Classification of the sublattices of a lattice

Chuanming Zong

Abstract. In 1945-46, 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. This paper presents a systematic treatment for counting the sublattices and deduces a formula for the number of the sublattice classes of determinant $m\cdot\det(\Lambda)$.

2010 Mathematics Subject Classification: 52C05, 52C07, 11H06.

1. Introduction

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

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

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

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

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

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

where P is the parallelopiped defined by

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

A subset Λ^* of Λ is called its *sublattice* if itself is an n-dimensional lattice as well. If $\{\mathbf{b}_1,\mathbf{b}_2,\ldots,\mathbf{b}_n\}$ is a basis of Λ^*, where $\mathbf{b_i}=(b_{i1},b_{i2},\ldots,b_{in})$, then we have

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

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 we get

$$B=DA$$

and therefore

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

where m is the absolute value of the determinant of D. Usually, we call m the *index* of Λ^* in Λ.

The structures and representations of the sublattices have been studied by many authors such as Minkowski, Siegel, Cassels, Hlawka, Rogers and Schmidt. Many results and their applications can be found in classic references such as [4, 8, 9, 12, 16]. Particular sublattices have been studied by [3, 5, 6, 14, 15].

Let Λ be an n-dimensional lattice, let m be a positive integer, let $f_n(m)$ denote the number of the different sublattices of Λ with index m, and let $f^*_n(m)$ denote the number of the different sublattice classes of Λ with index m.

In 1945-46, C. L. Siegel gave a series of lectures on Geometry of Numbers at New York University. His lecture notes [16] contained the first upper bound for $f_n(m)$, namely

$$f_n(m)\le m^{n^2}. \tag{1}$$

Since the lecture notes was published only in 1989, this result and many others were neglected. In 1959, J. W. S. Cassels [4] presented some basic result about the structures of the bases of the sublattices. In 1997, M. Baake [2] deduced the following formula based on a recursion in Algebra

$$f_n(m) = \sum_{d_1 d_2 \ldots d_n = m} d_1^0 d_2^1 \ldots d_n^{n-1}. \tag{2}$$

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

$$m = p_1^{\alpha_1} \ldots p_\ell^{\alpha_\ell}, \tag{3}$$

where p_i are prime numbers. Baake's formula was simplified by B. Gruber [7] as

$$f_n(m) = \prod_{i=1}^{\ell} \prod_{j=1}^{\alpha_\ell} \frac{p_i^{j+n-1} - 1}{p_i^j - 1} = \prod_{i=1}^{\ell} \prod_{j=1}^{n-1} \frac{p_i^{j+\alpha_i} - 1}{p_i^j - 1}. \tag{4}$$

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

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

and

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

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

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

The purpose of this paper is to present a systematic treatment on this topic, to complete both the statement and the proof. First, we present detailed proofs for (2) and (4). Then, we prove the following classification theorem.

Theorem Z. *If $m = p_1^{\alpha_1} \ldots p_\ell^{\alpha_\ell}$, where p_i are prime numbers, then we have*

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

Remark 1. *When $m = p_1 p_2 \ldots p_\ell$, where p_1, p_2, …, p_ℓ are pairwise distinct primes, we have*

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

and

$$f_n^*(m) = 1.$$

Then, all the sublattices of index m are equivalent to each others under unimodular transformations.

2. C. L. Siegel's Upper Bound

Siegel's upper bound (1) was obtained in 1945-46. However, it was published only in 1989 in his lecture notes by Chandrasekharan [16]. So, this beautiful result has been neglected by almost all authors on related topics. 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.

Lemma 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 linear independent vectors in $\mathbb{E}^n$ with*

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

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 1 (Siegel [16]). *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. In other words, we have*

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

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 we have

$$\mathbf{u}_i = u_{i1}\mathbf{a}_1 + u_{i2}\mathbf{a}_2 + \ldots + u_{in}\mathbf{a}_n, \quad i = 1, 2, \ldots, n, \tag{5}$$

where all 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 we have

$$\mathbf{v}_i = v_{i1}\mathbf{a}_1 + v_{i2}\mathbf{a}_2 + \ldots + v_{in}\mathbf{a}_n, \quad i = 1, 2, \ldots, n, \tag{6}$$

where all v_{ij} are integers and $\det(v_{ij}) = \pm m$. We denote the $n \times n$ matrix (v_{ij}) by V.

