Visualize the Gaussian Integers

Timo Chang
timo65537@protonmail.com

Last edited: June 2, 2025

The quadratic field $\mathbb{Q}(i)$ possesses several great structures. For example, it is a norm-Euclidean field, which means that the field norm on $\mathbb{Q}(i)$ over $\mathbb{Q}$ induces a Euclidean function on its ring of integers $\mathbb{Z}[i]$, the Gaussian integers. In particular, this Euclidean function coincides with the complex norm, which allows us to visualize some properties of $\mathbb{Z}[i]$ on the complex plane. In this essay, we will examine several of them using this picutre.

1 Euclidean domain $\implies$ principal ideal domain

Definition 1.1. A *Euclidean function (norm)* on an integral domain D is a function $\nu : D \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that the following two conditions hold:

- For any $a, b \in D$ with $b \neq 0$, there exist $q, r \in D$ such that $a = bq + r$ where either $r = 0$ or $\nu(r) < \nu(b)$.
- For any non-zero $a, b \in D$, we have $\nu(a) \leq \nu(ab)$.

An integral domain is called a *Euclidean domain* if it has a Euclidean function.

Definition 1.2. An integral domain D is called a *principal ideal domain* if every ideal I in D is principal. That is, $I = (\alpha) = \alpha \cdot D$ for some $\alpha \in I$.

We have the following basic fact.

Theorem 1.3. *Every Euclidean domain is a principal ideal domain.*

Proof. Let D be a Euclidean domain with a Euclidean function ν, and I be a non-zero ideal in D. We choose $0 \neq b \in I$ which has minimal Euclidean norm among non-zero elements in I. We claim that b generates the ideal I. Suppose there is an element $a \in I$ that is not in (b). We write $a = bq + r$ for some $q, r \in D$ where either $r = 0$ or $\nu(r) < \nu(b)$. Note that r can not be 0 because otherwise we would have $a = bq \in (b)$. But if $\nu(r) < \nu(b)$, then it would contradict to our choice of b because we have $r = a - bq \in I$. Hence, we conclude that $I = (b)$. $\square$

The argument of this proof is fairly easy to understand. We now try to visualize it through the example of Gaussian integers $\mathbb{Z}[i]$.

Example 1.4. To begin with, we recall that a natural Euclidean function on $\mathbb{Z}[i]$ is given by the field norm on $\mathbb{Q}(i)$ (see [Fra03, Theorem 47.4]). That is, $N(u+vi) := u^2+v^2$ where $u, v \in \mathbb{Z}$. One sees that for any $z \in \mathbb{Z}[i]$, $N(z) = z \cdot \overline{z} = |z|^2$, where $\bar{\cdot}$ denotes the complex conjugation and $|\cdot|$ denotes the absolute value on $\mathbb{C}$. So the quantity $N(z)$ measures the distance from z to 0 on the complex plane. The smaller the norm is, the closer it is from the origin.

According to the proof of Theorem 1.3, any non-zero ideal I in $\mathbb{Z}[i]$ is generated by an element $b \in I$ where $N(b)$ is minimized among all non-zero elements in I. This means b is the closest from the origin among all non-zero elements in I. On the other hand, note that

$$(b) = \{n \cdot b + m \cdot ib \mid n, m \in \mathbb{Z}\}$$

consists of all $\mathbb{Z}$-linear combinations of b and ib. The operation "$+(n \cdot b)$" (resp. "$+(m \cdot ib)$") represents moving a point on the complex plane toward the direction $\vec{v}_1$ (see Figure 1) (resp. $\vec{v}_2$) for n (resp. m) steps, where each step is of length $|b|$. So any of their combination $n \cdot b + m \cdot ib$ represents the movement $n \cdot \vec{v}_1 + m \cdot \vec{v}_2$. Thus, when n, m run through all pairs of integers, the elements in (b) will form a lattice in the complex plane, as shown in Figure 1. In other words, the ideal $(b) \subseteq I$ consists of all vertices of the squares. (Figure 1 demonstrates the situation when $b = 1 - 2i$, but the other cases are similar.)

