Discrete Comput Geom (2016) 56:693–710
DOI 10.1007/s00454-016-9812-4

Lattice Embeddings of Planar Point Sets

Michael Knopf[1] · Jesse Milzman[2] · Derek Smith[3] · Dantong Zhu[4] · Dara Zirlin[5]

Received: 13 September 2015 / Revised: 21 April 2016 / Accepted: 20 July 2016 /
Published online: 31 August 2016

Abstract Let $\mathcal{M}$ be a finite non-collinear set of points in the Euclidean plane, with the squared distance between each pair of points integral. Considering the points as lying in the complex plane, there is at most one positive square-free integer D, called the "characteristic" of $\mathcal{M}$, such that a congruent copy of $\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$. We generalize the work of Yiu and Fricke on embedding point sets in $\mathbb{Z}^2$ by providing conditions that characterize when $\mathcal{M}$ embeds in the lattice corresponding to $\mathcal{O}_{-D}$, the ring of integers in $\mathbb{Q}(\sqrt{-D})$. In particular, we show that if the square of every ideal in $\mathcal{O}_{-D}$ is principal and the distance between at least one pair of points in $\mathcal{M}$ is integral, then $\mathcal{M}$ embeds in $\mathcal{O}_{-D}$. Moreover, if $\mathcal{M}$ is primitive, so that the squared distances

Editor in Charge: János Pach

Michael Knopf
mknopf@gmail.com

Jesse Milzman
jmilzman@math.umd.edu

Derek Smith
smithder@lafayette.edu

Dantong Zhu
dantongzhu@gatech.edu

Dara Zirlin
zirlin2@illinois.edu

[1] University of California, Berkeley, Berkeley, CA, USA

[2] University of Maryland, College Park, MD, USA

[3] Lafayette College, Easton, PA 18042, USA

[4] Georgia Institute of Technology, Atlanta, GA, USA

[5] University of Illinois, Urbana-Champaign, Champaign, IL, USA

between pairs of points are relatively prime, and $\mathcal{O}_{-D}$ is a principal ideal domain, then $\mathcal{M}$ embeds in $\mathcal{O}_{-D}$.

Keywords Lattice embedding · Heronian triangle · n-Cluster · Ring of integers · Maximal order · Imaginary quadratic extension

Mathematics Subject Classification 52C10 · 52C05 · 11Z05 · 11R11 · 11R04

1 Introduction

Many classic problems in low-dimensional geometry ask whether certain point sets can satisfy integrality or rationality constraints. For example, is there a "perfect box," one whose edges, face diagonals, and body diagonals are integers? Is there a point inside of a unit square that is a rational distance from each of the corners of the square? Is there a set of points that is dense in the plane with all pairwise distances rational? Two standard sources for these and related problems are *Unsolved Problems in Number Theory* by Guy [6] and *Research Problems in Discrete Geometry* by Brass et al. [2].

The last of the three problems listed above is due to Ulam, and a related problem due to Erdős suggests how far Ulam's problem is from being resolved: For what n do there exist n points in the plane, no three on a line and no four on a circle, with all pairwise distances integral? To date, the only known examples have $n \leq 7$ [9]. The first published heptagon has coordinates of the form $(a, b\sqrt{2002})$ with $a, b \in \mathbb{Z}$; however, the majority of known examples are "n-clusters," sets whose points have integer coordinates and thus lie in the lattice $\mathbb{Z}^2$ [11,14]. These n-clusters necessarily satisfy another integrality condition, namely that any triple of non-collinear points determines a triangle with integral area.

In this article, we generalize the notion of n-cluster by considering point sets with all pairwise squared distances integral and whose triangles have arbitrary area. We determine when these point sets can be embedded in certain rings of algebraic integers; geometrically, these rings are the 2-dimensional lattices that are the most natural analogues of $\mathbb{Z}^2$. By "embedded" we mean that a congruent point set can be found in the lattice (as compared to [1], which considers similarity). Our methods and results involve the ideal theory of imaginary quadratic extensions of $\mathbb{Q}$; for another example of these ideals assisting the solution of a geometric problem, see the study of geodetic angles in [4].

It is not difficult to embed a triangle with integer side lengths and integer area (a *Heronian* triangle) in $\mathbb{Q}^2$: simply placing one vertex at the origin and another on the x-axis forces rational coordinates for the third vertex. More intriguing is the fact, first shown by Yiu [18], that any Heronian triangle can be embedded in $\mathbb{Z}^2$, so that its vertices have integer coordinates. Fricke [5] proved this same result in a different manner, viewing $\mathbb{Z}^2$ as the Gaussian integer ring $\mathbb{Z}[i]$ and utilizing unique factorization. Although many Heronian triangles, like a (3, 4, 5) right triangle, embed in $\mathbb{Z}[i]$ by placing an appropriate side on the x-axis, this is not the case for all of them: for example, consider the (15, 34, 35) triangle of area 252 on the left in Fig. 1, which has only non-

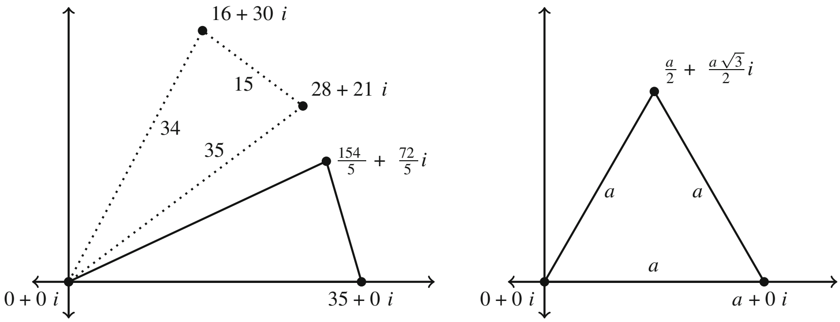


Fig. 1 A (15, 34, 35) triangle, and an equilateral triangle of side length a. We identify the point (a, b) in the plane with the complex number $a + bi$. On the left, the solid triangle is rotated to the dotted triangle via multiplication by $\frac{4}{5} + \frac{3}{5}i$

trivial embeddings in $\mathbb{Z}[i]$. Lunnon [12] and Marshall and Perlis [13] followed Fricke's idea in their work on embeddings of Heronian triangles and tetrahedra.

On the other hand, consider an equilateral triangle with integer side length a; it does not have integer area. Placed with one side on the x-axis, as shown on the right in Fig. 1, the opposite vertex is $(\frac{a}{2}, \frac{a\sqrt{3}}{2})$, which is clearly not in $\mathbb{Q}^2$; later we will give a quick proof that there is no possible embedding of this triangle in $\mathbb{Q}^2$. However, the area of the equilateral triangle is of the form $q\sqrt{3}$ for a rational number q, and the triangle does embed in $\mathbb{Q}(\sqrt{-3})$. Moreover, it embeds in the ring $\mathcal{O}_{-3}$ of Eisenstein integers, the ring of integers in $\mathbb{Q}(\sqrt{-3})$.

We will show that similar results hold for a large family of planar point sets whose pairwise distances are square roots of integers: each embeds in the ring of integers in an appropriate quadratic extension of $\mathbb{Q}$. For instance, here is a restatement of the second part of Corollary 1 in Sect. 5.1:

> Let $\mathcal{M}$ be a finite non-collinear set of points $\{P_i\}$ in the plane with $|P_i - P_j|^2 \in \mathbb{Z}$ for all i, j. Let D be the square-free integer part of the squared area of any non-degenerate triangle (P_i, P_j, P_k) in $\mathcal{M}$. If at least one distance $|P_i - P_j| \in \mathbb{Z}$, and if the square of every ideal in the ring of integers $\mathcal{O}_{-D}$ in $\mathbb{Q}(\sqrt{-D})$ is principal, then M embeds in $\mathcal{O}_{-D}$.

Embedding Heronian triangles in the principal ideal domain $\mathcal{O}_{-1} \cong \mathbb{Z}[i]$ is the special case of $n = 3$ and $D = 1$. For examples of embeddings when $D = 2$ and $D = 3$, see Fig. 2.

