other words, $p_n(k)$ is the number of the integer solutions of

$$\begin{cases} x_1 + x_2 + \cdots + x_n = k, \\ x_1 \geq x_2 \geq \cdots \geq x_n \geq 0. \end{cases}$$

The partition function $p_n(k)$ has a long history (see Andrews and Eriksson [1]).

The purpose of this paper is to present a systematic treatment on counting and classifying sublattices. First, we present a detailed proof of (1.2). Then we prove the following classification theorem.

Theorem 1.2. *If $m = p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell}$, where the p_i are prime numbers, then*

$$g_n(m) = \prod_{i=1}^{\ell} p_n(\alpha_i).$$

Corollary 1.3. *When $m = p_1 p_2 \dots p_\ell$, where $p_1, p_2, \dots, p_\ell$ are distinct primes,*

$$g_n(m) = 1.$$

For large $m = 2^k$ and fixed n,

$$g_n(m) \sim \frac{(\log_2 m)^{n-1}}{n!(n-1)!}.$$

2. Siegel's upper bound

Siegel's upper bound (1.1) was obtained in 1945–1946 but only published in 1989 in his lecture notes written by Chandrasekharan [22]. So, this beautiful result has been neglected. For this reason, we reproduce it here. First of all, let us introduce a well-known basic lemma which can be found in every book on lattices.

https://doi.org/10.1017/S0004972720000325 Published online by Cambridge University Press

Lemma 2.1. *Let* $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$ *be a basis of an n-dimensional lattice* Λ. *Assume that* $\mathbf{u}_1$, $\mathbf{u}_2$, …, $\mathbf{u}_n$ *are n linearly independent vectors in* $\mathbb{E}^n$ *with*

$$\mathbf{u}_i = u_{i1}\mathbf{a}_1 + u_{i2}\mathbf{a}_2 + \cdots + u_{in}\mathbf{a}_n, \quad i = 1, 2, \ldots, n.$$

Then $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ *is also a basis of* Λ *if and only if* $U = (u_{ij})$ *is an* $n \times n$ *unimodular matrix.*

Theorem 2.2 (Siegel [22]). *Assume that* Λ *is an n-dimensional lattice and m is a positive integer. Then* Λ *has at most* m^{n^2} *different sublattices of index m, that is,*

$$f_n(m) \le m^{n^2}.$$

Proof. Assume that $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$ is a basis of Λ. If Λ^* is a sublattice of Λ of index m with a basis $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$, then

$$\mathbf{u}_i = u_{i1}\mathbf{a}_1 + u_{i2}\mathbf{a}_2 + \cdots + u_{in}\mathbf{a}_n, \quad i = 1, 2, \ldots, n, \tag{2.1}$$

where all the u_{ij} are integers and $\det(u_{ij}) = \pm m$. For convenience, we denote the $n \times n$ matrix (u_{ij}) by U. If $\Lambda^\bullet$ is another sublattice of Λ of index m with a basis $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$, then

$$\mathbf{v}_i = v_{i1}\mathbf{a}_1 + v_{i2}\mathbf{a}_2 + \cdots + v_{in}\mathbf{a}_n, \quad i = 1, 2, \ldots, n, \tag{2.2}$$

where all the v_{ij} are integers and $\det(v_{ij}) = \pm m$. We denote the $n \times n$ matrix (v_{ij}) by V. From (2.1) and (2.2), the matrix that transforms $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ into $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ is UV^{-1}. In other words, if $W = UV^{-1} = (w_{ij})$, then

$$\mathbf{u}_i = w_{i1}\mathbf{v}_1 + w_{i2}\mathbf{v}_2 + \cdots + w_{in}\mathbf{v}_n, \quad i = 1, 2, \ldots, n.$$

