Lattice Embeddings of Planar Point Sets

Michael Knopf · Jesse Milzman · Derek
Smith · Dantong Zhu · Dara Zirlin

Abstract Let $\mathcal{M}$ be a finite non-colinear set of points in the Euclidean plane, with the squared distance between each pair of points integral. Identifying the plane with $\mathbb{C}$, there is at most one positive square-free integer D such that a congruent copy of $\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$. Generalizing the work of Yiu and Fricke on embedding point sets in $\mathbb{Z}^2$ (the case when $D = 1$), we determine when $\mathcal{M}$ embeds in the lattice corresponding to $\mathcal{O}_{-D}$, the maximal order in $\mathbb{Q}(\sqrt{-D})$. In particular, we show that if the square of every ideal in $\mathcal{O}_{-D}$ is principal and if the distance between at least one pair of points in $\mathcal{M}$ is integral, then $\mathcal{M}$ embeds in $\mathcal{O}_{-D}$.

Michael Knopf
University of California, Berkeley

Jesse Milzman
University of Maryland

Derek Smith
Lafayette College
Easton, PA 18042
Tel.: 610-330-5283
Fax.: 610-330-5721
E-mail: smithder@lafayette.edu

Dantong Zhu
Lafayette College

Dara Zirlin
University of Illinois, Urbana-Champaign

1 Introduction

Many classical 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, Moser, and Pach [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 3 on a line and no 4 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 $\mathbb{Z}^2$ [14], [11]. These n-clusters satisfy another integrality condition, namely that any triple of non-colinear 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 complex 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 complex 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 [17], 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 Figure 1, which has only non-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 Figure 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
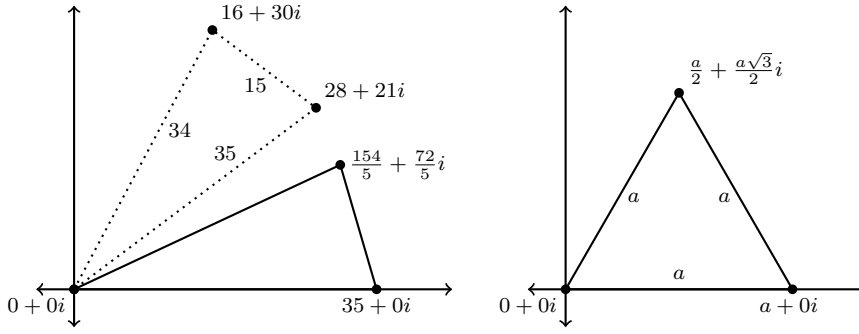
Fig. 1 A $(15, 34, 35)$ triangle, and an equilateral triangle of side length a. We identify the point (a, b) in the plane with the complex number $a + bi$. On the left, the solid triangle is rotated to the dotted triangle via multiplication by $\frac{4}{5} + \frac{3}{5}i$.

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 maximal order of $\mathbb{Q}(\sqrt{-3})$.

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 maximal order of an appropriate quadratic extension of $\mathbb{Q}$. For instance, here is a restatement of the second part of Corollary 1 in Section 5.1:

> Let $\mathcal{M}$ be a finite non-colinear 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 maximal order $\mathcal{O}_{-D}$ of $\mathbb{Q}(\sqrt{-D})$ 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 Figure 2.

The structure of this paper is as follows. In Section 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 Section 4 presents our main results about embedding point sets in maximal orders. 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 Section 6.