The structure of this paper is as follows. In Sect. 2, we introduce notation and review the results from algebraic number theory that we will use later. Section 3 contains a brief discussion about embedding point sets in quadratic extensions of $\mathbb{Q}$, while Sect. 4 presents our main results about embedding point sets in rings of integers. Section 5 considers particular values of D, namely the cases where $\mathcal{O}_{-D}$ is a PID or the ideal class group is isomorphic to $\mathbb{Z}_2^k$ for some positive integer k. Our two main theorems are applied to examples in Sect. 6.

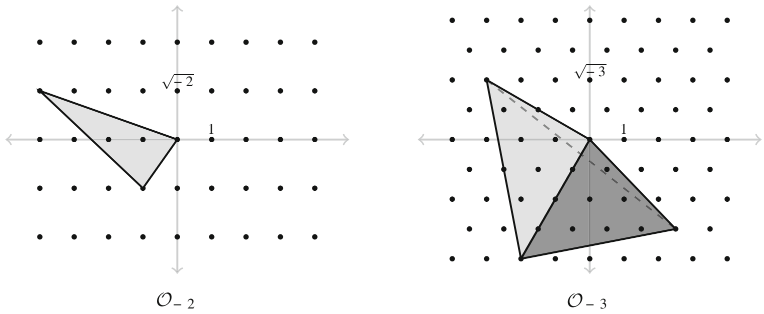


Fig. 2 On the left is a $(\sqrt{3}, \sqrt{17}, \sqrt{18})$ triangle with area $\frac{5}{2}\sqrt{2}$ embedded in $\mathcal{O}_{-2}$. The lighter triangle of the point set embedded in $\mathcal{O}_{-3}$ on the right has area $3\sqrt{3}$ and the darker one has area $4\sqrt{3}$; the three edge lengths of the lighter triangle are $\sqrt{12}$, 4, and $\sqrt{28}$, and the remaining three edge lengths are $\sqrt{13}$, $\sqrt{21}$, and 7 (dashed segment)

2 Notation and Number Theory Preliminaries

Unless otherwise stated, for the remainder of this article $\mathcal{M}$ refers to a non-collinear point set in the complex plane with $|\mathcal{M}| \geq 3$ and such that for any points $\alpha, \beta \in \mathcal{M}$ we have $|\alpha - \beta|^2 \in \mathbb{Z}$. Since the norm of a complex number is the square of its length, we call $\mathcal{M}$ an *integer norm point set*, and an *integer norm triangle* when $|\mathcal{M}| = 3$. If in fact $|\alpha - \beta| \in \mathbb{Z}$ for all $\alpha, \beta \in \mathcal{M}$, we use the more restrictive terms *integer point set* and *integer triangle*. We say that $\mathcal{M}$ has (directed) edges of the form $\beta - \alpha$ for all $\alpha \neq \beta$ in $\mathcal{M}$.

We are interested in knowing when an integer norm point set $\mathcal{M}$ can be embedded in $\mathbb{Q}(\sqrt{-D})$ or its ring of integers $\mathcal{O}_{-D}$ for certain positive square-free integer values D. We define the imaginary quadratic field

$$\mathbb{Q}(\sqrt{-D}) = \{a + b\sqrt{-D} \mid a, b \in \mathbb{Q}\},$$

and we define $\mathcal{O}_{-D}$ as the ring of integers in this field, which is also its unique maximal order:

$$\mathcal{O}_{-D} = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\},$$

where

$$\omega = \begin{cases} \sqrt{-D} & \text{if } -D \not\equiv 1 \pmod 4, \\ \frac{1+\sqrt{-D}}{2} & \text{if } -D \equiv 1 \pmod 4. \end{cases}$$

For $-D \equiv 1 \pmod 4$, an equivalent definition is

$$\mathcal{O}_{-D} = \left\{ \tfrac{c+d\sqrt{-D}}{2} \;\middle|\; c, d \in \mathbb{Z},\ c \equiv d \,(\mathrm{mod}\, 2) \right\}.$$

Since $\mathbb{Q}(\sqrt{-D})$ and $\mathcal{O}_{-D}$ are invariant under translation by their elements, we will always assume that $\mathcal{M}$ contains the origin as one of its points.

The rest of this section contains some of the basic results about the number theory of $\mathbb{Q}(\sqrt{-D})$ and the integer ring $\mathcal{O}_{-D}$ that will be used in this article; for more information, see [3]. We will refer to elements of $\mathbb{Z}$ as *rational integers* in order to distinguish them from other elements of $\mathcal{O}_{-D}$. Note that any element of $\mathbb{Q}(\sqrt{-D})$ can be expressed in the form $\frac{\alpha}{r}$ for some $\alpha \in \mathcal{O}_{-D}$ and $r \in \mathbb{Z}$, where α and r share no rational integer factors.

Upon defining the *conjugate* of $\alpha = a + b\sqrt{-D}$ as $\bar{\alpha} = a - b\sqrt{-D}$, the *norm* of α is $[\alpha] = \alpha\bar{\alpha}$, and the *trace* is $tr(\alpha) = \alpha + \bar{\alpha}$. Useful identities involving these three terms include $\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$, $\bar{\bar{\alpha}} = \alpha$, $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$, $[\alpha][\beta] = [\alpha\beta]$, and

$$[\alpha - \beta] = [\alpha] + [\beta] - (\alpha\bar{\beta} + \bar{\alpha}\beta) = [\alpha] + [\beta] - tr(\alpha\bar{\beta}).$$

For our purposes, the conjugate of α is the same as its complex conjugate, so we have $tr(\alpha) = 2\,\mathrm{Re}(\alpha)$, which is a rational integer when $\alpha \in \mathcal{O}_{-D}$. Also, $[\alpha] = |\alpha|^2 = a^2 + Db^2$, which is a non-negative rational integer when $\alpha \in \mathcal{O}_{-D}$.

For $\alpha, \beta \in \mathcal{O}_{-D}$, we say that $\alpha \mid \beta$ if there exists $\gamma \in \mathcal{O}_{-D}$ such that $\beta = \alpha\gamma$. If $\alpha \mid \beta$, then $\bar{\alpha} \mid \bar{\beta}$ as well. Since any rational integer r is its own conjugate, $r \mid \alpha$ if and only if $r \mid \bar{\alpha}$. An element $\pi \in \mathcal{O}_{-D}$ is *prime* if $\pi \mid \alpha\beta$ implies $\pi \mid \alpha$ or $\pi \mid \beta$ for all $\alpha, \beta \in \mathcal{O}_{-D}$.

We call $\gamma \in \mathcal{O}_{-D}$ *irreducible* if γ is not a unit (so $[\gamma] > 1$) and $\gamma = \alpha\beta$ implies that α or β is a unit. Then $\mathcal{O}_{-D}$ is a *unique factorization domain* (UFD) if every element has a unique factorization into irreducible elements, up to the order of the factors and multiplication by units. A prime is irreducible in any $\mathcal{O}_{-D}$; if $\mathcal{O}_{-D}$ is a UFD, then irreducible elements are prime as well. For most values of D, $\mathcal{O}_{-D}$ is not a UFD. For example, $6 \in \mathcal{O}_{-5}$ factors into irreducibles in two distinct ways: $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. By the celebrated Stark–Heegner Theorem [16], the only rings $\mathcal{O}_{-D}$ that are UFDs have $D = 1, 2, 3, 7, 11, 19, 43, 67, 163$; these nine rings are precisely the *principal ideal domains* (PIDs) as well, meaning that every ideal in $\mathcal{O}_{-D}$ is of the form $\langle\alpha\rangle = \{\alpha\beta \mid \beta \in \mathcal{O}_{-D}\}$ for some $\alpha \in \mathcal{O}_{-D}$.

We end this section with some of the properties of ideals that we use in the remaining sections. An ideal J divides the ideal I if $I = JK$ for some ideal K; this is equivalent to $J \supseteq I$. I is a *prime* ideal if $I \mid JK$ implies $I \mid J$ or $I \mid K$. Every ideal in $\mathcal{O}_{-D}$ factors uniquely into a product of prime ideals, whether $\mathcal{O}_{-D}$ is a UFD or not.