Now, we proceed to show that if

$$u_{ij} \equiv v_{ij} \pmod{m}$$

for all $i, j = 1, 2, \ldots, n$, then Λ^* is identical with $\Lambda^\bullet$. Clearly, mV^{-1} is an integer matrix. Since $U \equiv V \pmod{m}$,

$$mW = mUV^{-1} \equiv mVV^{-1} \equiv mE \equiv O \pmod{m},$$

where E is the $n \times n$ unit matrix and O is the $n \times n$ zero matrix. This means that all elements of mW are divisible by m and therefore all elements of W are integers. On the other hand,

$$\det(W) = \det(UV^{-1}) = \pm\frac{m}{m} = \pm 1.$$

Thus, W must be a unimodular matrix and, by Lemma 2.1, Λ^* is identical with $\Lambda^\bullet$.

This shows that there are at most m possible values for any element of U such that the corresponding sublattices of Λ are different. Since U has n^2 elements, the total number of possibilities for U is m^{n^2}. In other words,

$$f_n(m) \le m^{n^2}$$

and the theorem is proved. □

https://doi.org/10.1017/S0004972720000325 Published online by Cambridge University Press

3. Sublattices of given index

In 1907, Minkowski [17] studied the relation between the bases of a three-dimensional lattice and its sublattices. His result was generalised to arbitrary dimensions (see [6] and [11]) as follows. Assume that Λ^* is a sublattice of an n-dimensional lattice Λ. If $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ is a basis of Λ^*, then Λ has a basis $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$ such that

$$\mathbf{u}_i = u_{i1}\mathbf{a}_1 + u_{i2}\mathbf{a}_2 + \cdots + u_{ii}\mathbf{a}_i, \quad i = 1, 2, \ldots, n,$$

where $u_{ii} > 0$ and $0 \le u_{ij} < u_{ii}$ for all $j < i$.

It is rather unexpected that the following inverse of this result is also true (see [6] and [11]).

LEMMA 3.1 (Cassels [6]). *Assume that Λ is an n-dimensional lattice with a basis $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$. If Λ^* is a sublattice of Λ of index m, then Λ^* has a basis $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ satisfying*

$$\mathbf{u}_i = u_{i1}\mathbf{a}_1 + u_{i2}\mathbf{a}_2 + \cdots + u_{ii}\mathbf{a}_i, \quad i = 1, 2, \ldots, n$$

and

$$m = u_{11}u_{22} \ldots u_{nn},$$

where $u_{ii} > 0$ and $0 \le u_{ij} < u_{jj}$ for all $j < i$.

Clearly, this lemma provides a means of counting the number of the different sublattices of given index m. To do the explicit counting, we need another simple result.

LEMMA 3.2. *Assume that Λ is an n-dimensional lattice with a basis $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$ and m is a positive integer. Let $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ be n linearly independent vectors satisfying*

$$\mathbf{u}_i = u_{i1}\mathbf{a}_1 + u_{i2}\mathbf{a}_2 + \cdots + u_{ii}\mathbf{a}_i, \quad i = 1, 2, \ldots, n$$

and

$$m = u_{11}u_{22} \ldots u_{nn},$$

where all the u_{ij} are integers, $u_{ii} > 0$ and $0 \le u_{ij} < u_{jj}$ for all $j < i$. Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ be n linearly independent vectors satisfying

$$\mathbf{v}_i = v_{i1}\mathbf{a}_1 + v_{i2}\mathbf{a}_2 + \cdots + v_{ii}\mathbf{a}_i, \quad i = 1, 2, \ldots, n$$

and

$$m = v_{11}v_{22} \ldots v_{nn},$$

where all the v_{ij} are integers, $v_{ii} > 0$ and $0 \le v_{ij} < v_{jj}$ for all $j < i$. Let Λ^* be the sublattice of Λ generated by $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ and let $\Lambda^\bullet$ be the sublattice of Λ generated by $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$. Then the two sublattices Λ^* and $\Lambda^\bullet$ are identical if and only if

$$u_{ij} = v_{ij}, \quad 1 \le j \le i \le n.$$

https://doi.org/10.1017/S0004972720000325 Published online by Cambridge University Press

PROOF. The if part is obvious. Now, let us prove the only if part.