Clearly, it follows by (5) and (6) that 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 $W = UV^{-1} = (w_{ij})$, we have

$$\mathbf{u}_i = w_{i1}\mathbf{v}_1 + w_{i2}\mathbf{v}_2 + \ldots + w_{in}\mathbf{v}_n, \quad i = 1, 2, \ldots, n. \tag{7}$$

Now, we proceed to show that if

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

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

$$mW = mUV^{-1} \equiv mVV^{-1} \equiv mE \equiv O \pmod{m}, \tag{8}$$

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, we have

$$\det(W) = \det(UV^{-1}) = \pm\frac{m}{m} = \pm 1. \tag{9}$$

Thus, W must be a unimodular matrix. Then it follows by Lemma 1 that 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,

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

The theorem is proved. □

3. The Sublattices of Given Index

In 1907, Minkowski [12] studied the relation between the bases of a three-dimensional lattice and its sublattices. Afterwards, his result was generalized into arbitrary dimensions (see [4] or [8]) as following. Assume that Λ^* is a sublattice of an n-dimensional Λ. If $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$ is a basis of Λ^*, then Λ has a basis $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$ satisfying

$$\mathbf{u}_i = u_{i1}\mathbf{a}_1 + u_{i2}\mathbf{a}_2 + \ldots + u_{ii}\mathbf{a}_i, \quad i = 1, 2, \ldots, n, \tag{10}$$

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

It is rather unexpected that the following inverse of this result is also true. It can be found in both [4] and [8], neither of them indicated further reference.

Lemma 2 (Cassels [4]). *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*

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

and

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

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

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

Lemma 3. *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*

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

and

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

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

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

and

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

where all 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* $\{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n\}$*, and let* $\Lambda^\bullet$ *be the sublattice of* Λ *generated by* $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$*. Then the two sublattices* Λ^* *and* $\Lambda^\bullet$ *are identical if and only if*

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

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}, $i, j = 1, 2, \dots, n$, where $u_{ij} = 0$ for all $j > i$, let V denote the $n \times n$ matrix with elements v_{ij}, $i, j = 1, 2, \dots, n$, where $v_{ij} = 0$ for all $j > i$, and define

$$W = UV^{-1} = (w_{ij})\,. \tag{11}$$

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

By (11) we have

$$WV = U. \tag{12}$$

Then, by comparing both sides of (12) for u_{1n}, $u_{1,n-1}$, …, u_{11}, we get

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

and thus

$$\begin{cases} w_{1n} = w_{1,n-1} = \dots = w_{12} = 0, \\ w_{11}v_{11} = u_{11}. \end{cases} \tag{13}$$

Repeating this process for u_{2i}, u_{3i}, …, u_{ni} successively, we get

$$\begin{cases} w_{ij} = 0, \quad i < j \le n, \\ w_{ii}v_{ii} = u_{ii}, \quad i = 1, 2, \dots, n. \end{cases} \tag{14}$$

If W is a unimodular matrix, all its elements are integers, it follows by (14) and the assumption

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

that

$$w_{11} = w_{22} = \dots = w_{nn} = 1. \tag{15}$$

Then, by comparing both sides of (12) for u_{21}, u_{32}, …, $u_{n,n-1}$, we get

$$w_{i+1,i}v_{ii} + v_{i+1,i} = u_{i+1,i}, \qquad i = 1, 2, \dots, n-1. \tag{16}$$

If $w_{i+1,i} \ne 0$, by (16) we get

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

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, we must have

$$\begin{cases} w_{i+1,i} = 0, \\ u_{i+1,i} = v_{i+1,i} \end{cases} \tag{17}$$

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

Inductively, assume that

$$w_{i+j,i} = 0 \tag{18}$$

holds for all $1 \le j \le k-1 < n-1$ and $i = 1, 2, \dots, n-j$, by comparing both sides of (12) for $u_{i+k,i}$, $i = 1, 2, \dots, n-k$, similar to (16) we can get

$$w_{i+k,i} = 0, \quad i = 1, 2, \dots, n-k. \tag{19}$$

As a conclusion, we obtain that, if W is a unimodular matrix, it must be the $n \times n$ unit matrix. In other words, if $\Lambda^* = \Lambda^\bullet$, then $U = V$. The theorem is proved. $\square$

Clearly, an n-dimensional lattice is a free module of rank n over $\mathbb{Z}$. By studying the algebraic structures of the submodules it was shown (see [13]) that

$$f_n(m) = \sum_{d|m} d \cdot f_{n-1}(d). \tag{20}$$

In 1997, it was deduced from (20) by Baake [2] that

$$f_n(m) = \sum_{d_1 d_2 \dots d_n = m} d_1^0 d_2^1 \dots d_n^{n-1}. \tag{21}$$

In fact, Baake's formula can be easily deduced from Lemma 2 and Lemma 3. Gruber [7] did realize this possible connection and simplified (21). However, he neglected the necessity of Lemma 3.