Two ideals I, J are *relatively prime* if there is no nontrivial ideal that divides both of them, in which case we write $\langle I, J\rangle = \langle 1\rangle = \mathcal{O}_{-D}$. If I and J are relatively prime, then $I \mid K$ and $J \mid K$ implies $IJ \mid K$ for any ideal K. The minimal ideal that contains the ideals $I_1, \ldots, I_n$ is written $\langle I_1, \ldots, I_n\rangle$.

Conjugating every element of an ideal I gives the *conjugate* ideal $\bar{I}$, and $I\bar{I}$ is a principal ideal generated by a positive rational integer $[I]$ we call the *norm* of I. For a principal ideal $\langle\alpha\rangle$ with $\alpha \in \mathcal{O}_{-D}$, we have $[\langle\alpha\rangle] = [\alpha]$. The norm of a product of ideals is the product of the norms of those ideals.

The ideals of $\mathcal{O}_{-D}$ form a finite abelian group under multiplication, called the *ideal class group* $C(\mathcal{O}_{-D})$, once we take the quotient by the principal ideals. We write $I \sim J$ if the images of I and J under this quotient map are equal, i.e. if $I\bar{J}$ is principal. Several results in this paper concern $\mathcal{O}_{-D}$ such that the square of every ideal is principal, which is equivalent to $C(\mathcal{O}_{-D}) \cong \mathbb{Z}_2^k$ for some non-negative rational integer k, i.e. for $k > 0$, the class group has exponent 2.

3 Quadratic Field Embeddings

In this section, we are interested in knowing when an integer norm point set $\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$ for some positive square-free integer D. Propositions 1 and 2 are not new (see [8, 15]), but short proofs are given to keep the paper self-contained; Proposition 3 will be used in the proof of Theorem 3 in Sect. 5.2. As stated in the previous section, we assume that $\mathcal{M}$ is non-collinear and contains the origin.

Suppose that T is a triangle in $\mathcal{M}$ with side lengths (a, b, c); all triangles are assumed to be non-degenerate. By Heron's formula,

$$\begin{aligned} A &= \tfrac{1}{4}\sqrt{(a+b+c)(a+b-c)(a-b+c)(-a+b+c)} \\ &= \tfrac{1}{4}\sqrt{-a^4-b^4-c^4+2a^2b^2+2a^2c^2+2b^2c^2}. \end{aligned}$$

Since the squares of the edge lengths of T are all integers, the area will be of the form $\frac{m}{4}\sqrt{D}$ where $m \in \mathbb{Z}$ and D is a positive square-free integer. This integer D is called the *characteristic* of T [8, 10]; for example, any Heronian triangle has characteristic 1, and any equilateral triangle with side length $\sqrt{a}$, $a \in \mathbb{Z}$, has characteristic 3.

The notion of characteristic extends to points sets $\mathcal{M}$ containing any number of points.

Proposition 1 *Suppose an integer norm point set $\mathcal{M}$ has more than three points. Then all triangles in $\mathcal{M}$ have the same characteristic.*

Proof We will show that any two triangles that share an edge have the same characteristic. The proof of the proposition follows from this, since any two triangles in $\mathcal{M}$ can be joined by a sequence of triangles where each shares an edge with the next one.

Let $\triangle 0\alpha\beta$ and $\triangle 0\gamma\beta$ be two triangles sharing the edge β, after rotating and possibly reflecting $\mathcal{M}$ so that β lies on the x-axis, as depicted in Fig. 3. Let D and E be the respective characteristics of the two triangles, so that the area of $\triangle 0\alpha\beta$ is $p\sqrt{D}$ and the area of $\triangle 0\gamma\beta$ is $q\sqrt{E}$ for some $p, q \in \mathbb{Q}$. The coordinates of α and γ can be expressed in terms of the triangles' side lengths and areas, with the real parts determined by the

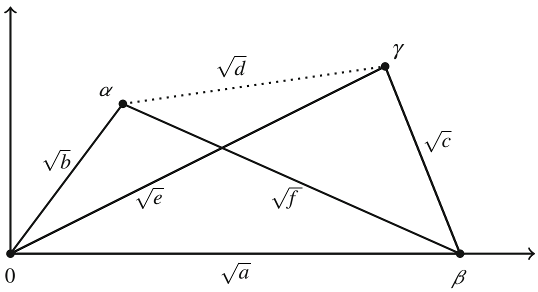


Fig. 3 If two triangles share an edge, their characteristics are equal

law of cosines and the imaginary parts by the triangles' areas:

$$\alpha = \frac{a+b-f}{2\sqrt{a}} + \frac{2p\sqrt{D}}{\sqrt{a}}i \quad \text{and} \quad \gamma = \frac{a+e-c}{2\sqrt{a}} + \frac{2q\sqrt{E}}{\sqrt{a}}i.$$

Thus,

$$\begin{aligned} d &= \Big(\frac{a+b-f}{2\sqrt{a}} - \frac{a+e-c}{2\sqrt{a}}\Big)^2 + \Big(\frac{2p\sqrt{D}}{\sqrt{a}} - \frac{2q\sqrt{E}}{\sqrt{a}}\Big)^2 \\ &= \frac{1}{4a}(b+c-e-f)^2 + \frac{4p^2}{a}D + \frac{4q^2}{a}E - \frac{8pq}{a}\sqrt{DE} \end{aligned}$$

is an integer. The first three terms and the coefficient of $\sqrt{DE}$ are rational, so $\sqrt{DE}$ must also be rational. Since DE is a perfect square and D and E are both square-free, we must have $D = E$. □

Define the characteristic of $\mathcal{M}$ to be the characteristic of any triangle in $\mathcal{M}$. The next two propositions explain the relationship between the characteristic of $\mathcal{M}$ and embeddability in $\mathbb{Q}(\sqrt{-D})$.

Proposition 2 *Let D be a square-free positive integer. If an integer norm point set $\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$, then $\mathcal{M}$ has characteristic D.*

Proof Any triangle formed by the origin and two other points in $\mathcal{M}$ is of the form $\{0, a + b\sqrt{-D}, c + d\sqrt{-D}\}$ with $a, b, c, d \in \mathbb{Q}$. The area of this triangle is

$$\tfrac{1}{2}\begin{vmatrix} a & c \\ b\sqrt{D} & d\sqrt{D} \end{vmatrix} = \frac{|ad-bc|}{2}\sqrt{D},$$

so $\mathcal{M}$ has characteristic D. □

Proposition 3 *Suppose an integer norm point set $\mathcal{M}$ has characteristic D. Then $\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$ if and only if there exists a rotation ϕ about the origin such that $\phi(\alpha') \in \mathbb{Q}(\sqrt{-D})$ for some non-zero $\alpha' \in \mathcal{M}$. In particular, $\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$ if $\mathcal{M}$ contains an integer edge length.*

Proof The forward direction of the proof is trivial. For the reverse direction, let $\alpha = \phi(\alpha')$, and let $\beta = \phi(\beta')$ for any other non-zero $\beta' \in \mathcal{M}$. Then $\alpha = a + b\sqrt{-D}$ with $a, b \in \mathbb{Q}$ and $\beta = c+d\sqrt{-D}$ with $c, d \in \mathbb{R}$. The area of $\triangle 0\alpha\beta$ is $|ad-bc|\sqrt{D}/2$, and since $\mathcal{M}$ has characteristic D this area equals $m\sqrt{D}/4$ for some $m \in \mathbb{Z}$. Thus $2(ad-bc) \in \mathbb{Z}$, so $2a^2d - 2abc \in \mathbb{Q}$. Also, since

$$[\alpha - \beta] = [\alpha] + [\beta] - (\alpha\bar{\beta} + \bar{\alpha}\beta),$$

and since $[\alpha - \beta]$, $[\alpha]$, and $[\beta]$ are integers, we know that

$$\alpha\bar{\beta} + \bar{\alpha}\beta = 2\ \mathrm{Re}(\alpha\bar{\beta}) = 2ac + 2bdD \in \mathbb{Z},$$

so $2abc+2b^2dD \in \mathbb{Q}$. Adding these two rational expressions gives $2(a^2+b^2D)d \in \mathbb{Q}$, so $d \in \mathbb{Q}$, which implies that $c \in \mathbb{Q}$ as well. Thus $\beta \in \mathbb{Q}(\sqrt{-D})$. $\square$

For an example of an integer norm triangle of characteristic D that does not embed in $\mathbb{Q}(\sqrt{-D})$, see Sect. 5.1.