Let U denote the $n \times n$ matrix with elements u_{ij}, $i, j = 1, 2, \ldots, n$, where $u_{ij} = 0$ for all $j > i$. Let V denote the $n \times n$ matrix with elements v_{ij}, $i, j = 1, 2, \ldots, n$, where $v_{ij} = 0$ for all $j > i$. Define

$$W = UV^{-1} = (w_{ij}). \tag{3.1}$$

It is easy to see that $\Lambda^* = \Lambda^\bullet$ if and only if W is a unimodular matrix.

By (3.1),

$$WV = U. \tag{3.2}$$

By comparing both sides of (3.2) for $u_{1n}, u_{1,n-1}, \ldots, u_{11}$,

$$\begin{cases} w_{11}v_{1n} + w_{12}v_{2n} + \cdots + w_{1n}v_{nn} = 0, \\ w_{11}v_{1,n-1} + w_{12}v_{2,n-1} + \cdots + w_{1n}v_{n,n-1} = 0, \\ \quad \ldots, \\ w_{11}v_{11} + w_{12}v_{21} + \cdots + w_{1n}v_{n1} = u_{11} \end{cases}$$

and thus

$$\begin{cases} w_{1n} = w_{1,n-1} = \cdots = w_{12} = 0, \\ w_{11}v_{11} = u_{11}. \end{cases}$$

Repeating this process for $u_{2i}, u_{3i}, \ldots, u_{ni}$ successively,

$$\begin{cases} w_{ij} = 0, & i < j \le n, \\ w_{ii}v_{ii} = u_{ii}, & i = 1, 2, \ldots, n. \end{cases} \tag{3.3}$$

If W is a unimodular matrix, all its elements are integers; it follows by (3.3) and the assumption

$$m = u_{11}u_{22}\ldots u_{nn} = v_{11}v_{22}\ldots v_{nn}$$

that

$$w_{11} = w_{22} = \cdots = w_{nn} = 1. \tag{3.4}$$

Then, by comparing both sides of (3.2) for $u_{21}, u_{32}, \ldots, u_{n,n-1}$,

$$w_{i+1,i}v_{ii} + v_{i+1,i} = u_{i+1,i}, \quad i = 1, 2, \ldots, n-1. \tag{3.5}$$

If $w_{i+1,i} \neq 0$, by (3.5),

$$w_{i+1,i}v_{ii} = u_{i+1,i} - v_{i+1,i},$$

which contradicts the assumptions that $0 \le u_{i+1,i} < u_{ii} = v_{ii}$ and $0 \le v_{i+1,i} < v_{ii}$. Thus,

$$\begin{cases} w_{i+1,i} = 0, \\ u_{i+1,i} = v_{i+1,i} \end{cases}$$

for all $i = 1, 2, \ldots, n-1$.

Inductively, assume that

$$w_{i+j,i} = 0$$

https://doi.org/10.1017/S0004972720000325 Published online by Cambridge University Press

holds for $1 \le j \le k-1 < n-1$ and $i = 1, 2, \ldots, n-j$. By comparing both sides of (3.2) for $u_{i+k,i}$, $i = 1, 2, \ldots, n-k$, in the same way as for (3.5),

$$w_{i+k,i} = 0, \quad i = 1, 2, \ldots, n-k.$$

Consequently, if W is a unimodular matrix, it must be the $n \times n$ unit matrix. In other words, if $\Lambda^* = \Lambda^\bullet$, then $U = V$. □

By studying the algebraic structures of the submodules, it can be shown (see [18]) that

$$f_n(m) = \sum_{d|m} d \cdot f_{n-1}(d). \tag{3.6}$$

In 1997, Baake [2] deduced from (3.6) that

$$f_n(m) = \sum_{d_1 d_2 \cdots d_n = m} d_1^0 d_2^1 \cdots d_n^{n-1}. \tag{3.7}$$

In fact, Baake's formula can be easily deduced from Lemmas 3.1 and 3.2. Gruber [10] did realise this connection and simplified (3.7). However, he neglected the fact that Lemma 3.2 needs a proof.