2 Notation and Number Theory Preliminaries

Unless otherwise stated, for the remainder of this article $\mathcal{M}$ refers to a non-colinear 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
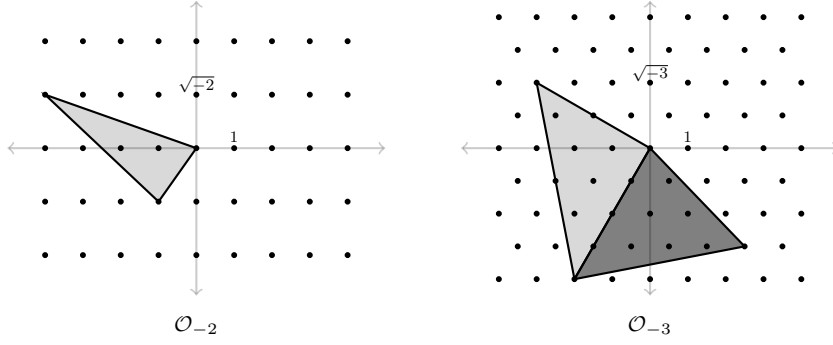
Fig. 2 On the left is a $(\sqrt{3},\ \sqrt{17},\ \sqrt{18})$ triangle with area $\frac{5}{2}\sqrt{2}$ embedded in $\mathcal{O}_{-2}$. The lighter triangle of the quadrilateral embedded in $\mathcal{O}_{-3}$ on the right has area $3\sqrt{3}$ and the darker one has area $4\sqrt{3}$; the three edge lengths of the lighter triangle are $\sqrt{12}$, $\sqrt{16}$, and $\sqrt{28}$, and the remaining three edge lengths are $\sqrt{13}$, $\sqrt{21}$, and $\sqrt{49}$.

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 maximal order $\mathcal{O}_{-D}$ 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 maximal order in this field:

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

where

$$\omega = \begin{cases} \sqrt{-D} & \text{if } D \not\equiv 3 \pmod{4} \\ \frac{1+\sqrt{-D}}{2} & \text{if } D \equiv 3 \pmod{4}. \end{cases}$$

For $D \equiv 3 \pmod{4}$, an equivalent definition is

$$\mathcal{O}_{-D} = \left\{ \frac{c + d\sqrt{-D}}{2} \mid c, d \in \mathbb{Z},\ c \equiv d \pmod{2} \right\}.$$

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.

The *norm* of a complex number $\alpha = a + bi$ is $[\alpha] = |\alpha|^2 = a^2 + b^2$. Defining the conjugate of α as $\overline{\alpha} = a - bi$, we have $[\alpha] = \alpha\overline{\alpha}$ along with several other useful identities: $\overline{\overline{\alpha}} = \alpha$, $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$, $[\alpha][\beta] = [\alpha\beta]$, $[\alpha - \beta] = [\alpha] + [\beta] - (\alpha\overline{\beta} + \overline{\alpha}\beta)$, and $\alpha + \overline{\alpha} = 2\mathrm{Re}(\alpha)$, which is a rational integer when $\alpha \in \mathcal{O}_{-D}$. In the field $\mathbb{Q}(\sqrt{-D})$, the norm of an element $a + b\sqrt{-D}$ takes the form $\left[a + b\sqrt{-D}\right] = a^2 + Db^2$; when restricted to the ring $\mathcal{O}_{-D}$, it is non-negative and integer-valued.

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 $\overline{\alpha} \mid \overline{\beta}$ as well. Since any rational integer r is its own conjugate, $r \mid \alpha$ if and only if $r \mid \overline{\alpha}$. 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: $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. The only orders $\mathcal{O}_{-D}$ that are UFDs have $D = 1, 2, 3, 6, 7, 11, 19, 43, 167$; these nine orders 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 $\overline{I}$, and $I\overline{I}$ 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 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 $I\overline{J}$ 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.

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 square-free integer D. Propositions 1 and 2 are not new (see [8], [15]), but short proofs are given to keep the paper self-
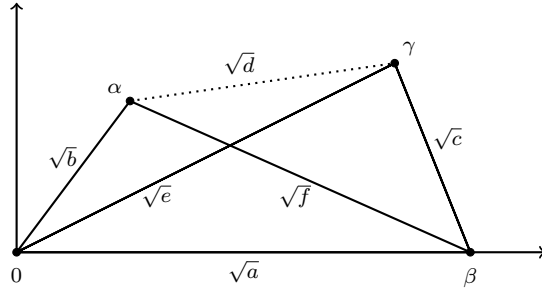
Fig. 3 If two triangles share an edge, their characteristics are equal.

contained; Proposition 3 will be used in the proof of Theorem 3 in section 5.2. As stated in the previous section, we assume that $\mathcal{M}$ is non-colinear and contains the origin.