4 Quadratic Ring Embeddings

We now know that an integer norm point set $\mathcal{M}$ has a well-defined characteristic D, and we can embed $\mathcal{M}$ in $\mathbb{Q}(\sqrt{-D})$ if and only if there are two points $\alpha, \beta \in \mathcal{M}$ such that $\beta - \alpha \in \mathbb{Q}(\sqrt{-D})$. In this section we will prove our main theorem, which characterizes exactly when $\mathcal{M}$ will embed in $\mathcal{O}_{-D}$, given that $\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$.

We will first prove a useful result about factorization in $\mathcal{O}_{-D}$.

Lemma 1 *Suppose p is a rational prime and there exists an $\alpha \in \mathcal{O}_{-D}$ such that $p \nmid \alpha$ but $p^2 \mid [\alpha]$. Then $\langle p\rangle = I\bar{I}$ for two distinct conjugate prime ideals $I, \bar{I} \subset \mathcal{O}_{-D}$.*

Proof There are three options: $\langle p\rangle$ is a prime ideal in $\mathcal{O}_{-D}$, $\langle p\rangle$ ramifies by factoring into two identical prime ideals of norm p, or $\langle p\rangle$ splits into two distinct conjugate prime ideals of norm p.

Suppose $\langle p\rangle$ is a prime ideal. Then p is prime in $\mathcal{O}_{-D}$. Since $p^2 \mid \alpha\bar{\alpha}$ implies $p \mid \alpha\bar{\alpha}$, we have $p \mid \alpha$ or $p \mid \bar{\alpha}$. Since $p \in \mathbb{Z}$, either way we have $p \mid \alpha$, a contradiction.

Suppose instead that $\langle p\rangle$ ramifies as $\langle p\rangle = I^2$ for some prime ideal I. Since $\alpha\bar{\alpha} = p^2m$ for some $m \in \mathbb{Z}$, $\langle\alpha\rangle\langle\bar{\alpha}\rangle = I^4\langle m\rangle$. Since I is prime, $I^2 \mid \langle\alpha\rangle$ or $I^2 \mid \langle\bar{\alpha}\rangle$, so at least one of $\langle p\rangle \mid \langle\alpha\rangle$ and $\langle p\rangle \mid \langle\bar{\alpha}\rangle$ is true. Thus, $p \mid \alpha$ or $p \mid \bar{\alpha}$, either of which implies $p \mid \alpha$, a contradiction. $\square$

For the rest of this section, we assume that $\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$ for some square-free characteristic D. Thus we can write our $(n+1)$-element point set as $\mathcal{M} = \{0, \frac{\alpha_1}{r_1}, \ldots, \frac{\alpha_n}{r_n}\}$, where $\alpha_i \in \mathcal{O}_{-D}$ and $r_i \in \mathbb{Z}$ have no common rational integer factor in $\mathcal{O}_{-D}$. If r is the least common denominator for the final n points in $\mathcal{M}$, for each i we have $\frac{\beta_i}{r} = \frac{\alpha_i}{r_i}$ for some $\beta_i \in \mathcal{O}_{-D}$. Thus, we can express $\mathcal{M}$ as

$$\mathcal{M} = \left\{0, \tfrac{\beta_1}{r}, \ldots, \tfrac{\beta_n}{r}\right\},$$

where the greatest common rational integer factor of $\beta_1, \ldots, \beta_n$, and r is 1.

Lemma 2 is a structural result that relies on the following two facts, which are direct consequences of the integer norm condition for $\mathcal{M}$. First, since $[\frac{\beta_i}{r}] \in \mathbb{Z}$ for all i, we know that $r^2 \mid [\beta_i] = \beta_i\bar{\beta}_i$ for all i. Second, since $[\frac{\beta_i}{r} - \frac{\beta_j}{r}] \in \mathbb{Z}$ for all i and j, we know that

$$r^2 \mid [\beta_i - \beta_j] = [\beta_i] + [\beta_j] - (\beta_i\bar{\beta}_j + \bar{\beta}_i\beta_j),$$

and thus $r^2 \mid \beta_i\bar{\beta}_j + \bar{\beta}_i\beta_j = 2\,\mathrm{Re}(\beta_i\bar{\beta}_j)$ for all i and j.

Lemma 2 *Suppose that the integer norm point set $\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$, so that $\mathcal{M} = \{0, \frac{\beta_1}{r}, \ldots, \frac{\beta_n}{r}\}$, as defined above. Then there is a unique ideal I_* such that*

$\langle r\rangle = I_*\bar{I}_*$ and such that for each i, $\langle \beta_i\rangle = I_*^2 K_i$ for some ideal K_i. If $r \neq 1$, then $I_* \neq \bar{I}_*$. In addition, $\frac{\beta_j\bar{\beta}_k}{r^2} \in \mathcal{O}_{-D}$ for all j and k.

Proof If $r = 1$, we can let $I_* = \langle 1\rangle$, for clearly $\langle r\rangle = \langle 1\rangle\langle\bar{1}\rangle$ and $\langle 1\rangle^2 \mid \beta_i$ for all i. If $r > 1$, let $r = p_1^{c_1}\cdots p_m^{c_m}$ be the prime factorization of r, and consider any p_i. Since the greatest common rational integer factor of $\beta_1,\ldots,\beta_n$, and r is 1, there is some j for which $p_i \nmid \beta_j$. Since $p_i^2 \mid p_i^{2c_1} \mid r^2 \mid [\beta_j]$, by Lemma 1 we have $\langle p_i\rangle = I_i\bar{I}_i$ for two distinct conjugate prime ideals $I_i, \bar{I}_i$. Thus,

$$I_i^{2c_i}\bar{I}_i^{2c_i} = \langle p_i^{2c_i}\rangle \mid \langle \beta_j\bar{\beta}_j\rangle = \langle\beta_j\rangle\langle\bar{\beta}_j\rangle.$$

Since I_i is a prime ideal, we know $I_i \mid \langle\beta_j\rangle$ or $I_i \mid \langle\bar{\beta}_j\rangle$. Both of these cannot happen simultaneously because the latter implies $\bar{I}_i \mid \langle\beta_j\rangle$, which with $\langle I_i, \bar{I}_i\rangle = \langle 1\rangle$ would lead to $I_i\bar{I}_i = \langle p_i\rangle \mid \langle\beta_j\rangle$ and thus $p_i \mid \beta_j$. Without loss of generality assume $I_i \nmid \langle\bar{\beta}_j\rangle$, so we know that $I_i^{2c_i} \mid \langle\beta_j\rangle$.

Now consider an arbitrary $k \neq j$. Since $p_i^{2c_i} \mid r^2 \mid \beta_j\bar{\beta}_k + \bar{\beta}_j\beta_k$, we know that

$$I_i^{2c_i} \mid \langle p_i^{2c_i}\rangle \mid \langle \beta_j\bar{\beta}_k + \bar{\beta}_j\beta_k\rangle,$$

and so $\beta_j\bar{\beta}_k + \bar{\beta}_j\beta_k \in I_i^{2c_i}$. Also, since $I_i^{2c_i} \mid \langle\beta_j\rangle$ we know that $\beta_j \in I_i^{2c_i}$; and since ideals are closed under multiplication by any ring element, $\beta_j\bar{\beta}_k \in I_i^{2c_i}$. Thus,

$$(\beta_j\bar{\beta}_k + \bar{\beta}_j\beta_k) - \beta_j\bar{\beta}_k = \bar{\beta}_j\beta_k \in I_i^{2c_i},$$

and so $I_i^{2c_i} \mid \langle\bar{\beta}_j\beta_k\rangle = \langle\bar{\beta}_j\rangle\langle\beta_k\rangle$. Since $I_i \nmid \langle\bar{\beta}_j\rangle$, we have $I_i^{2c_i} \mid \langle\beta_k\rangle$.

