Journal of Number Theory 132 (2012) 371–378

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On a property of 2-dimensional integral Euclidean lattices

Eiichi Bannai [a], Tsuyoshi Miezaki [b,*]

[a] Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai 200240, China
[b] Oita National College of Technology, 1666 Oaza-Maki, Oita 870-0152, Japan

ARTICLE INFO

Article history:
Received 25 January 2011
Revised 28 April 2011
Accepted 5 July 2011
Available online 18 November 2011
Communicated by D. Zagier

MSC:
primary 05E99
secondary 11R04

Keywords:
Quadratic fields
Lattices

ABSTRACT

Let Λ be any integral lattice in the 2-dimensional Euclidean space. Generalizing the earlier works of Hiroshi Maehara and others, we prove that for every integer $n > 0$, there is a circle in the plane $\mathbb{R}^2$ that passes through exactly n points of Λ.

1. Introduction

We consider the following condition on 2-dimensional lattices $\Lambda \subset \mathbb{R}^2$.

Definition 1.1. If there is a circle in the plane $\mathbb{R}^2$ that passes through exactly n points of Λ for every integer $n > 0$, then Λ is called universally concyclic.

A lattice generated by $(a,b), (c,d) \in \mathbb{R}^2$, $(ad - bc \neq 0)$ is denoted by $\Lambda[(a,b),(c,d)]$. In [3], Maehara introduced the term "universally concyclic". Then, he and others showed the following results. In [5] and [4], Schinzel, Maehara and Matsumoto proved that $\mathbb{Z}^2$, that is, $\Lambda[(1,0),(0,1)]$ is universally concyclic. Moreover let $a,b,c,d \in \mathbb{Z}$ be such that $q := ad - bc$ is a prime and $q \equiv 3 \pmod 4$. Then $\Lambda[(a,b),(c,d)]$ is universally concyclic. The equilateral triangular lattice $\Lambda[(1,0),(-1/2,\sqrt{-3}/2)]$ and rectangular lattice $\Lambda[(1,0),(0,\sqrt{-3})]$ are universally concyclic.

* Corresponding author. Fax: +81 22 795 4654.
E-mail addresses: bannai@sjtu.edu.cn (E. Bannai), miezaki@oita-ct.ac.jp (T. Miezaki).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2011.07.011

Let $\mathbb{Z}[x] := \{a + bx \mid a, b \in \mathbb{Z}\}$. We remark that for a positive integer d, a lattice $\Lambda[(1,0),(a,b\sqrt{d})]$ is also given by $\mathbb{Z}[a + b\sqrt{-d}]$ in the complex plane. We define the set $A(k)$ as follows:

$$A(k) := \{z \in \mathbb{Z}[\sqrt{-3}] \mid |z|^2 = 7^k\}.$$

In [3], Maehara proved the following result:

Lemma 1.1. *(Cf. [3].)* $\sharp A(k) = 2(k+1)$.

Then, Maehara [3] proposed the following problems:

Problem 1.1. (Cf. [3].) For every square-free integer $d > 1$ and a prime p such that $p = x^2 + y^2 d$, we have $\sharp\{z \in \mathbb{Z}[\sqrt{-d}] \mid |z|^2 = p^k\} \geqslant 2(k+1)$ for every k. Does equality always hold?

Problem 1.2. (Cf. [3].) Is $\Lambda[(a,b),(c,d)]$ universally concyclic if $a, b, c, d \in \mathbb{Z}$ and $ad - bc \neq 0$?