Suppose that T is a triangle in $\mathcal{M}$ with side lengths (a, b, c); any triangle mentioned in this article is non-degenerate. By Heron's formula,

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

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 and $\mathcal{M}$ is as depicted in Figure 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:

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

Thus,

$$d = \left(\frac{a+b-f}{2\sqrt{a}} - \frac{a+e-c}{2\sqrt{a}} \right)^2 + \left(\frac{2p\sqrt{D}}{\sqrt{a}} - \frac{2q\sqrt{E}}{\sqrt{a}} \right)^2$$

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

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 embedability 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

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

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

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

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

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

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 $\beta \in \mathbb{Q}(\sqrt{-D})$.

For an example of an integer norm triangle of characteristic 10 that does not embed in $\mathbb{Q}(\sqrt{-10})$, see section 5.1.

4 Quadratic Order 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 will we 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 $\alpha \in \mathcal{O}_{-D}$ such that $p \nmid \alpha$ but $p^2 \mid [\alpha]$. Then $\langle p \rangle = I\overline{I}$ for two distinct conjugate prime ideals $I, \overline{I} \subset \mathcal{O}_{-D}$.*

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 $p^2 \mid \alpha\overline{\alpha}$ implies $p \mid \alpha\overline{\alpha}$, we have $p \mid \alpha$ or $p \mid \overline{\alpha}$. 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 $\alpha\overline{\alpha} = p^2 m$ for some $m \in \mathbb{Z}$, $\langle \alpha \rangle \langle \overline{\alpha} \rangle = I^4 \langle m \rangle$. Since I is prime, $I^2 \mid \langle \alpha \rangle$ or $I^2 \mid \langle \overline{\alpha} \rangle$, so at least one of $\langle p \rangle \mid \langle \alpha \rangle$ and $\langle p \rangle \mid \langle \overline{\alpha} \rangle$ is true. Thus, $p \mid \alpha$ or $p \mid \overline{\alpha}$, either of which implies $p \mid \alpha$, a contradiction.

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 $\mathcal{M} = \{0, \frac{\alpha_1}{r_1}, ..., \frac{\alpha_n}{r_n}\}$, 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

$$\mathcal{M} = \{0, \frac{\beta_1}{r}, ..., \frac{\beta_n}{r}\},$$

where the greatest common rational integer factor of $\beta_1, ..., \beta_n$, 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 $\left[\frac{\beta_i}{r}\right] \in \mathbb{Z}$ for all i, we know that $r^2 \mid [\beta_i] = \beta_i\overline{\beta_i}$ for all i. Second, since $\left[\frac{\beta_i}{r} - \frac{\beta_j}{r}\right] \in \mathbb{Z}$ for all i and j, we know that

$$r^2 \mid [\beta_i - \beta_j] = [\beta_i] + [\beta_j] - (\beta_i\overline{\beta_j} + \overline{\beta_i}\beta_j),$$

and thus $r^2 \mid \beta_i\overline{\beta_j} + \overline{\beta_i}\beta_j = 2\mathrm{Re}(\beta_i\overline{\beta_j})$ for all i and j.

Lemma 2 *Suppose that the interger norm point set $\mathcal{M}$ embeds in $\mathbb{Q}(\sqrt{-D})$, so that $\mathcal{M} = \{0, \frac{\beta_1}{r}, ..., \frac{\beta_n}{r}\}$, as defined above. Then there is a unique ideal I_* such that $\langle r \rangle = I_*\overline{I_*}$ and such that for each i, $\langle \beta_i \rangle = I_*^2 K_i$ for some ideal K_i. If $r \neq 1$, then $I_* \neq \overline{I_*}$.*