We now set $I_* = I_1^{c_1}\cdots I_m^{c_m}$, so that

$$I_*\bar{I}_* = I_1^{c_1}\bar{I}_1^{c_i}\ldots I_m^{c_m}\bar{I}_m^{c_m} = \langle p_1^{c_1}\rangle\ldots\langle p_m^{c_m}\rangle = \langle r\rangle$$

and

$$I_*^2 = I_1^{2c_1}\cdots I_m^{2c_m} \mid \langle\beta_l\rangle$$

for all l; the latter fact and $I_* \neq \bar{I}_*$ follow from $\bar{I}_i \neq I_i \neq I_j$ for $i \neq j$.

The final statement of the lemma then follows from

$$\langle\beta_j\bar{\beta}_k\rangle = I_*^2 K_j\bar{I}_*^2\bar{K}_k = r^2 K_j\bar{K}_k \subseteq r^2\mathcal{O}_{-D}.$$

□

We are now in position to prove our main theorem, which is stated in terms of the ideals I_* and K_i from Lemma 2:

Theorem 1 *The integer norm point set* $\mathcal{M} = \{0, \frac{\beta_1}{r}, \ldots, \frac{\beta_n}{r}\} \subseteq \mathbb{Q}(\sqrt{-D})$ *embeds in* $\mathcal{O}_{-D}$ *if and only if there is some ideal* J_* *such that* $I_*^2 J_*^2$ *is principal and* $J_* \mid K_i$ *for all* i.

Proof First suppose that J_* exists, and for each i let $K_i = J_* X_i$. Since $I_*^2 J_*^2$ is principal, so is $\bar{I_*}^2 \bar{J_*}^2$; so there exists $\sigma \in \mathcal{O}_{-D}$ such that $\bar{I_*}^2 \bar{J_*}^2 = \langle\sigma\rangle$, where $|\sigma| = [I_*][J_*]$. Thus for each i,

$$\begin{aligned}\langle\sigma\beta_i\rangle &= \bar{I_*}^2 \bar{J_*}^2 I_*^2 J_* X_i \\ &= [I_*][J_*][I_*]\,\bar{J}_* X_i \\ &= |\sigma| r\, \bar{J}_* X_i,\end{aligned}$$

so we know that $\sigma\beta_i \in |\sigma| r\, \mathcal{O}_{-D}$.

Let $\varepsilon = \frac{\sigma}{|\sigma|}$, and define the rotation $R(\tau) = \varepsilon\tau$ for all $\tau \in \mathbb{C}$. Then $\mathcal{M}$ embeds in $\mathcal{O}_{-D}$ since

$$R\big(\tfrac{\beta_i}{r}\big) = \varepsilon \tfrac{\beta_i}{r} = \tfrac{\sigma\beta_i}{|\sigma| r} \in \mathcal{O}_{-D}$$

for all i.

For the other half of the proof, suppose that after embedding $\mathcal{M}$ we have $\varepsilon\frac{\beta_i}{r} = \gamma_i \in \mathcal{O}_{-D}$ for all i, where $\varepsilon = \frac{\sigma}{|\sigma|}$ for some $\sigma \in \mathcal{O}_{-D}$. Since $|\sigma| r\gamma_i = \sigma\beta_i$, we have $\langle |\sigma| r\gamma_i\rangle = \langle\sigma\beta_i\rangle = \langle\sigma\rangle I_*^2 K_i$. Taking norms gives $r^2[\langle\gamma_i\rangle] = [I_*]^2[K_i]$ and thus $[\langle\gamma_i\rangle] = [K_i]$.

Factor $\langle\gamma_1\rangle$ and K_1 into prime ideals and cancel all common factors. Let J_* be the product of the remaining factors of K_1, and let F be the product of the remaining factors of $\langle\gamma_1\rangle$. Since $\langle\bar{\gamma}_1\rangle\langle\gamma_1\rangle = \bar{K}_1 K_1$, we know that $\bar{F}F = \bar{J}_* J_*$. Since $\langle F, J_*\rangle = \langle\bar{F}, \bar{J}_*\rangle = \langle 1\rangle$, we get $\bar{F} = J_*$. From $\langle\bar{\gamma}_1\rangle\langle\gamma_1\rangle = \bar{K}_1 K_1$ we deduce that $J_*\langle\gamma_1\rangle = \bar{J}_* K_1$.

We know that $J_* \mid K_1$ by definition. If $i \neq 1$, since $\gamma_i\beta_1 = \gamma_1\beta_i$ for all i,

$$J_*\langle\gamma_i\rangle\langle\beta_1\rangle = J_*\langle\gamma_1\rangle\langle\beta_i\rangle.$$

From this we have

$$J_*\langle\gamma_i\rangle I_*^2 K_1 = \bar{J}_* K_1 I_*^2 K_i,$$

so $J_*\langle\gamma_i\rangle = \bar{J}_* K_i$. Since $\langle J_*, \bar{J}_*\rangle = \langle 1\rangle$, we know that $J_* \mid K_i$ for all i.

Finally, note that

$$\langle[J_*]\rangle\langle\gamma_1\rangle = \bar{J}_* J_*\langle\gamma_1\rangle = \bar{J_*}^2 K_1,$$

so $\bar{J_*}^2 K_1$ is principal. Since $\langle\beta_i\rangle = I_*^2 K_1$ is also principal, $\bar{J_*}^2 K_1 \sim I_*^2 K_1$. Thus $I_*^2 \sim \bar{J_*}^2$, so $I_*^2 J_*^2$ is principal. □

We call an integer norm point set $\mathcal{M}$ *primitive* if the greatest common divisor of the norms of all edges is 1. Primitive $\mathcal{M}$ have a simpler embedding condition, as stated in Theorem 2 below. To prove this result, we begin with the following lemma.

Lemma 3 *Let $K = \langle K_1, \ldots, K_n \rangle$. Then $K = \langle 1 \rangle$ if $\mathcal{M}$ is primitive.*

Proof Suppose that $\mathcal{M}$ is primitive. Since $K \mid K_i$, we immediately have

$$[K] \mid [K_i] = \frac{[\beta_i]}{[I_*]^2} = \left[\frac{\beta_i}{r}\right]$$

for all i.

For each i, there is an ideal Y_i such that $K_i = KY_i$, so

$$\begin{aligned}\langle \beta_i \rangle \langle \bar{\beta}_j \rangle &= I_*^2 K_i \bar{I_*}^2 \bar{K}_j \\ &= [I_*]^2 K \bar{K} Y_i \bar{Y}_j \\ &= r^2 [K] Y_i \bar{Y}_j\end{aligned}$$

for all i and j. This means that $\langle \frac{\beta_i \bar{\beta}_j}{r^2} \rangle = [K] Y_i \bar{Y}_j$, and thus $[K] \mid \frac{\beta_i \bar{\beta}_j}{r^2} \in \mathcal{O}_{-D}$.

We now know that

$$[K] \mid \left[\frac{\beta_i}{r}\right] + \left[\frac{\beta_j}{r}\right] - \left(\frac{\beta_i \bar{\beta}_j}{r^2} + \frac{\beta_j \bar{\beta}_i}{r^2}\right) = \left[\frac{\beta_i}{r} - \frac{\beta_j}{r}\right]$$

for all i and j, so $[K]$ divides all edge lengths in $\mathcal{M}$. Since $\mathcal{M}$ is primitive, $[K] = 1$, so $K = \langle 1 \rangle$. □

Theorem 2 *Suppose the integer norm point set $\mathcal{M} = \{0, \frac{\beta_1}{r}, \ldots, \frac{\beta_n}{r}\} \subseteq \mathbb{Q}(\sqrt{-D})$ is primitive. Then $\mathcal{M}$ embeds in $\mathcal{O}_{-D}$ if and only if I_*^2 is principal.*

Proof From Theorem 1, by simply letting $J_* = \langle 1 \rangle$ we know that $\mathcal{M}$ embeds in $\mathcal{O}_{-D}$ if I_*^2 is principal. If $\mathcal{M}$ is primitive, then by Lemma 3 we know that $\langle K_1, \ldots, K_n \rangle = \langle 1 \rangle$, so $J_* \mid K_i$ for all i would imply $J_* = \langle 1 \rangle$. Therefore, $\mathcal{M}$ embeds only if I_*^2 is principal. □

5 Particular Characteristics

In this section, we apply the results of the previous section to rings $\mathcal{O}_{-D}$ whose class groups $C(\mathcal{O}_{-D})$ are isomorphic to $\mathbb{Z}_2^k$ for non-negative integers k.