Here, we answer Problems 1.1 and 1.2 affirmatively. In fact, we prove a slightly stronger assertion in Theorems 1.1 and 1.2 below. Let d be a square-free positive integer and K be the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$. We define $\mathcal{O}_K$ as the integer ring of K. Let $\mathbb{Z} \cdot a + \mathbb{Z} \cdot b$ denote the linear combination of a and b with integer coefficients. Then $\mathcal{O}_K$ will be written as follows:

$$\mathcal{O}_K = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot w_K, \tag{1}$$

where

$$w_K = \begin{cases} \sqrt{-d} & \text{if } -d \equiv 2, 3 \pmod 4, \\ \frac{-1+\sqrt{-d}}{2} & \text{if } -d \equiv 1 \pmod 4). \end{cases} \tag{2}$$

We denote by d_K the discriminant of K:

$$d_K = \begin{cases} -4d & \text{if } -d \equiv 2, 3 \pmod 4, \\ -d & \text{if } -d \equiv 1 \pmod 4). \end{cases}$$

We review the concept of order in a quadratic field (for more details, see [2]). An order $\mathcal{O}$ in a quadratic field K is a subset $\mathcal{O} \subset K$ such that

1. $\mathcal{O}$ is a subring of K containing 1.
2. $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module.
3. $\mathcal{O}$ contains a $\mathbb{Q}$-basis of K.

We can now describe all orders in a quadratic fields:

Lemma 1.2. *(Cf. [2, p. 133].) Let $\mathcal{O}$ be an order in a quadratic field K of discriminant d_K. Then $\mathcal{O}$ has a finite index in $\mathcal{O}_K$, and if we set $f = [\mathcal{O}_K : \mathcal{O}]$, then*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot f w_K, \tag{3}$$

where w_K is as in (2). Here f is called a conductor of the order $\mathcal{O}$.

We denote $\mathcal{O}$ by $\mathcal{O}_f$ if $f = [\mathcal{O}_K : \mathcal{O}]$. Now, we introduce the concept of proper ideals of an order. For any ideal $\mathfrak{a}$ of $\mathcal{O}_f$, notice that

$$\mathcal{O}_f \subset \{\beta \in K \mid \beta\mathfrak{a} \subset \mathfrak{a}\}$$

since $\mathfrak{a}$ is an ideal of $\mathcal{O}_f$. We say that an ideal $\mathfrak{a}$ of $\mathcal{O}_f$ is proper whenever equality holds, i.e., when

$$\mathcal{O}_f = \{\beta \in K \mid \beta\mathfrak{a} \subset \mathfrak{a}\}.$$

A quadratic form F is called integral if all the coefficients of F are rational integers. A lattice Λ is called integral if $(x, y) \in \mathbb{Z}$ for all $x, y \in \Lambda$, where (x, y) is the standard inner product. Generally, it is well known that there exists a one-to-one correspondence between the set of proper ideal classes of the order $\mathcal{O}_f$ and the equivalence class of primitive positive definite integral quadratic forms $F(x, y)$ with discriminant $f^2 d_K < 0$ (see Theorem 2.2 in Section 2 [1, Chapter 2, §7-6], [6, §11]). Hence, we consider the proper ideal classes of $\mathcal{O}_f$ to be the lattice in $\mathbb{R}^2$ corresponding to a quadratic forms $F(x, y)$. On the other hand, any 2-dimensional integral Euclidean lattice can be considered as some proper ideal class of $\mathcal{O}_f$. We define Λ as the proper ideal classes of $\mathcal{O}_f$. Then, we prove the following theorems:

Theorem 1.1. *Let $n \in \mathbb{N}$ and assume that $n \neq 1$. Let p be a prime number such that there exists a $z \in \mathbb{Z}[\sqrt{-n}\,]$ with $|z|^2 = p$, $(\frac{d_K}{p}) = 1$ and $(p, f) = 1$, where $(\frac{\cdot}{\cdot})$ is the Legendre symbol. Then,*

$$\sharp\left\{z \in \mathbb{Z}[\sqrt{-n}\,] \;\middle|\; |z|^2 = p^k\right\} = 2(k+1).$$

Theorem 1.2. *All the 2-dimensional integral lattices in $\mathbb{R}^2$ are universally concyclic.*

Remark 1.1. We remark that there exist some non-integral lattices which are not universally concyclic. Maehara also proved in [3] that if τ is a transcendental number, then $\Lambda[(1, \tau), (0, 1)]$ cannot contain four concyclic points, hence is not universally concyclic. The rectangular lattice $\Lambda[(\alpha, 0), (0, \beta)]$ does not contain five concyclic points if and only if $(\alpha/\beta)^2$ is an irrational number. Hence, some additional integrality conditions are necessary to ensure this property.