Proof If $r = 1$, we can let $I_* = \langle 1 \rangle$, for clearly $\langle r \rangle = \langle 1 \rangle \overline{\langle 1 \rangle}$ 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 $\beta_1, ..., \beta_n$, 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 $\langle p_i \rangle = I_i \overline{I_i}$ for two distinct conjugate prime ideals $I_i, \overline{I_i}$. Thus,

$$I_i^{2c_i} \overline{I_i}^{2c_i} = \langle p_i^{2c_i} \rangle \mid \langle \beta_j \overline{\beta_j} \rangle = \langle \beta_j \rangle \langle \overline{\beta_j} \rangle .$$

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

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

$$I_i^{2c_i} \mid \langle p_i^{2c_i} \rangle \mid \langle \beta_j \overline{\beta_k} + \overline{\beta_j} \beta_k \rangle ,$$

and so $\beta_j \overline{\beta_k} + \overline{\beta_j} \beta_k \in I_i^{2c_i}$. 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, $\beta_j \overline{\beta_k} \in I_i^{2c_i}$. Thus,

$$(\beta_j \overline{\beta_k} + \overline{\beta_j} \beta_k) - \beta_j \overline{\beta_k} = \overline{\beta_j} \beta_k \in I_i^{2c_i} ,$$

and so $I_i^{2c_i} \mid \langle \overline{\beta_j} \beta_k \rangle = \langle \overline{\beta_j} \rangle \langle \beta_k \rangle$. Since $I_i \nmid \langle \overline{\beta_j} \rangle$, 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

$$I_* \overline{I_*} = I_1^{c_1} \overline{I_1}^{c_i} \ldots I_m^{c_m} \overline{I_m}^{c_m} = \langle p_1^{c_1} \rangle \ldots \langle p_m^{c_m} \rangle = \langle r \rangle$$

and

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

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

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 $\mathcal{M} = \{0, \frac{\beta_1}{r}, ..., \frac{\beta_n}{r}\} \subseteq \mathbb{Q}(\sqrt{-D})$ 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 $\overline{I_*}^2 \overline{J_*}^2$; so there exists $\sigma \in \mathcal{O}_{-D}$ such that $\overline{I_*}^2 \overline{J_*}^2 = \langle \sigma \rangle$, where $|\sigma| = [I_*][J_*]$. Thus for each i,

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

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

Let $\epsilon = \frac{\sigma}{|\sigma|}$, and define the rotation $R(\tau) = \epsilon\tau$ for all $\tau \in \mathbb{C}$. Then

$$R(\frac{\beta_i}{r}) = \epsilon\frac{\beta_i}{r} = \frac{\sigma\beta_i}{|\sigma|r} \in \mathcal{O}_{-D}$$

for all i, which means that $\mathcal{M}$ embeds in $\mathcal{O}_{-D}$.

For the other half of the proof, suppose that after embedding $\mathcal{M}$ we have $\epsilon\frac{\beta_i}{r} = \gamma_i \in \mathcal{O}_{-D}$ for all i, where $\epsilon = \frac{\sigma}{|\sigma|}$ 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 $\langle\overline{\gamma_1}\rangle\langle\gamma_1\rangle = \overline{K_1}K_1$, we know that $\overline{F}F = \overline{J_*}J_*$. Since $\langle F, J_*\rangle = \langle\overline{F}, \overline{J_*}\rangle = \langle 1\rangle$, we get $\overline{F} = J_*$. From $\langle\overline{\gamma_1}\rangle\langle\gamma_1\rangle = \overline{K_1}K_1$ we deduce that $J_*\langle\gamma_1\rangle = \overline{J_*}K_1$.