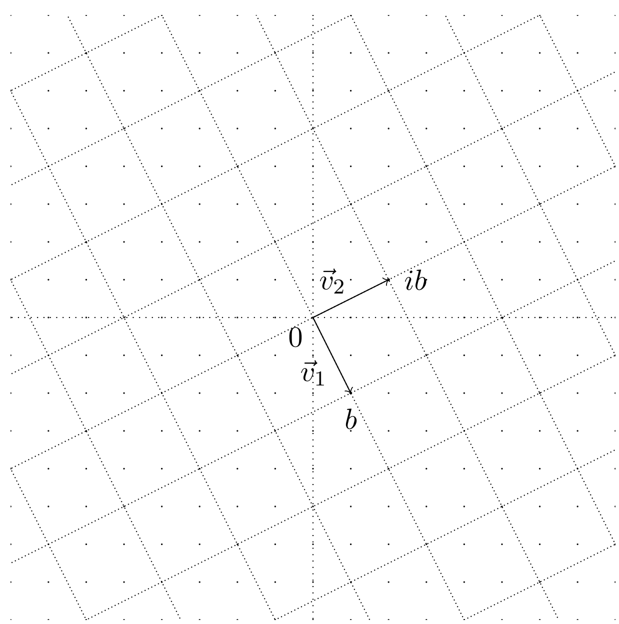

Figure 1

Now, if $(b) \subsetneq I$, then there exists an $a \in I$ but $a \notin (b)$. This means a is not one of the vertices (as in Figure 2). Since $\mathbb{Z}[i]$ is a Euclidean domain with a Euclidean function N, we may take $q, r \in \mathbb{Z}[i]$ such that $a = bq + r$ where either $r = 0$ or $N(r) < N(b)$.

Consider the inequality

$$N(r) = N(a - bq) < N(b).$$

Algebraically, it means that after doing the operation $-bq$ to the number a, its Euclidean norm $N(a-bq) = N(r)$ will become smaller than $N(b)$. But geometrically, this means that after moving around on the complex plane, the point a will arrive at r and become closer to the origin than b. That is, the final point r will lie in the circle centered at the origin with radius $|b|$. See Figure 2 below.

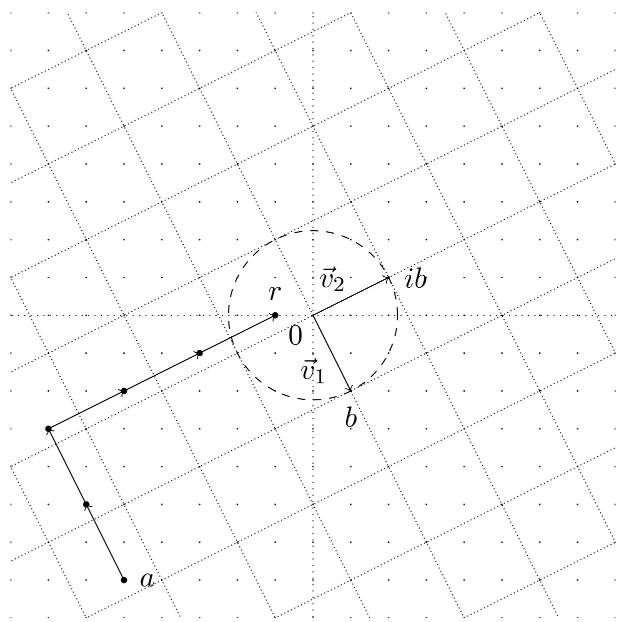

Figure 2

Note that since a is not one of the vertices, it will not end up at the origin. In other words, we have $r \neq 0$. Moreover, since $a \in I$ is moving along the directions $\vec{v}_1$ and $\vec{v}_2$, all of its stopping points (the black dots in Figure 2) are still in the ideal I. In particular, we have $r \in I$ and $N(r) < N(b)$. But this contradicts to our choice of b. Hence, we conclude that $I = (b)$.

Remark 1.5. The points $a, b \in \mathbb{Z}[i]$ are in fact $a = -5 - 7i$ and $b = 1 - 2i$. Thus, the path of a in Figure 2 also suggests that

$$a + (-2b + 3ib) = r = -1 \quad \text{and} \quad N(r) < N(b).$$

Or equivalently,

$$a = bq + r \quad \text{where} \quad q = 2 - 3i \quad \text{and} \quad r = -1.$$

This is the division algorithm on $\mathbb{Z}[i]$ induced from the Euclidean function N.

2 Finite Quotients of $\mathbb{Z}[i]$

Using the division algorithm on $\mathbb{Z}[i]$ mentioned above, one shows that the quotient of $\mathbb{Z}[i]$ by any ideal is a finite ring (see [Fra03, Exercise 47.15]). We now try to visualize this property on the complex plane.