2. Preliminaries

In this paper, we consider the 2-dimensional integral Euclidean lattices. We shall always assume that d denotes a positive square-free integer. Let $K = \mathbb{Q}(\sqrt{-d}\,)$ be an imaginary quadratic field, and let $\mathcal{O}_K$ be its ring of algebraic integers defined by (1). As we mentioned in Section 1, there exists a one-to-one correspondence between the set of fractional ideal classes of the unique quadratic field $\mathbb{Q}(\sqrt{-d}\,)$ and the equivalence class of primitive positive definite integral quadratic forms $F(x, y)$ with discriminant $d_K < 0$ [6, §10]. More generally, there exists a one-to-one correspondence between the set of fractional proper ideal classes of order $\mathcal{O}_f$ and the equivalence class of primitive positive definite integral quadratic forms $F(x, y)$ with discriminant $f^2 d_K < 0$ [1, Chapter 2, §7-6], [6, §11]. We remark that the value $f^2 d_K$ is called the discriminant of the order $\mathcal{O}_f$. Finally, we give the well-known theorems needed later.

Theorem 2.1. *(Cf. [2, p. 104].) We can classify prime ideals of a quadratic field as follows*:

1. *If p is an odd prime and $(\frac{d_K}{p}) = 1$ (resp. $d_K \equiv 1 \pmod 8$) then*

$$(p) = \mathfrak{p}\mathfrak{p}' \quad \big(\textit{resp. } (2) = \mathfrak{p}\mathfrak{p}'\big),$$

where $\mathfrak{p}$ and $\mathfrak{p}'$ are prime ideals with $\mathfrak{p} \neq \mathfrak{p}'$, $N(\mathfrak{p}) = N(\mathfrak{p}') = p$ (resp. $N(\mathfrak{p}) = 2$).

2. *If p is an odd prime and $(\frac{d_K}{p}) = -1$ (resp. $d_K \equiv 5 \pmod 8$) then*

$$(p) = \mathfrak{p} \quad \bigl(\textit{resp. } (2) = \mathfrak{p}\bigr),$$

where $\mathfrak{p}$ is a prime ideal with $N(\mathfrak{p}) = p^2$ (resp. $N(\mathfrak{p}) = 4$).

3. *If $p \mid d_k$ then*

$$(p) = \mathfrak{p}^2,$$

where $\mathfrak{p}$ is a prime ideal with $N(\mathfrak{p}) = p$.

Theorem 2.2. *(Cf. [2, Theorem 7.7].) Let $\mathcal{O}$ be an order of discriminant D in an imaginary quadratic field K.*

1. *If $F(x, y) = ax^2 + bxy + cy^2$ is a primitive positive definite integral quadratic form of discriminant D, then $[a, (-b + \sqrt{D})/2]$ is a proper ideal of $\mathcal{O}$.*
2. *The map sending $F(x, y)$ to $[a, (-b + \sqrt{D})/2]$ induces an isomorphism between the form class group and the ideal class group.*
3. *A positive integer m is represented by a form $F(x, y)$ if and only if m is the norm $N(\mathfrak{a})$ of some ideal $\mathfrak{a}$ in the corresponding ideal class mentioned in 2.*

Lemma 2.1. *(Cf. [2, Lemma 7.18].) Let $\mathcal{O}_f$ be an order of conductor f. We say that a non-zero $\mathcal{O}_f$-ideal $\mathfrak{a}$ is prime to f provided that $\mathfrak{a} + f\mathcal{O}_f = \mathcal{O}_f$.*