Theorem 2 (Baake [2]**, Gruber** [7]**).** *If $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\ell^{\alpha_\ell}$, where p_i are prime numbers and α_i are positive integers, then*

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

Remark 2. Noticing that

$$\left(p_i^{j+n-1} - 1\right) / \left(p_i^j - 1\right) \le p_i^n$$

and

$$\left(p_i^{j+\alpha_i} - 1\right) / \left(p_i^j - 1\right) \ge p_i^{\alpha_i},$$

one can easily deduce that

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

Comparing with Theorem 1, it is interesting to see that Siegel's upper bound is far away from the exact values of $f_n(m)$.

4. Classification of the Sublattices of Given Index

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

$$\sigma(\Lambda) = \Lambda \tag{22}$$

and

$$\sigma(\Lambda^*) = \Lambda^\bullet. \tag{23}$$

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

Example 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, we have $\Lambda^* \sim \Lambda^\bullet$.

It is shown in Gruber [8] that, if Λ^* is a sublattice of Λ, then Λ has a basis $\{\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n\}$ and Λ^* has a basis $\{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n\}$ such that

$$\mathbf{u}_i = u_{ii} \mathbf{a}_i, \quad i = 1, 2, \dots, n, \tag{24}$$

where u_{ii} are suitable positive integers.

On page 26 of [11], Martinet wrote "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 exists a basis $B = \{\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n\}$ for M and nonzero elements a_1, a_2, …, a_n of R such that $B' = \{a_1\mathbf{e}_1, a_2\mathbf{e}_2, \dots, a_n\mathbf{e}_n\}$ is a basis for M', and a_i divides a_{i-1} for $2 \le i \le n$." This implies that u_{ii} divides $u_{i-1,i-1}$ in (24).

For the completeness, we restate this result as Lemma 4 in the following and give a detailed proof.

Lemma 4. *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 u_{ii} are positive integers satisfying $u_{ii} \mid u_{i-1,i-1}$ for all $2 \le i \le n$.

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, we have

$$\mathbf{v}_i = v_{i1}\mathbf{e}_1 + v_{i2}\mathbf{e}_2 + \ldots + v_{in}\mathbf{e}_n, \quad i = 1, 2, \ldots, n. \tag{25}$$

For convenience, let $\overline{\mathbf{X}}$ denote the $n \times 1$ matrix with elements $\mathbf{x}_1$, $\mathbf{x}_2$, ..., $\mathbf{x}_n$ and let X denote the $n \times n$ matrix with elements x_{ij}. Then, one can rewrite (25) as

$$\overline{\mathbf{V}} = V\overline{\mathbf{E}}. \tag{26}$$

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

$$\overline{\mathbf{V}} = U_1\overline{\mathbf{U}}, \tag{27}$$

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

$$\overline{\mathbf{E}} = U_2\overline{\mathbf{A}}, \tag{28}$$

where U_2 is an $n \times n$ unimodular matrix. Then, it follows by (26), (27) and (28) that

$$\overline{\mathbf{U}} = U_1^{-1}VU_2\overline{\mathbf{A}}. \tag{29}$$

It is known in Algebra (see Chapter 14 of Hua [10]) that, for a given integer matrix V there are two suitable unimodular matrices U_1 and U_2 such that

$$U_1^{-1}VU_2 = \begin{pmatrix} u_{11} & 0 & \ldots & 0 \\ 0 & u_{22} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & u_{nn} \end{pmatrix},$$

where $u_{ii} \mid u_{i-1,i-1}$ for all $2 \le i \le n$. Then, by (29) we have

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

The lemma is proved. □

Lemma 5. *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 u_{ii} are positive integers satisfying $u_{ii} \mid u_{i-1,i-1}$ for all $2 \le i \le n$, 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 v_{ii} are positive integers satisfying $v_{ii} \mid v_{i-1,i-1}$ for all $2 \le i \le n$. Then, $\Lambda^* \sim \Lambda^\bullet$ if and only if