5.1 When $C(\mathcal{O}_{-D}) \cong \mathbb{Z}_2^k$

Assuming the Generalized Riemann Hypothesis, there are only 65 square-free integers D such that $C(\mathcal{O}_{-D}) \cong \mathbb{Z}_2^k$ for some non-negative integer k [7,17]:

k	D
0	1, 2, 3, 7, 11, 19, 43, 67, 163
1	5, 6, 10, 13, 15, 22, 35, 37, 51, 58, 91, 115, 123, 187, 235, 267, 403, 427
2	21, 30, 33, 42, 57, 70, 78, 85, 93, 102, 130, 133, 177, 190, 195, 253, 435, 483, 555, 595, 627, 715, 795, 1435
3	105, 165, 210, 273, 330, 345, 357, 385, 462, 1155, 1995, 3003, 3315
4	1365

An immediate consequence of Theorem 1 is the following.

Corollary 1 *Suppose that an integer norm point set $\mathcal{M}$ has characteristic D and the square of every ideal in $\mathcal{O}_{-D}$ is principal. Then*

1. *$\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$ if and only if $\mathcal{M}$ embeds in $\mathcal{O}_{-D}$.*
2. *If some edge of $\mathcal{M}$ has integer length, then $\mathcal{M}$ embeds in $\mathcal{O}_{-D}$.*

Proof The proof of the forward direction of the first part follows from Theorem 1 by setting $J_* = \langle 1\rangle$, and the reverse direction is trivial. The second part of the corollary follows from the first part and Proposition 3. □

Consider the $(\sqrt{2}, \sqrt{5}, \sqrt{7})$ triangle with area $\frac{1}{2}\sqrt{10}$. Since $C(\mathcal{O}_{-10}) \cong \mathbb{Z}_2$, it follows from part 1 of the corollary that if this triangle were to embed in $\mathbb{Q}(\sqrt{-10})$, it would embed in $\mathcal{O}_{-10}$. However, it is easy to verify that $\mathcal{O}_{-10}$ contains no elements of norm 2, 5, or 7, so no embedding is possible. Thus, it cannot embed in $\mathbb{Q}(\sqrt{-10})$ either.

By part 2 of the corollary, if the square of every ideal in $\mathcal{O}_{-D}$ is principal, then every integer triangle of characteristic D embeds in $\mathcal{O}_{-D}$. We conjecture that these two conditions are equivalent:

Conjecture 1 Let D be a positive square-free integer. Then every integer triangle of characteristic D embeds in $\mathcal{O}_{-D}$ if and only if the square of every ideal in $\mathcal{O}_{-D}$ is principal.

For the forward direction of this conjecture, we have only been able to prove a weaker version:

Proposition 4 *Suppose that the square of some ideal of $\mathcal{O}_{-D}$ is non-principal. Then there exists an integer norm triangle with two integral edge lengths that has characteristic D but does not embed in $\mathcal{O}_{-D}$.*

Proof If $\mathcal{O}_{-D}$ contains an ideal whose square is not principal, then the same must be true of one of its prime ideal factors I_*. Since I_* is prime, there is a rational prime p such that $\langle p\rangle = I_*\bar{I}_*$. Moreover, by [3] there exists an ideal H where I_*H is principal and $\langle \bar{I}_*, H\rangle = \langle 1\rangle$. Let $I_*^2H^2 = \langle\alpha\rangle$.

Now, consider the triangle defined by the point set $\{0, \frac{\alpha}{p}, p\}$. Since the triangle embeds in $\mathbb{Q}(\sqrt{-D})$, by Proposition 2 it has characteristic D. Also, note that $[\frac{\alpha}{p}] = [H]^2$ and $[p] = p^2$ are both perfect squares, and

$$\left[\tfrac{\alpha}{p} - p\right] = [H]^2 + p^2 - (\alpha + \bar{\alpha})$$

is an integer.

In the terminology of Theorem 1, we have a triangle

$$\mathcal{M} = \left\{0, \tfrac{\alpha}{p}, p\right\} = \left\{0, \tfrac{\beta_1}{r}, \tfrac{\beta_2}{r}\right\}$$

with $r = p$, $\beta_1 = \alpha$, $\beta_2 = p^2$, $K_1 = H^2$, and $K_2 = \bar{I}_*^{\,2}$. Because $\langle \bar{I}_*, H\rangle = \langle 1\rangle$, we know that the only ideal J_* such that $J_* \mid K_1$ and $J_* \mid K_2$ is $J_* = \langle 1\rangle$. Thus $\mathcal{M}$ will embed in $\mathcal{O}_{-D}$ only if $I_*^2J_*^2 = I_*^2$ is principal. However, I_*^2 is not principal. □

We have been unable to find a general construction of an integer triangle that does not embed in $\mathcal{O}_{-D}$ for all square-free D with $C(\mathcal{O}_{-D}) \not\cong \mathbb{Z}_2^k$. However, computer searches verify our conjecture holds for all $D < 325{,}000$. The table below gives examples of integer triangles of characteristic D that do not embed in $\mathcal{O}_{-D}$; these triangles have their longest side as small as possible.

D	Triangle	D	Triangle	D	Triangle
14	(3, 5, 6)	46	(11, 15, 20)	71	(18, 25, 28)
17	(9, 11, 14)	47	(10, 16, 21)	73	(28, 55, 63)
23	(4, 9, 10)	53	(23, 38, 45)	74	(22, 25, 27)
26	(7, 9, 10)	55	(2, 6, 7)	77	(3, 12, 13)
29	(15, 21, 22)	59	(7, 25, 27)	79	(20, 26, 33)
31	(5, 12, 14)	61	(33, 40, 49)	82	(21, 26, 35)
34	(5, 14, 15)	62	(15, 21, 26)	83	(17, 29, 37)
38	(9, 14, 15)	65	(3, 11, 12)	86	(25, 27, 34)
39	(2, 5, 6)	66	(5, 7, 10)	87	(7, 10, 12)
41	(19, 30, 33)	69	(14, 15, 17)	89	(50, 63, 65)

5.2 When $\mathcal{O}_{-D}$ is a PID

In this section, we give a less restrictive embedding condition than Corollary 1 in the case that $\mathcal{O}_{-D}$ is one of the nine PIDs. In particular, it does not assume that $\mathcal{M}$ already embeds in $\mathbb{Q}(\sqrt{-D})$:

Theorem 3 *Suppose an integer norm point set $\mathcal{M}$ has characteristic D, and $\mathcal{O}_{-D}$ is a PID. Let s be the greatest common divisor of the norms of the edges in $\mathcal{M}$. Then $\mathcal{M}$ embeds in $\mathcal{O}_{-D}$ if and only if every rational prime p which is also prime in $\mathcal{O}_{-D}$ divides s with even multiplicity. In particular, every primitive integer norm point set with characteristic D embeds in $\mathcal{O}_{-D}$.*

The proof follows two lemmas, neither of which requires that $\mathcal{O}_{-D}$ be a PID.

Lemma 4 *Let $\mathcal{M}$ be a primitive integer norm point set with characteristic D. If p is a rational prime that is also prime in $\mathcal{O}_{-D}$, then p divides the norm of each edge in $\mathcal{M}$ with even multiplicity.*

Proof Translate and rotate $\mathcal{M}$ in the plane so that p divides the norm of $\beta \in \mathcal{M}$ lying on the positive x-axis, as in Fig. 4. We assume for contradiction that p divides $[\beta]$ with odd multiplicity, so there exist positive integers c and k such that $\beta = \sqrt{p^{2k-1}c}$ and $\gcd(p, c) = 1$.