1. *An $\mathcal{O}_f$-ideal $\mathfrak{a}$ is prime to f if and only if its norm $N(\mathfrak{a})$ is relatively prime to f.*
2. *Every $\mathcal{O}_f$-ideal prime to f is proper.*

Proposition 2.1. *(Cf. [2, Proposition 7.20].) Let $\mathcal{O}_f$ be an order of conductor f in an imaginary quadratic field K. We say that a non-zero $\mathcal{O}_K$-ideal $\mathfrak{a}$ is prime to f provided that $\mathfrak{a} + f\mathcal{O}_K = \mathcal{O}_K$. If $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal prime to f, then $\mathfrak{a} \cap \mathcal{O}_f$ is an $\mathcal{O}_f$-ideal prime to f of the same norm.*

Proposition 2.2. *(Cf. [2, Exercise 7.26].) Let $\mathcal{O}_f$ be an order of conductor f. Then $\mathcal{O}_f$-ideals prime to the conductor can be factored uniquely into prime $\mathcal{O}_f$-ideals (which are also prime to f).*

Theorem 2.3. *(Cf. [2, Theorem 9.4].) Let $n > 0$ be an integer, and L be the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$ in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-n})$. If p is an odd prime not dividing n, then*

$$p = x^2 + ny^2 \quad \Leftrightarrow \quad p \textit{ splits completely in } L.$$

3. Proof of Theorem 1.1

Proof of Theorem 1.1. We remark that $\mathbb{Z}[\sqrt{-n}]$ can be considered as the order $\mathbb{Z}[\sqrt{-n}] = \mathcal{O}_f \subset K = \mathbb{Q}(\sqrt{-d})$ for some f and d with the following condition $-4n = f^2 d_K$, namely,

$$n = \begin{cases} f^2 d & \text{if } -d \equiv 2, 3 \pmod 4, \\ \frac{f^2 d}{4} & \text{if } -d \equiv 1 \pmod 4. \end{cases}$$

Therefore, we remark that $\mathbb{Z}[\sqrt{-n}] = \mathcal{O}_f$.

We fix a prime p such that there exists a $z \in \mathbb{Z}[\sqrt{-n}]$ with $|z|^2 = p$, $(\frac{d_K}{p}) = 1$ and $(p, f) = 1$. Because of Theorem 2.1, $(p) = \mathfrak{p}\mathfrak{p}'$ in $\mathcal{O}_K$ for some $\mathfrak{p}$. Moreover, the condition $z \in \mathbb{Z}[\sqrt{-n}]$ implies that the ideals $\mathfrak{p}$ and $\mathfrak{p}'$ are principal ideals. We set

$$\mathfrak{q} = \mathfrak{p} \cap \mathcal{O}_f,$$
$$\mathfrak{q}' = \mathfrak{p}' \cap \mathcal{O}_f.$$

Then, by Proposition 2.1, the ideals $\mathfrak{q}$ and $\mathfrak{q}'$ are principal ideals of $\mathcal{O}_f$ prime to f. Because of Lemma 2.1, $\mathcal{O}_f$-ideal prime to f is proper and using the unique factorization of proper ideals in Proposition 2.2, the ideals of norm p^k are as follows:

$$\mathfrak{q}^k, \mathfrak{q}^{k-1}\mathfrak{q}', \ldots, \mathfrak{q}'^k. \tag{4}$$

Let z_1 be the element of $\mathbb{Z}[\sqrt{-n}\,]$ with norm p^k. Because of Lemma 2.1, (z_1) is a proper $\mathcal{O}_f$-ideal. Moreover, for $-z_1 \in \mathbb{Z}[\sqrt{-n}\,]$, the ideals (z_1) and $(-z_1)$ are same proper $\mathcal{O}_f$-ideals. Hence, there exists a one-to-one correspondence between the non-equivalent elements of $\mathbb{Z}[\sqrt{-n}\,]$ with norm p^k under the action of $\{\pm 1\}$ and the set of proper $\mathcal{O}_f$-ideals of norm p^k defined by (4). This completes the proof of Theorem 1.1. □

4. Proof of Theorem 1.2

4.1. Setup

Proposition 4.1. *For any positive integers n and a, there exists a prime p not dividing n such that*

$$p = x^2 + ny^2$$

with $y \equiv 0 \pmod{4a}$.