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

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

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

then we have

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

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

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

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

$$\overline{\mathbf{U}} = U\overline{\mathbf{A}}, \tag{30}$$

$$\overline{\mathbf{V}} = V\overline{\mathbf{B}}, \tag{31}$$

$$\sigma\left(\overline{\mathbf{U}}\right) = W\overline{\mathbf{V}} \tag{32}$$

and

$$\sigma\left(\overline{\mathbf{A}}\right) = T\overline{\mathbf{B}}, \tag{33}$$

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

It follows by $\sigma(\Lambda^*) = \Lambda^\bullet$, (30), (31), (32) and (33) that

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

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

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

and thus

$$V = W^{-1}UT. \tag{34}$$

It is known in Algebra (see Chapter 14 of Hua [10]) that (34) implies

$$V = U.$$

Lemma 5 is proved. □

Proof of Theorem Z. Recall that

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

where p_i are prime numbers. It follows by Lemma 4 and Lemma 5 that $f_n^*(m)$ is the number of the factorizations

$$m = d_1 d_2 \ldots d_n \tag{35}$$

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

$$d_j = p_1^{\beta_{1j}} p_2^{\beta_{2j}} \ldots p_\ell^{\beta_{\ell j}}, \tag{36}$$

then we have

$$\begin{cases} \sum_{j=1}^n \beta_{ij} = \alpha_i, \\ \beta_{i1} \geq \beta_{i2} \geq \ldots \geq \beta_{in} \geq 0 \end{cases} \tag{37}$$

for all $i = 1, 2, \ldots, \ell$. Clearly (37) has $p_n(\alpha_i)$ solutions and each solution corresponds to one factorization of (35). Thus, we have

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

Theorem Z is proved. □

Remark 3. The partition function $p_n(k)$ has been studied by many authors. See Andrews and Eriksson [1] for references.

Acknowledgements. For helpful correspondence, the author is grateful to Prof. Baake. This work is supported by 973 Program 2013CB834201.

References

1. G. E. Andrews and K. Eriksson, *Integer Partitions*, Cambridge University Press, 2004.
2. M. Baake, Solution of the coincidence problem in dimensions $d \le 4$, *The Mathematics of Long-Range Aperiodic Order*, edited by R. V. Moody, 1997, 9-44. Dordrecht, Kluwer Academic Publishers. arXiv:math/0605222.
3. M. Bernstein, N. J. A. Sloane, P. E. Wright, On sublattices of the hexagonal lattice, *Discrete Math.* **170** (1997), 29-39.
4. J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer-Verlag, Berlin, 1959.
5. L. Fukshansky, On distribution of well-rounded sublattices of $\mathbb{Z}^2$, *J. Number Theory*, **128** (2008), 2359-2393.
6. L. Fukshansky, On similarity classes of well-rounded sublattices of $\mathbb{Z}^2$, *J. Number Theory*, **129** (2009), 2530-2556.
7. B. Gruber, Alternative formulae for the number of sublattices, *Acta Cryst.* **A53** (1997), 807-808.
8. P. M. Gruber, *Convex and Discrete Geometry*, Springer-Verlag, New York, 2007.
9. P. M. Gruber and C. G. Lekkerkerker, *Geometry of Numbers*, North-Holland, Amsterdam, 1987.
10. L. K. Hua, *Introduction to Number Theory*, Springer, 1987.
11. J. Martinet, *Perfect Lattices in Euclidean Spaces*, Springer-Verlag, Berlin, 2003.
12. H. Minkowski, *Diophantische Approximationen*, Teubner, Leipzig, 1907; Chelsea, New York, 1957.
13. G. Scheja and U. Storch, *Lehrbuch der Algebra*, Teil 2, Teubner, Stuttgart, 1988.
14. W. M. Schmidt, The distribution of the sublattices of $\mathbb{Z}^n$, *Monatsh. Math.* **125** (1998), 37-81.
15. W. M. Schmidt, Integer matrices, sublattices of $\mathbb{Z}^n$, and Frobenius numbers, *Monatsh. Math.* **178** (2015), 405-451.
16. C. L. Siegel, *Lectures on the Geometry of Numbers*, Springer-Verlag, Berlin, 1989.

Chuanming Zong, Center for Applied Mathematics, Tianjin University, Tianjin 300072, China
Email: cmzong@math.pku.edu.cn