Example 2.1. Lut us first consider the ideal $(b) = (1-2i)$ given in Example 1.4. We wish to count the cardinality of $\mathbb{Z}[i]/(1-2i)$. Considert the following figure.

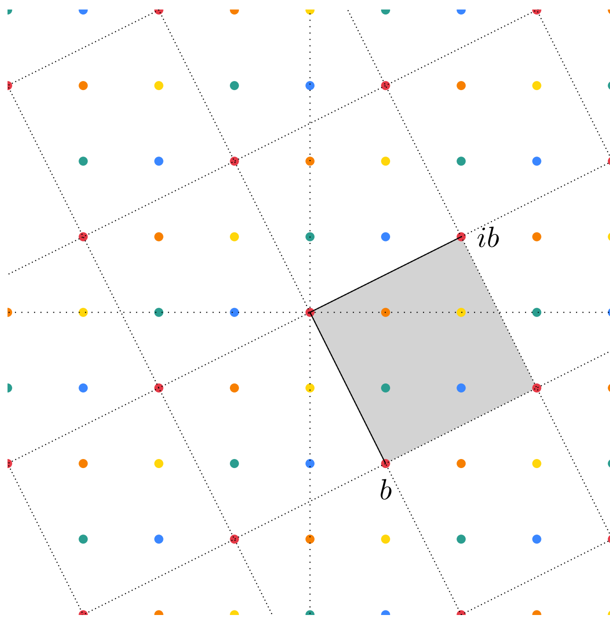

Figure 3

When visualizing the quotient ring $\mathbb{Z}[i]/(1-2i)$, we identify points in Figure 3 with the same relative position. For example, the red dots should be viewed as the same, and so should the orange and the other colors. This suggests that $\#(\mathbb{Z}[i]/(1-2i)) = 5$. (Exercise: Identify the addition and multiplication on $\mathbb{Z}[i]/(1-2i)$ through these dots.)

Example 2.2. More generally, we claim that the cardinality of $\mathbb{Z}[i]/(u+vi)$ is u^2+v^2 if $\gcd(u,v) = 1$. Put $z := u+vi \neq 0$. We may assume that neither u nor v is 0 because otherwise z will be a unit, in which case the result is trivial. By choosing a suitable generator, we may assume $u, v \in \mathbb{N}$. That is, z is in the first quadrant. (This amounts to taking $ib = 2+i$ as the generator instead of $b = 1-2i$ in Example 2.1; see Figure 3 also.)

One checks that the only points in $\mathbb{Z}[i]$ lying on the segment from 0 to $z = u+vi$ are the endpoints. Indeed, if there exist $m+ni \in \mathbb{Z}[i]$ with $0 < m < u$ such that $un = vm$, then since $\gcd(u, v) = 1$, we would have u divides m, which is absurd. Since $\mathbb{Z}[i]$ is closed under multiplication by i (i.e., rotating counterclockwise by 90 degrees), the same is also true for the segment from 0 to iz.

The above argument shows that there are four points in $\mathbb{Z}[i]$ which lie on the boundary of the retangle spanned by z and iz, and they are the same in $\mathbb{Z}[i]/(z)$. Take $A = u^2 + v^2$ to be its area, $B = 4$ to be the number of boundary points, and I to be the number of interior points. Then by Pick's theorem[1], we have

$$A = I + \frac{B}{2} - 1.$$

Hence,

$$\#(\mathbb{Z}[i]/(z)) = I + 1 = A = u^2 + v^2.$$

Remark 2.3. Let d be a square-free integer. The norm-Euclidean quadratic fields $\mathbb{Q}(\sqrt{d})$ (i.e., the field norm on $\mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$ induces a Euclidean function on its ring of integers) have been fully classified:[2]

$$d = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Thus, the readers are welcome to give similar geometric interpretations for others rings, such the ring of Eisenstein integers $\mathbb{Z}[\omega]$ where $\omega := (-1 + \sqrt{-3})/2$ as in Examples 1.4, 2.1, and 2.2.

References

[Fra03] John B. Fraleigh. *A First Course in Abstract Algebra*. 7th. Addison-Wesley, 2003.

[1]Given a polygon with integral coordinate vertices, let A be its area, B be the number of its integral boundary points, and I be the number of its integral interior points. Then we have

$$A = I + \frac{B}{2} - 1.$$

[2]The On-Line Encyclopedia of Integer Sequences (OEIS): squarefree values of n for which the quadratic field $\mathbb{Q}(\sqrt{n})$ is norm-Euclidean