Proof. We set $n' = 16a^2n$. Let L be the ring class field of the order $\mathbb{Z}[\sqrt{-n}\,]$. (We refer to Cox [2] for the concept of ring class fields.) Because of Theorem 2.3, there exists a prime p such that

$$\begin{aligned} p &= x^2 + n'y^2 \\ &= x^2 + n(4ay)^2 \end{aligned}$$

if and only if p splits completely in L. Then the primes that split completely in L have density $1/[L:K]$, and in particular there are infinitely many of them (cf. [2, Corollary 5.21] and [2, Corollary 8.18]). Hence, there exists a prime p not dividing n. Therefore, we complete the proof of Proposition 4.1. □

Because of Proposition 4.1, there exists prime p not dividing n such that $p = x_1^2 + ny_1^2$ with $y_1 \equiv 0 \pmod{4a}$. We fix such a prime and denote it by $p_{n,a}$. Then we define $A_{n,a}(k)$ as follows:

$$A_{n,a}(k) := \left\{ z \in \mathbb{Z}[\sqrt{-n}\,] \;\middle|\; |z|^2 = p_{n,a}^k \right\}.$$

By Proposition 4.1, if $x + y\sqrt{-n} \in A_{n,a}(k)$ then $y \equiv 0 \pmod{4a}$ and

$$x + y \equiv \pm j \pmod{4a}, \tag{5}$$

where $j \equiv x_1^k \pmod{4a}$, $1 \leqslant j \leqslant 4a-1$. So, we define $\check{A}_{n,a}(k)$ as follows:

$$\check{A}_{n,a}(k) := \left\{ x + y\sqrt{-n} \in A_{n,a}(k) \;\middle|\; x + y \equiv -j \pmod{4a} \right\}.$$

Lemma 4.1. $\sharp A_{n,a}(k) = 2(k+1)$ *and* $\sharp \check{A}_{n,a}(k) = k+1$.

Proof. Because of Proposition 4.1, $(d_K/p_{n,a}) = 1$ and $(p_{n,a}, f) = 1$. Hence, by Theorem 1.1 $\sharp A_{n,a}(k) = 2(k+1)$. If $x + y\sqrt{-n} \in A_{n,a}(k)$, then $x \neq 0$, $-x + y\sqrt{-n} \in A_{n,a}(k)$, and only one of them belongs to $\check{A}_{n,a}(k)$. Therefore, $\sharp \check{A}_{n,a}(k) = k+1$. □

4.2. Proof of Theorem 1.2

Here, we start the proof of Theorem 1.2.

Proof of Theorem 1.2. Let Λ be a 2-dimensional integral lattice and let the associated quadratic form be $ax^2 + bxy + cy^2$. Let $\mathcal{O}_f \subset \mathbb{Q}[\sqrt{-d}\,]$ be the order corresponding to the lattice Λ. We set $n = -f^2 d_K$ and $\alpha := (-b + \sqrt{-n}\,)/(2\sqrt{a}\,)$. It is enough to show that for each integer $k > 0$, there is a circle in the complex plane that passes through exactly $k+1$ points of Λ. For $k > 0$, define a circle Γ_k in complex plane as follows:

$$|4\sqrt{a}z - j|^2 = p_{n,a}^k,$$

where j is defined by (5). Let $C(k)$ be the subset of Λ lying on the circle Γ_k. We show that $\sharp C(k) = k+1$. If $z = \sqrt{a}x + \alpha y \in C(k)$ then $4\sqrt{a}z - j = 4ax - 2by - j + 2y\sqrt{-n}$, so $4ax - 2by - j + 2y \equiv -j \pmod{4a}$. Therefore $4\sqrt{a}z - j \in \check{A}_{n,a}(k)$. Hence we can define the map $\varphi : C(k) \to \check{A}_{n,a}(k)$ by:

$$z \mapsto 4\sqrt{a}z - j.$$

This map is a bijection. To see this, suppose $x + y\sqrt{-n} \in \check{A}_{n,a}(k)$. Then $x + y \equiv -j \pmod{4a}$, that is, $x + by + j \equiv 0 \pmod{4a}$. Moreover, by Proposition 4.1, $y \equiv 0 \pmod{4a}$, and hence y is even. Therefore, we can define a map from $\check{A}_{n,a}(k)$ to $C(k)$ as follows:

$$x + y\sqrt{-n} \mapsto \frac{x + by + j}{4\sqrt{a}} + \frac{y}{2}\alpha.$$

This gives the inverse of φ. Therefore φ is surjective, that is, $\sharp C(k) = \sharp \check{A}_{n,a}(k) = k+1$. □

Informing Hiroshi Maehara of Theorem 1.2, he proved the following fact:

Corollary 4.1. *If* $(\alpha/\beta)^2 \in \mathbb{Q}$ *then* $\Lambda[(\alpha, 0), (0, \beta)]$ *is universally concyclic.*

Proof. We assume that $(\alpha/\beta)^2 = b/a$, where b/a is irreducible fraction. Then, the lattices $\Lambda[(\alpha, 0), (0, \beta)]$ and $\Lambda[(a, 0), (0, \sqrt{ab}\,)]$ are similar under the similarity transformation α/a and $\Lambda[(a, 0), (0, \sqrt{ab}\,)]$ is integral lattice. Because of Theorem 1.2, $\Lambda[(a, 0), (0, \sqrt{ab}\,)]$ is universally concyclic, so is $\Lambda[(\alpha, 0), (0, \beta)]$. □

Remark 4.1. Finally, we generalize the definition of universally concyclic to higher dimensions.

Definition 4.1. Let $\Lambda \subset \mathbb{R}^d$ be a d-dimensional lattice. If there is a spherical surface S^{d-1} in $\mathbb{R}^d$ that passes through exactly n points of Λ for every integer $n > 0$, then Λ is called universally concyclic.

In [3], Maehara remarks that $\mathbb{Z}^3$ is universally concyclic because the spherical surface $(4x-1)^2 + (4y)^2 + (4z - \sqrt{2})^2 = 17k + 2$ passes through exactly $k+1$ points of $\mathbb{Z}^3$. We also remark that any integral lattice in higher dimension $d \geqslant 2$ is universally concyclic.

Corollary 4.2. *All integral lattices in $\mathbb{R}^d$ with $d \geqslant 2$ are universally concyclic.*

Proof. Let Λ be an integral lattice in $\mathbb{R}^d$. We define sublattices $\{\Lambda^{(i)}\}_{i=2}^d$ such that

$$\Lambda^{(2)} \subset \Lambda^{(3)} \subset \cdots \subset \Lambda^{(d)} = \Lambda$$

and $\Lambda^{(i)}$ spans $\mathbb{R}^i$ which we denote by $\mathbb{R}^{(i)}$ for all i. Because of Theorem 1.2, for each $k > 0$, we can define the circle $S^{(1)} \subset \mathbb{R}^{(2)}$ that passes through exactly k points of $\Lambda^{(2)}$.

Let $O^{(1)}$ be the center of $S^{(1)}$ and let ℓ be a half line in $\mathbb{R}^{(3)}$ whose origin is $O^{(1)}$, which is orthogonal to $\mathbb{R}^{(2)}$. We define the sphere $S^{(2)}(a)$, whose center $O^{(2)}(a)$ lies on ℓ, the distance between $O^{(1)}$ and $O^{(2)}(a)$ is a and whose radius is $\sqrt{a^2 + (\text{radius of } S^{(1)})^2}$. We assume that $0 \leqslant a \leqslant 1$.