Theorem 3.3 (Baake [2], Gruber [10]). *If $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\ell^{\alpha_\ell}$, where the p_i are distinct prime numbers and the α_i are positive integers, then*

$$f_n(m) = \sum_{d_1 d_2 \cdots d_n = m} d_1^0 d_2^1 \cdots d_n^{n-1} = \prod_{i=1}^{\ell} \prod_{j=1}^{\alpha_i} \frac{p_i^{j+n-1} - 1}{p_i^j - 1} = \prod_{i=1}^{\ell} \prod_{j=1}^{n-1} \frac{p_i^{j+\alpha_i} - 1}{p_i^j - 1}.$$

Remark 3.4. Noticing that

$$(p_i^{j+n-1} - 1)/(p_i^j - 1) \le p_i^n \quad \text{and} \quad (p_i^{j+\alpha_i} - 1)/(p_i^j - 1) \ge p_i^{\alpha_i},$$

one can easily deduce that

$$m^{n-1} \le f_n(m) \le m^n.$$

Comparing with Theorem 2.2, it is interesting to see that Siegel's upper bound is far from the exact value of $f_n(m)$.

4. Classification of sublattices

Let Λ be an n-dimensional lattice in $\mathbb{E}^n$ and let Λ^* and $\Lambda^\bullet$ be two sublattices of Λ. We say that Λ^* and $\Lambda^\bullet$ are *equivalent* if there is a linear transformation σ satisfying both

$$\sigma(\Lambda) = \Lambda$$

and

$$\sigma(\Lambda^*) = \Lambda^\bullet.$$

Then, for convenience, we write $\Lambda^* \sim \Lambda^\bullet$. Clearly, a linear transformation σ satisfies $\sigma(\Lambda) = \Lambda$ if and only if σ corresponds to a unimodular matrix.

https://doi.org/10.1017/S0004972720000325 Published online by Cambridge University Press

EXAMPLE 4.1. Let $\Lambda = \mathbb{Z}^2$ with $\mathbf{e}_1 = (1, 0)$ and $\mathbf{e}_2 = (0, 1)$. Let Λ^* be the sublattice generated by $\mathbf{u}_1 = \mathbf{e}_1$ and $\mathbf{u}_2 = 2\mathbf{e}_2$ and let $\Lambda^\bullet$ be the sublattice generated by $\mathbf{u}_1 = 2\mathbf{e}_1$ and $\mathbf{u}_2 = \mathbf{e}_2$. It is obvious that $\Lambda^* \neq \Lambda^\bullet$. Let σ denote the linear transformation determined by $\sigma(\mathbf{e}_1) = \mathbf{e}_2$ and $\sigma(\mathbf{e}_2) = \mathbf{e}_1$; it can be verified that $\sigma(\Lambda) = \Lambda$ and $\sigma(\Lambda^*) = \Lambda^\bullet$. Thus, $\Lambda^* \sim \Lambda^\bullet$.

It is shown in Gruber [11] that, if Λ^* is a sublattice of Λ, then Λ has a basis $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$ and Λ^* has a basis $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ such that

$$\mathbf{u}_i = u_{ii}\mathbf{a}_i, \quad i = 1, 2, \ldots, n, \tag{4.1}$$

where the u_{ii} are positive integers.

From Martinet [16, page 26]: 'Let M be an R-module and let M' be a submodule of M, both having the same rank n. (When $R = \mathbb{Z}$, this amounts to saying that $[M : M'] < \infty$.) There then exist a basis $B = \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$ for M and nonzero elements $a_1, a_2, \ldots, a_n$ of R such that $B' = \{a_1\mathbf{e}_1, a_2\mathbf{e}_2, \ldots, a_n\mathbf{e}_n\}$ is a basis for M', and a_i divides a_{i-1} for $2 \leq i \leq n$.'. This implies that u_{ii} divides $u_{i-1,i-1}$ in (4.1).