Let $\alpha = x + yi$ be any other point in $\mathcal{M}$. We will show that α takes the form

$$\alpha = \frac{\delta\sqrt{p}}{2\sqrt{c}}$$

for some $\delta \in \mathcal{O}_{-D}$. Since $[\alpha]$, $[\beta]$, and $[\alpha - \beta]$ are integers, we know that

$$[\alpha] + [\beta] - [\alpha - \beta] = 2\,\mathrm{Re}(\alpha\bar{\beta}) = 2x\sqrt{p^{2k-1}c} = a$$

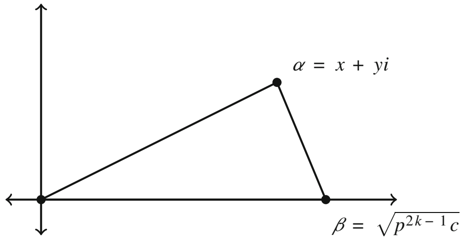


Fig. 4 The rational prime p divides $[\beta]$

for some $a \in \mathbb{Z}$. Also, the area of the triangle formed by 0, α, and β is

$$\tfrac{1}{2}y\sqrt{p^{2k-1}c} = \tfrac{b}{4}\sqrt{D}$$

for some $b \in \mathbb{Z}$.

If we let $\gamma = a + b\sqrt{-D} \in \mathcal{O}_{-D}$, we have $(2\sqrt{p^{2k-1}c})\alpha = \gamma$, and thus $p^{2k-1} \mid [\gamma] = \gamma\bar{\gamma}$. Since p is prime in $\mathcal{O}_{-D}$, we must have $p^k \mid \gamma$. Thus $\gamma = p^k\delta$ for some $\delta \in \mathcal{O}_{-D}$, which leads to the form for α displayed above.

We now show that p divides both $[\alpha]$ and $[\alpha - \beta]$. From $4c[\alpha] = p[\delta]$ we find that $p \mid [\alpha]$, regardless of whether p is 2 or odd. Also, since

$$\begin{aligned}[\alpha - \beta] &= [\alpha] + [\beta] - (\alpha\bar{\beta} + \bar{\alpha}\beta) = [\alpha] + [\beta] - \sqrt{p^{2k-1}c}\big(\tfrac{\delta\sqrt{p}}{2\sqrt{c}} + \tfrac{\overline{\delta\sqrt{p}}}{2\sqrt{c}}\big)\\ &= [\alpha] + [\beta] - p^k\,\mathrm{Re}(\delta),\end{aligned}$$

and since p divides all three of these terms, p divides $[\alpha - \beta]$.

Now, since α was an arbitrary point in $\mathcal{M}$ other than 0 or β, we know if we take some other point $\eta \in \mathcal{M}$, p will divide both $[\eta]$ and $[\eta - \beta]$. The point η will take the form $\eta = \frac{\varepsilon\sqrt{p}}{2\sqrt{c}}$ for some $\varepsilon \in \mathcal{O}_{-D}$, and thus

$$p\frac{[\delta - \varepsilon]}{4c} = [\alpha - \eta],$$

which leads to $p \mid [\alpha - \eta]$, regardless of whether p is 2 or odd. So p divides the norms of the edges in $\mathcal{M}$, contradicting our assumption that $\mathcal{M}$ is primitive. □

Lemma 5 *Let $\mathcal{M}$ be an integer norm point set with characteristic D, and let s be the greatest common divisor of the norms of the edges in M. Then every rational prime p which is also prime in $\mathcal{O}_{-D}$ divides s with even multiplicity if and only if for each edge $\alpha \in \mathcal{M}$ there exists an ideal $L \subset \mathcal{O}_{-D}$ such that $\langle[\alpha]\rangle = L\bar{L}$.*

Proof Let α be an edge in $\mathcal{M}$. Scale $\mathcal{M}$ by $1/\sqrt{s}$ to obtain a primitive integer norm point set $\mathcal{M}'$ with $\frac{\alpha}{\sqrt{s}} \in \mathcal{M}'$. By Lemma 4, every rational prime which is also prime in $\mathcal{O}_{-D}$ divides $[\frac{\alpha}{\sqrt{s}}] = \frac{[\alpha]}{s}$ with even multiplicity. Thus, $\langle[\alpha]\rangle$ factors as

$$\langle[\alpha]\rangle = \langle s\rangle\langle\tfrac{[\alpha]}{s}\rangle = (\langle p_1\rangle^{j_1}\cdots\langle p_u\rangle^{j_u}J\bar{J})(\langle q_1\rangle^{2k_1}\cdots\langle q_v\rangle^{2k_v}K\bar{K})$$

for some ideals J and K, where the p_i are the distinct rational primes dividing s that are also primes in $\mathcal{O}_{-D}$, and the q_i are those dividing $[\alpha]/s$. This factorization of $\langle[\alpha]\rangle$ equals $L\bar{L}$ for some ideal L if and only if each j_i is even, since each $\langle p_i\rangle$ needs to be a factor of both L and $\bar{L}$. ◻

We remark that if $\mathcal{O}_{-D}$ is a PID, it contains an element of norm $[\alpha]$ if and only if $\langle[\alpha]\rangle = L\bar{L}$ for some principal ideal L. We are now in position to prove Theorem 3.

Proof If some rational prime p which is also prime in $\mathcal{O}_{-D}$ does not divide s with even multiplicity, then Lemma 5 implies that $\langle[\alpha]\rangle$ does not factor as $L\bar{L}$ for each edge $\alpha \in \mathcal{M}$. This means that no edge of $\mathcal{M}$ is in $\mathcal{O}_{-D}$, so $\mathcal{M}$ doesn't embed in $\mathcal{O}_{-D}$.

For the other direction, suppose every rational prime p which is also prime in $\mathcal{O}_{-D}$ divides s with even multiplicity. Then by Lemma 5 each edge $\alpha \in \mathcal{M}$ leads to $\langle[\alpha]\rangle = L\bar{L}$ for some principal ideal L. So for any non-zero $\alpha' \in \mathcal{M}$, there is a rotation ϕ of $\mathcal{M}$ about the origin such that $\phi(\alpha') \in \mathcal{O}_{-D} \subseteq \mathbb{Q}(\sqrt{-D})$. By Proposition 3, $\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$; and since the square of every ideal of $\mathcal{O}_{-D}$ is principal, Corollary 1 implies that $\mathcal{M}$ embeds in $\mathcal{O}_{-D}$. ◻

6 Examples

In this section we apply Theorems 1 and 2 to two integer triangles, one primitive and one imprimitive.

Consider the primitive integer triangle (7, 11, 14) with area $12\sqrt{10}$, so $D = 10$. It can be embedded in $\mathbb{Q}(\sqrt{-10})$ with a side on the x-axis as shown on the right of Fig. 5. Since $C(\mathcal{O}_{-10}) \cong \mathbb{Z}_2$, by Theorem 2 we know this triangle embeds in $\mathcal{O}_{-10}$.

We set

$$\mathcal{M} = \left\{0, 14, \tfrac{67}{7} + \tfrac{12}{7}\sqrt{-10}\right\} = \left\{0, \tfrac{98}{7}, \tfrac{67+12\sqrt{-10}}{7}\right\},$$

so that $r = 7$, $\beta_1 = 98$, and $\beta_2 = 67 + 12\sqrt{-10}$. Note that

$$\langle r\rangle = \langle 7\rangle = \langle 7, 5 + \sqrt{-10}\rangle\langle 7, 2 + \sqrt{-10}\rangle = I_*\bar{I}_*,$$

where ${I_*}^2 = \langle 7, 5 + \sqrt{-10}\rangle^2 = \langle 3 + 2\sqrt{-10}\rangle$ is principal. Also note that

$$\langle\beta_1\rangle = \langle 3 + 2\sqrt{-10}\rangle\langle -6 + 4\sqrt{-10}\rangle = {I_*}^2 K_1$$

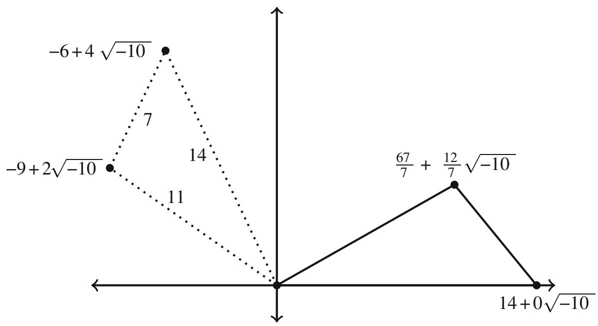
and

$$\langle\beta_2\rangle = \langle 3 + 2\sqrt{-10}\rangle\langle -9 + 2\sqrt{-10}\rangle = {I_*}^2 K_2.$$