Since Λ is an integral lattice, the number of the points of $\Lambda^{(3)}$ which intersect in $S^{(1)}(a)$ is finite for any $0 \leqslant a \leqslant 1$. Moreover, for $a_1 \neq a_2$, the intersection of $S^{(1)}(a_1)$ and $S^{(1)}(a_2)$ is the points of $\Lambda^{(2)}$ in Λ, namely, the points of $S^{(1)}$. On the other hand, for $0 \leqslant a \leqslant 1$, the number of the spheres $S^{(2)}(a)$ is infinite. Therefore, there exists a number a_0 such that the intersection of $S^{(2)}(a_0)$ and Λ is the points of $\Lambda^{(2)}$. We denote $S^{(2)}(a)$ by $S^{(2)}$ and $S^{(2)}$ passes through exactly k points of $\Lambda^{(3)}$. We can define the spheres $S^{(3)}, \ldots, S^{(d-1)}$ recursively such that each of $\{S^{(i)}\}_{i=3}^{d-1}$ passes through exactly k points of Λ, as we defined $S^{(2)}$ in $\mathbb{R}^{(3)}$. $\square$

So, we have shown that any integral lattices in $\mathbb{R}^d$ are universally concyclic. However, the points of lattice lying on the sphere constructed in the proof of Corollary 4.2 are on the plane $x_3 = \cdots = x_d = 0$. Hence, Maehara added some conditions to Definition 4.1 and showed the following theorem:

Theorem 4.1. *(Cf. [3].) For $n > d \geqslant 2$, there is a sphere in $\mathbb{R}^d$ that passes through exactly n lattice points on $\mathbb{Z}^d$, and moreover, the n lattice points span a d-dimensional polytope.*

Therefore, we can state the following problem:

Problem 4.1. Let Λ be an integral lattice in $\mathbb{R}^d$. We assume $n > d \geqslant 2$. Is there a sphere in $\mathbb{R}^d$ that passes through exactly n lattice points on Λ, which span a d-dimensional polytope?

A set of points in the d-dimensional Euclidean space is said to be in general position if no $d + 1$ of them lie in a $(d - 1)$-dimensional plane. Then, Maehara also proposed the following problem:

Problem 4.2. (Cf. [3].) Is there a sphere in $\mathbb{R}^3$ that passes through a given number of lattice points in general position on $\mathbb{Z}^3$?

It is also an interesting open problem to prove or disprove a similar conclusion as in Problem 4.2 for any integral lattices in higher dimension $\mathbb{R}^d$.

Acknowledgments

The authors are indebted to Hiroshi Maehara for interesting us to the property universally concyclic of Euclidean lattices and giving the proof of Corollary 4.1. The authors also thank Masanobu Kaneko of Kyushu University for informing us the concept of ring class field [2], and for his help in completing the proof of Proposition 4.1 and Kensaku Kinjo of Tohoku University for the careful reading of this manuscript and helpful comments. The second author was supported by JSPS Research Fellowship.

References

[1] A.I. Borevich, I.R. Shafarevich, Number Theory, Pure Appl. Math., vol. 20, Academic Press, New York–London, 1966, translated from the Russian by Newcomb Greenleaf.

[2] D.A. Cox, Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory and Complex Multiplication, A Wiley–Interscience Publication/John Wiley & Sons, Inc., New York, 1989.
[3] H. Maehara, On the number of concyclic points in planar lattices, preprint.
[4] H. Maehara, M. Matsumoto, Is there a circle that passes through a given number of lattice points?, European J. Combin. 19 (1998) 591–592, doi:10.1006/eujc.1997.0189.
[5] A. Schinzel, Sur l'existence d'un cercle passant par un nombre donné de points aux coordonnées entières, Enseign. Math. (2) 4 (1958) 71–72 (in French).
[6] D.B. Zagier, Zetafunktionen und quadratische Körper: eine Einführung in die höhere Zahlentheorie, Springer-Verlag, Berlin, Heidelberg, New York, 1981.