For completeness, we restate this result next and give a detailed proof.

LEMMA 4.2. *If Λ^* is a sublattice of Λ, then Λ has a basis $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$ and Λ^* has a basis $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ such that*

$$\mathbf{u}_i = u_{ii}\mathbf{a}_i, \quad i = 1, 2, \ldots, n,$$

where all the u_{ii} are positive integers satisfying $u_{ii} \mid u_{i-1,i-1}$ for $2 \leq i \leq n$.

PROOF. Assume that $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n\}$ is a basis for Λ and $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ is a basis for Λ^*. Then

$$\mathbf{v}_i = v_{i1}\mathbf{e}_1 + v_{i2}\mathbf{e}_2 + \cdots + v_{in}\mathbf{e}_n, \quad i = 1, 2, \ldots, n. \tag{4.2}$$

For convenience, let $\overline{\mathbf{X}}$ denote the $n \times 1$ matrix with elements $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ and let X denote the $n \times n$ matrix with elements x_{ij}. Then one can rewrite (4.2) as

$$\overline{\mathbf{V}} = V\overline{\mathbf{E}}. \tag{4.3}$$

Suppose that $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ is another basis for Λ^* such that

$$\overline{\mathbf{V}} = U_1\overline{\mathbf{U}}, \tag{4.4}$$

where U_1 is an $n \times n$ unimodular matrix and $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$ is another basis for Λ such that

$$\overline{\mathbf{E}} = U_2\overline{\mathbf{A}}, \tag{4.5}$$

where U_2 is an $n \times n$ unimodular matrix. Then it follows by (4.3), (4.4) and (4.5) that

$$\overline{\mathbf{U}} = U_1^{-1}VU_2\overline{\mathbf{A}}. \tag{4.6}$$

https://doi.org/10.1017/S0004972720000325 Published online by Cambridge University Press

For a given integer matrix V there are unimodular matrices U_1 and U_2 such that

$$U_1^{-1} V U_2 = \begin{pmatrix} u_{11} & 0 & \cdots & 0 \\ 0 & u_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & u_{nn} \end{pmatrix},$$

where $u_{ii} \mid u_{i-1,i-1}$ for $2 \le i \le n$ (see, for example, [14, Ch. 14]). Then, by (4.6),

$$\mathbf{u}_i = u_{ii}\mathbf{a}_i, \quad i = 1, 2, \ldots, n.$$

The lemma is proved. □

Lemma 4.3. *Assume that Λ^* and $\Lambda^\bullet$ are two sublattices of an n-dimensional lattice Λ. If $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ is a basis of Λ^* and $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$ is a basis of Λ such that*

$$\mathbf{u}_i = u_{ii}\mathbf{a}_i, \quad i = 1, 2, \ldots, n,$$

where the u_{ii} are positive integers satisfying $u_{ii} \mid u_{i-1,i-1}$ for $2 \le i \le n$, and $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ is a basis of $\Lambda^\bullet$ and $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ is a basis of Λ such that

$$\mathbf{v}_i = v_{ii}\mathbf{b}_i, \quad i = 1, 2, \ldots, n,$$

where the v_{ii} are positive integers satisfying $v_{ii} \mid v_{i-1,i-1}$ for $2 \le i \le n$, then $\Lambda^* \sim \Lambda^\bullet$ if and only if

$$u_{ii} = v_{ii}, \quad i = 1, 2, \ldots, n.$$

Proof. Suppose that $u_{ii} = v_{ii}$ for $i = 1, 2, \ldots, n$. Let σ be the linear transformation defined by