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

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

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

Finally, note that

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

so $\overline{J_*}^2 K_1$ is principal. Since $\langle\beta_i\rangle = I_*^2 K_1$ is also principal, $\overline{J_*}^2 K_1 \sim I_*^2 K_1$. Thus $I_*^2 \sim \overline{J_*}^2$, 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 a lemma that uses the fact that $\frac{\beta_j\overline{\beta_k}}{r^2} \in \mathcal{O}_{-D}$ for all j and k, which follows from Lemma 2 and

$$\langle\beta_j\overline{\beta_k}\rangle = I_*^2 K_j \overline{I_*}^2 \overline{K_k} = r^2 K_j \overline{K_k} \in r^2\mathcal{O}_{-D}.$$

Lemma 3 *Let $K = \langle K_1, ..., K_n\rangle$. 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

$$\langle \beta_i \rangle \langle \overline{\beta_j} \rangle = I_*^2 K_i \overline{I_*}^2 \overline{K_j}$$
$$= [I_*]^2 K\overline{K} Y_i \overline{Y_j}$$
$$= r^2 [K] Y_i \overline{Y_j}$$

for all i and j. This means that $\left\langle \frac{\beta_i \overline{\beta_j}}{r^2} \right\rangle = [K] Y_i \overline{Y_j}$, and thus $[K] \mid \frac{\beta_i \overline{\beta_j}}{r^2} \in \mathcal{O}_{-D}$.

We now know that

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

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 that the integer norm point set $\mathcal{M} = \{0, \frac{\beta_1}{r}, ..., \frac{\beta_n}{r}\} \subseteq \mathbb{Q}(\sqrt{-D})$ 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 $\langle K_1, ..., K_n \rangle = \langle 1 \rangle$, 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 orders $\mathcal{O}_{-D}$ 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 ([16], [7]):

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 $\langle p \rangle = I_* \overline{I_*}$. Moreover, by [3] there exists an ideal H where $I_* H$ is principal and $\langle \overline{I_*}, H \rangle = \langle 1 \rangle$. Let $I_*^2 H^2 = \langle \alpha \rangle$.

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 characterisic D. Also, note that $\left[\frac{\alpha}{p}\right] = [H]^2$ and $[p] = p^2$ are both perfect squares, and

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

is an integer.

In the terminology of Theorem 1, we have a triangle

$$\mathcal{M} = \{0, \frac{\alpha}{p}, p\} = \{0, \frac{\beta_1}{r}, \frac{\beta_2}{r}\}$$

with $r = p$, $\beta_1 = \alpha$, $\beta_2 = p^2$, $K_1 = H^2$, and $K_2 = \overline{I_*}^2$. Because $\langle \overline{I_*}, H \rangle = \langle 1 \rangle$, 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 $I_*^2 J_*^2 = I_*^2$ 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 such that $C(\mathcal{O}_{-D}) \not\cong \mathbb{Z}_2^k$. 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 $\mathcal{M}$ 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.
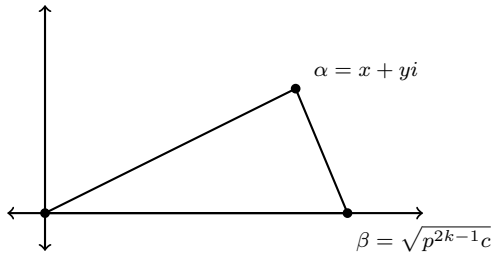
Fig. 4 The rational prime p divides $[\beta]$.

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 Figure 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

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

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

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

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 $p^{2k-1} \mid [\gamma] = \gamma\overline{\gamma}$. 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 $p|[\alpha]$, regardless of whether p is 2 or odd. Also, since

$$[\alpha - \beta] = [\alpha] + [\beta] - (\alpha\overline{\beta} + \overline{\alpha}\beta) = [\alpha] + [\beta] - \sqrt{p^{2k-1}c}\left(\frac{\delta\sqrt{p}}{2\sqrt{c}} + \frac{\overline{\delta\sqrt{p}}}{2\sqrt{c}}\right)$$

$$= [\alpha] + [\beta] - p^k\mathrm{Re}(\delta),$$

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 $\eta = \dfrac{\varepsilon\sqrt{p}}{2\sqrt{c}}$ for some $\varepsilon \in \mathcal{O}_{-D}$, and thus