Since ${\bar{I}_*}^2 = \langle -3 + 2\sqrt{-10}\rangle$, set $\varepsilon = \frac{-3}{7} + \frac{2}{7}\sqrt{-10}$. Since $[\varepsilon] = (\frac{-3}{7})^2 + (\frac{2}{7})^2 10 = 1$, $R(\tau) = \varepsilon\tau$ is a rotation about the origin for any $\tau \in \mathbb{C}$. We then find that

$$R\left(\tfrac{98}{7}\right) = -6 + 4\sqrt{-10}$$

Fig. 5 Embedding a (7, 11, 14) triangle in $\mathcal{O}_{-10}$



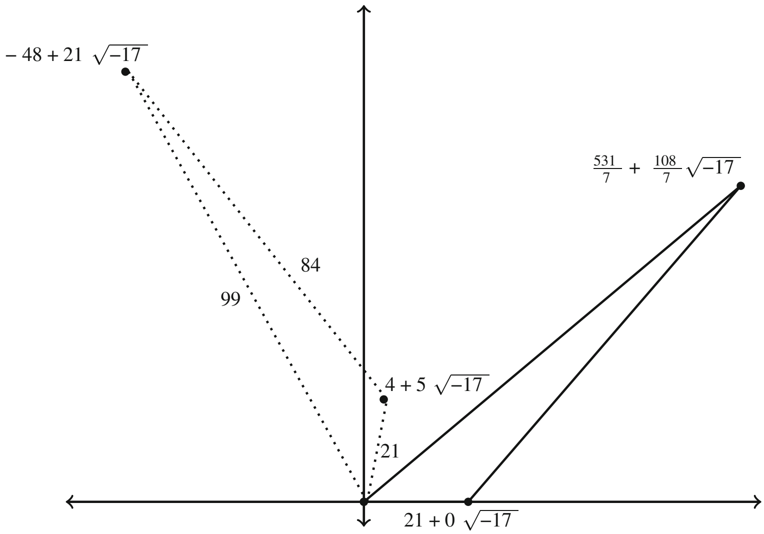


Fig. 6 Embedding a (21, 84, 99) triangle in $\mathcal{O}_{-17}$

and

$$R\left(\tfrac{67+12\sqrt{-10}}{7}\right) = -9 + 2\sqrt{-10},$$

so the triangle embeds as $\{0, -6 + 4\sqrt{-10}, -9 + 2\sqrt{-10}\}$, as shown on the left of Fig. 5.

We next apply Theorem 1 to the imprimitive integer triangle (21, 84, 99) with area $162\sqrt{17}$, so $D = 17$. It can be embedded in $\mathbb{Q}(\sqrt{-17})$ with an edge on the x-axis as shown on the right in Fig. 6. Since $C(\mathcal{O}_{-17}) \cong \mathbb{Z}_4$, Corollary 1 does not guarantee that the triangle embeds in $\mathcal{O}_{-17}$.

We set

$$\mathcal{M} = \left\{0, 21, \tfrac{531}{7} + \tfrac{108}{7}\sqrt{-17}\right\} = \left\{0, \tfrac{147}{7}, \tfrac{531+108\sqrt{-17}}{7}\right\},$$

so that $r=7$, $\beta_1=147$, and $\beta_2=531+108\sqrt{-17}$. Note that

$$\langle r\rangle=\langle 7\rangle=\langle 7,2+\sqrt{-17}\rangle\langle 7,5+\sqrt{-17}\rangle=I_*\bar{I}_*,$$

where ${I_*}^2=\langle 7,2+\sqrt{-17}\rangle^2=\langle 49,9+\sqrt{-17}\rangle$ is not principal. Also note that

$$\langle\beta_1\rangle=\langle 49,9+\sqrt{-17}\rangle\langle 147,120+3\sqrt{-17}\rangle={I_*}^2K_1$$

and

$$\langle\beta_2\rangle=\langle 49,9+\sqrt{-17}\rangle\langle 1089,135+9\sqrt{-17}\rangle={I_*}^2K_2.$$

Let $J_*=\langle 3,1+\sqrt{-17}\rangle$. Then $J_*\mid K_1,K_2$, and ${I_*}^2{J_*}^2=\langle -4+5\sqrt{-17}\rangle$ is principal. By Theorem 1, the triangle embeds in $\mathcal{O}_{-17}$.

Since ${\bar{I}_*}^2{\bar{J}_*}^2=\langle 4+5\sqrt{-17}\rangle$, set $\varepsilon=\frac{4}{21}+\frac{5}{21}\sqrt{-17}$. Since $[\varepsilon]=(\frac{4}{21})^2+(\frac{5}{21})^2 17=1$, $R(\tau)=\varepsilon\tau$ is a rotation about the origin for any $\tau\in\mathbb{C}$. We then find that

$$R\left(\tfrac{147}{7}\right)=4+5\sqrt{-17}$$

and

$$R\left(\tfrac{531+108\sqrt{-17}}{7}\right)=-48+21\sqrt{-17},$$

so the triangle embeds as $\{0,4+5\sqrt{-17},-48+21\sqrt{-17}\}$ as shown on the left of Fig. 6.

Acknowledgments We thank Sascha Kurz for introducing us to this problem in the context of his work on integer distance problems, and for confirming Conjecture 1 numerically. We thank several anonymous referees for their helpful corrections and suggestions to improve the exposition. We also thank Kiran Kedlaya for pointing out a connection between the 65 characteristics listed in Sect. 5.1 and Euler's idoneal numbers (see Sect. 2.6 of [7]). Supported by NSF Grant DMS-1063070.

References

1. Beeson, M.: Triangles with vertices on lattice points. Am. Math. Mon. **99**, 243–252 (1992)
2. Brass, P., Moser, W., Pach, J.: Research Problems in Discrete Geometry. Springer, New York (2005)
3. Cohn, H.: Advanced Number Theory. Dover, New York (1980)
4. Conway, J., Radin, C., Sadun, L.: On angles whose squared trigonometric functions are rational. Discrete Comput. Geom. **22**, 321–332 (1999)
5. Fricke, J.: On Heronian simplices and integer embedding. arXiv:math/0112239v1 (2001)
6. Guy, R.: Unsolved Problems in Number Theory, 3rd edn. Springer, New York (2004)
7. Kani, E.: Idoneal numbers and some generalizations. Ann. Sci. Math. Qué. **35**, 197–227 (2011)
8. Kemnitz, A.: Punktmengen mit ganzzahligen Abständen. Habilitationsschrift. TU Braunschweig, Braunschweig (1988)
9. Kreisel, T., Kurz, S.: There are integral heptagons, no three points on a line, no four on a circle. Discrete Comput. Geom. **39**, 786–790 (2008)
10. Kurz, S.: On the characteristic of integral point sets in $\mathbb{E}^m$. Australas. J. Comb. **36**, 241–248 (2006)

11. Kurz, S., Noll, L., Rathbun, R., Simmons, C.: Constructing 7-clusters. Serdica J. Comput. **8**, 47–70 (2014)
12. Lunnon, F.: Lattice embedding of Heronian simplices. arXiv:1202.3198v2 (2012)
13. Marshall, S., Perlis, A.: Heronian tetrahedra are lattice tetrahedra. Am. Math. Mon. **120**, 140–149 (2013)
14. Noll, L., Bell, D.: n-Clusters for $1 < n < 7$. Math. Comput. **53**, 439–444 (1989)
15. Solymosi, J., de Zeeuw, F.: On a question of Erdős and Ulam. Discrete Comput. Geom. **43**, 393–401 (2010)
16. Stark, H.M.: On the 'gap' in a theorem of Heegner. J. Number Theory **1**, 16–27 (1969)
17. Weinberger, P.J.: Exponents of the class groups of complex quadratic fields. Acta Arith. **22**, 117–124 (1973)
18. Yiu, P.: Heronian triangles are lattice triangles. Am. Math. Mon. **108**, 261–263 (2001)