$$\sigma(\mathbf{a}_i) = \mathbf{b}_i, \quad i = 1, 2, \ldots, n.$$

Then

$$\sigma(\mathbf{u}_i) = \sigma(u_{ii}\mathbf{a}_i) = u_{ii}\mathbf{b}_i = \mathbf{v}_i$$

for $i = 1, 2, \ldots, n$ and thus

$$\sigma(\Lambda^*) = \Lambda^\bullet.$$

On the other hand, if $\Lambda^* \sim \Lambda^\bullet$ with a suitable σ, then

$$\overline{\mathbf{U}} = U\overline{\mathbf{A}}, \tag{4.7}$$

$$\overline{\mathbf{V}} = V\overline{\mathbf{B}}, \tag{4.8}$$

$$\sigma\left(\overline{\mathbf{U}}\right) = W\overline{\mathbf{V}}, \tag{4.9}$$

$$\sigma\left(\overline{\mathbf{A}}\right) = T\overline{\mathbf{B}}, \tag{4.10}$$

where $u_{ij} = 0$ for $i \ne j$, $v_{ij} = 0$ for $i \ne j$ and both W and T are unimodular matrices.

It follows from $\sigma(\Lambda^*) = \Lambda^\bullet$, (4.7), (4.8), (4.9) and (4.10) that

$$\sigma\left(\overline{\mathbf{U}}\right) = U\sigma\left(\overline{\mathbf{A}}\right),$$

$$W\overline{\mathbf{V}} = UT\overline{B},$$

$$\overline{\mathbf{V}} = W^{-1}UT\overline{\mathbf{B}} = V\overline{\mathbf{B}}$$

https://doi.org/10.1017/S0004972720000325 Published online by Cambridge University Press

and thus

$$V = W^{-1}UT. \tag{4.11}$$

But (4.11) implies that $V = U$ (see [14, Ch. 14]) and Lemma 4.3 is proved. □

Proof of Theorem 1.2. Recall that

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\ell^{\alpha_\ell},$$

where the p_i are distinct prime numbers. It follows from Lemmas 4.2 and 4.3 that $g_n(m)$ is the number of the factorisations

$$m = d_1 d_2 \cdots d_n \tag{4.12}$$

satisfying $d_j \mid d_{j-1}$ for $2 \le j \le n$. If

$$d_j = p_1^{\beta_{1j}} p_2^{\beta_{2j}} \dots p_\ell^{\beta_{\ell j}},$$

then

$$\begin{cases} \sum_{j=1}^{n} \beta_{ij} = \alpha_i, \\ \beta_{i1} \ge \beta_{i2} \ge \cdots \ge \beta_{in} \ge 0 \end{cases} \tag{4.13}$$

for $i = 1, 2, \dots, \ell$. Clearly, (4.13) has $p_n(\alpha_i)$ solutions and (4.12) has exactly $\prod p_n(\alpha_i)$ factorisations. Thus,

$$g_n(m) = \prod_{i=1}^{\ell} p_n(\alpha_i).$$

Theorem 1.2 is proved. □

Proof of Corollary 1.3. It is well known (see [1]) that

$$p_n(k) \sim \frac{k^{n-1}}{n!(n-1)!}.$$

Corollary 1.3 follows immediately from Theorem 1.2. □

Remark 4.4. Assume that Λ is an n-dimensional lattice with a basis $\{\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n\}$. When $m = p_1 p_2 \cdots p_\ell$, where p_1, p_2, …, p_ℓ are distinct primes,

$$f_n(m) = \prod_{i=1}^{\ell} \sum_{j=0}^{n-1} p_i^j$$

and

$$g_n(m) = 1.$$

That is, all the $f_n(m)$ sublattices of index m are equivalent to each other under unimodular transformations. In particular, all of them are equivalent to the sublattice with a basis $\{m\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n\}$.