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

which leads to $p|[\alpha - \eta]$ 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 $\langle[\alpha]\rangle = L\overline{L}$.*

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 $\left[\frac{\alpha}{\sqrt{s}}\right] = \frac{[\alpha]}{s}$ with even multiplicity. Thus, $\langle[\alpha]\rangle$ factors as

$$\langle[\alpha]\rangle = \langle s \rangle \left\langle \frac{[\alpha]}{s} \right\rangle = (\langle p_1 \rangle^{j_1} \cdots \langle p_u \rangle^{j_u} \, J\overline{J})(\langle q_1 \rangle^{2k_1} \cdots \langle q_v \rangle^{2k_v} \, K\overline{K})$$

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 $L\overline{L}$ 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 $\overline{L}$.

We remark that if $\mathcal{O}_{-D}$ is a PID, it contains an element of norm $[\alpha]$ if and only if $\langle[\alpha]\rangle = L\overline{L}$ 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 $L\overline{L}$ 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 $\langle[\alpha]\rangle = L\overline{L}$ 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 Figure 5. Since $\mathcal{O}_{-10} \cong \mathbb{Z}_2$, by Theorem 2 we know this triangle embeds in $\mathcal{O}_{-10}$.

We set

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

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

$$\langle r \rangle = \langle 7 \rangle = \langle 7, 5 + \sqrt{-10} \rangle \langle 7, 2 + \sqrt{-10} \rangle = I_* \overline{I_*},$$
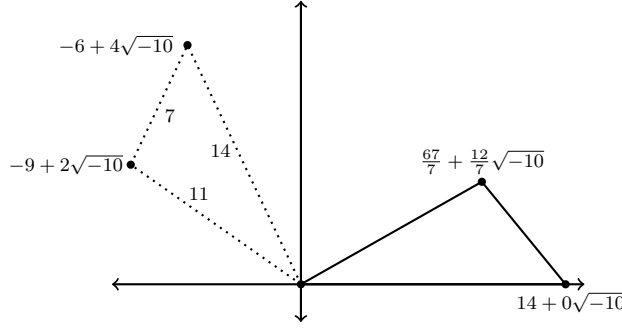
Fig. 5 Embedding a $(7, 11, 14)$ triangle in $\mathcal{O}_{-10}$.

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

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

and

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

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

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

and

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

so the triangle embeds as $\left\{ 0, -6 + 4\sqrt{-10}, -9 + 2\sqrt{-10} \right\}$, as shown on the left of Figure 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 Figure 6. Since $\mathcal{O}_{-17} \cong \mathbb{Z}_4$, Corollary 1 does not guarantee that the triangle embeds in $\mathcal{O}_{-17}$.

We set

$$\mathcal{M} = \left\{ 0, 21, \frac{531}{7} + \frac{108}{7}\sqrt{-17} \right\} = \left\{ 0, \frac{147}{7}, \frac{531 + 108\sqrt{-17}}{7} \right\},$$
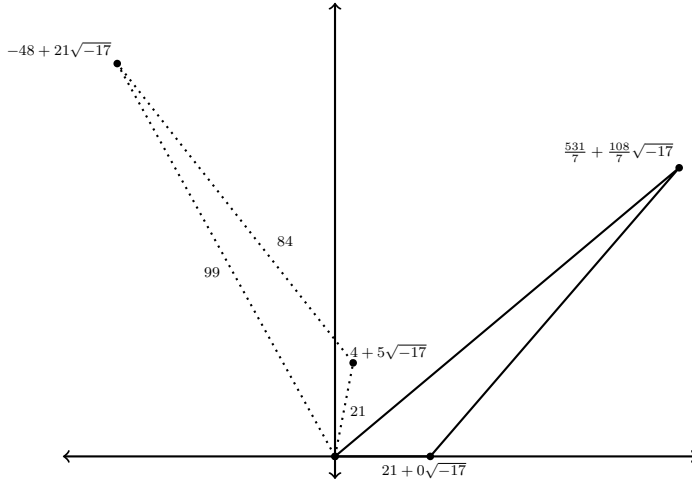
so that $r = 7$, $\beta_1 = 147$, and $\beta_2 = 531 + 108\sqrt{-17}$. Note that

$$\langle r \rangle = \langle 7 \rangle = \left\langle 7, 2 + \sqrt{-17} \right\rangle \left\langle 7, 5 + \sqrt{-17} \right\rangle = I_* \overline{I_*},$$

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

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

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

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

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 $\overline{I_*}^2 \overline{J_*}^2 = \langle 4 + 5\sqrt{-17} \rangle$, set $\epsilon = \frac{4}{21} + \frac{5}{21}\sqrt{-17}$. Since $[\epsilon] = \left(\frac{4}{21}\right)^2 + \left(\frac{5}{21}\right)^2 17 = 1$, $R(\tau) = \epsilon \tau$ is a rotation about the origin for any $\tau \in \mathbb{C}$. We then find that
$$R(\frac{147}{7}) = 4 + 5\sqrt{-17}$$

and
$$R(\frac{531 + 108\sqrt{-17}}{7}) = -48 + 21\sqrt{-17},$$

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

Acknowledgements

References

1. Michael Beeson, "Triangles with Vertices on Lattice Points," *The American Mathematical Monthly*, vol. 99, 1992, pp. 243-252.

2. Peter Brass, William Moser, and János Pach, *Research Problems in Discrete Geometry*, Springer, 2005.
3. Harvey Cohn, *Advanced Number Theory*, Dover, 1980.
4. John Conway, Charles Radin, and Lorenzo Sadun, "On Angles Whose Squared Trigonometric Functions are Rational," *Discrete and Computational Geometry*, vol. 22, 1999, pp. 321-332.
5. Jan Fricke, "On Heronian Simplices and Integer Embedding," arXiv:math/0112239v1 [math.NT] 21 Dec 2001.
6. Richard Guy, *Unsolved Problems in Number Theory*, 3rd edition, Springer, 2004.
7. Eike Hertel and Christian Richter, "Tiling Convex Polygons with Congruent Equilateral Triangles," *Discrete and Computational Geometry*, vol. 51, 2014, pp. 753-759.
8. A Kemnitz, *Punktmengen mit ganzzahligen Abständen*, Habilitationsschrift, TU Braunschweig, 1988.
9. Tobias Kreisel and Sascha Kurz, "There Are Integral Heptagons, no Three Points on a Line, no Four on a Circle," *Discrete and Computational Geometry*, vol. 39, 2008, pp. 786-790.
10. Sascha Kurz, "On the Characteristic of Integral Point Sets in $\mathbb{E}^m$", *The Australasian Journal of Combinatorics*, vol. 36, 2006, pp. 241-248.
11. Sascha Kurz, Landon Noll, Randall Rathbun, and Chuck Simmons, "Constructing 7-clusters," *Serdica Journal of Computing*, vol. 8, 2014, pp. 47-70.
12. Fred Lunnon, "Lattice Embedding of Heronian Simplices," arXiv:1202.3198v2 [math.MG] 1 July 2012.
13. Susan Marshall and Alexander Perlis, "Heronian Tetrahedra Are Lattice Tetrahedra," *The American Mathematical Monthly*, vol. 120, no. 2, February 2013, pp. 140-149.
14. Landon Noll and David Bell, "n-clusters for $1 < n < 7$," *Mathematics of Computation*, vol. 53, 1989, pp. 439-444.
15. Jozsef Solymosi and Frank de Zeeuw, "On a Question of Erdős and Ulam," *Discrete and Computational Geometry*, vol. 43, 2010, pp. 393-401.
16. PJ Weinberger, "Exponents of the class groups of complex quadratic fields," *Acta Arithmetica*, vol. 22, 1973, pp. 117-124.
17. Paul Yiu, "Heronian Triangles Are Lattice Triangles," *The American Mathematical Monthly*, vol. 108, no. 3, March 2001, pp. 261-263.