REMARK 4.5. It is interesting to compare the values of $f_n(m)$ and $g_n(m)$ for small n and m.

m	2	3	4	5	6	7	8	9	10	11	12	13
$f_2(m)$	3	4	7	6	12	8	15	13	18	12	28	14
$f_3(m)$	7	13	35	31	91	57	155	130	217	133	455	183
$g_2(m)$	1	1	2	1	1	1	2	2	1	1	2	1
$g_3(m)$	1	1	2	1	1	1	3	2	1	1	2	1

Acknowledgements

I am grateful to M. Baake, M. Henk, C. Voll and the referee for their helpful comments and suggestions.

References

[1] G. E. Andrews and K. Eriksson, *Integer Partitions* (Cambridge University Press, Cambridge, 2004).
[2] M. Baake, 'Solution of the coincidence problem in dimensions $d \leq 4$', in: *The Mathematics of Long-Range Aperiodic Order* (ed. R. V. Moody) (Kluwer, Dordrecht, 1997), 9–44.
[3] M. Baake, R. Scharlau and P. Zeiner, 'Similar sublattices of planar lattices', *Canad. J. Math.* **63** (2011), 1220–1237.
[4] M. Baake, R. Scharlau and P. Zeiner, 'Well-rounded sublattices of planar lattices', *Acta Arith.* **166** (2014), 301–334.
[5] M. Bernstein, N. J. A. Sloane and P. E. Wright, 'On sublattices of the hexagonal lattice', *Discrete Math.* **170** (1997), 29–39.
[6] J. W. S. Cassels, *An Introduction to the Geometry of Numbers* (Springer, Berlin, 1959).
[7] L. Fukshansky, 'On distribution of well-rounded sublattices of $\mathbb{Z}^2$', *J. Number Theory* **128** (2008), 2359–2393.
[8] L. Fukshansky, 'On similarity classes of well-rounded sublattices of $\mathbb{Z}^2$', *J. Number Theory* **129** (2009), 2530–2556.
[9] D. Goldfeld, A. Lubotzky and L. Pyber, 'Counting congruence subgroups', *Acta Math.* **193** (2004), 73–104.
[10] B. Gruber, 'Alternative formulae for the number of sublattices', *Acta Crystallogr. Sect. A* **53** (1997), 807–808.
[11] P. M. Gruber, *Convex and Discrete Geometry* (Springer, New York, 2007).
[12] P. M. Gruber and C. G. Lekkerkerker, *Geometry of Numbers* (North-Holland, Amsterdam, 1987).
[13] F. J. Grunewald, D. Segal and G. C. Smith, 'Subgroups of finite index in nilpotent groups', *Invent. Math.* **93** (1988), 185–223.
[14] L. K. Hua, *Introduction to Number Theory* (Springer, Berlin–Heidelberg, 1987).
[15] A. Lubotzky and D. Segal, *Subgroup Growth*, Progress in Mathematics, 212 (Birkhäuser, Basel, 2003).
[16] J. Martinet, *Perfect Lattices in Euclidean Spaces* (Springer, Berlin, 2003).
[17] H. Minkowski, *Diophantische Approximationen* (Chelsea, New York, 1957; Teubner, Leipzig, 1907).
[18] G. Scheja and U. Storch, *Lehrbuch der Algebra*, Teil 2 (Teubner, Stuttgart, 1988).
[19] W. M. Schmidt, 'The distribution of the sublattices of $\mathbb{Z}^n$', *Monatsh. Math.* **125** (1998), 37–81.
[20] W. M. Schmidt, 'Integer matrices, sublattices of $\mathbb{Z}^n$, and Frobenius numbers', *Monatsh. Math.* **178** (2015), 405–451.

[21] J.-P. Serre, *A Course in Arithmetic* (Springer, New York, 1973).
[22] C. L. Siegel, *Lectures on the Geometry of Numbers* (Springer, Berlin, 1989).

CHUANMING ZONG, Center for Applied Mathematics,
Tianjin University, Tianjin 300072, China
e-mail: cmzong@math.pku.edu.cn

https://doi.org/10.1017/S0004972720000325 Published online by Cambridge University Press