Problem Set 2 – Gaussian integers and primes

1 Gaussian integers

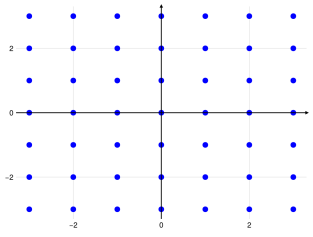


Figure 1: Some Gaussian integers

Definition 1.1. The Gaussian integers are the set $\mathbb{Z}[i] = \{x + iy : x, y \in \mathbb{Z}\}$ of complex numbers whose real and imaginary parts are both integers.

If we endow this set with addition and multiplication inherited from the complex numbers, we obtain a ring which is an extension of the usual ring of integers $\mathbb{Z}$.

Ring theory provides a detailed classification of numerous ring types. Here is a small selection:

$$\begin{matrix}\text{(commutative)}\\ \text{rings}\end{matrix} \supset \begin{matrix}\text{integral}\\ \text{domains}\end{matrix} \supset \begin{matrix}\text{unique}\\ \text{factorization}\\ \text{domains}\end{matrix} \supset \text{fields} \tag{1}$$

The ring of Gaussian integers $\mathbb{Z}[i]$ is a UFD *(unique factorization domain)*, just as $\mathbb{Z}$. That means we have a concept of divisibility, prime elements and unique factorization into these primes. The rules of the game differ slightly from those of $\mathbb{Z}$. For instance, 7 and 11 are prime elements in $\mathbb{Z}[i]$; however, 5 and 13 are composite:

Your expository paper may discuss how the following definitions are related to the algebraic structures in (1).

$$5 = (2 + i)(2 - i)$$
$$13 = (3 + 2i)(3 - 2i)$$

We will use Greek letters $\alpha, \beta, \ldots, \pi, \ldots$ for Gaussian numbers and primes and $a, b, \ldots, p, \ldots$ for numbers and primes in $\mathbb{Z}$.

1.1 Divisibility

Definition 1.2 (divisibility). Let $\alpha, \beta \in \mathbb{Z}[i]$. We call α a divisor of β and write $\alpha \mid \beta$ if there exists some $\gamma \in \mathbb{Z}[i]$ such that $\beta = \gamma\alpha$.

Example 1.3. Remember that complex division uses the 'expand the fraction by the conjugate' trick:

(i) Since $\dfrac{11 + 3i}{1 + 3i} = \dfrac{(11 + 3i)(1 - 3i)}{(1 + 3i)(1 - 3i)} = \dfrac{20 - 30i}{10} = 2 - 3i$, we see that $1+3i \mid 11+3i$.

(ii) Since $\dfrac{5 + i}{1 + 3i} = \dfrac{(5 + i)(1 - 3i)}{10} = \dfrac{4}{5} - \dfrac{7}{5}i \notin \mathbb{Z}[i]$, we see that $1 + 3i \nmid 5 + i$.

The ring $\mathbb{Z}$ of integers has the two units ± 1.

Definition 1.4 (units). Units are the elements that are divisors of 1. In other words: μ is a unit if there exists some (not necessarily different) ν such that $\mu\nu = 1$.

The ring $\mathbb{Z}[i]$ has the four units $1, -1, i$ and $-i$.

We say that α and β are *associates* if there exists a unit μ such that $\alpha = \mu\beta$. Every non-zero number $\alpha \in \mathbb{Z}[i]$ has four associates: $\pm\alpha$ and $\pm i\alpha$.

Definition 1.5 (prime elements). A non-zero element $\pi \in \mathbb{Z}[i]$ is a prime if it is not a unit, and it cannot be written as a product of two non-units. That is, if $\pi = \alpha\beta$, then either α or β is a unit.

Every associate $-\pi, i\pi, -i\pi$ of a prime element π is also prime.

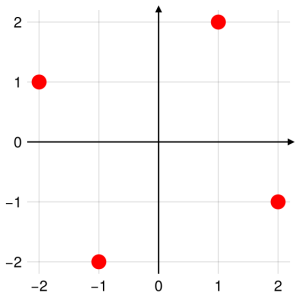


Figure 2: The associates of the prime $\pi = 1 + 2i$.

1.2 Prime factorization

The Gaussian integers are a unique factorization domain. This implies:

(i) Every Gaussian integer a is either zero, a unit, or it may be written as a product of Gaussian primes $\alpha = \pi_1\pi_2\cdots\pi_k$.

(ii) This prime factorization is essentially unique.

'Essentially unique' means (a) unique up to order and (b) unique up to multiplication of primes by units, i.e., up to the choice of associates.

Example 1.6. $5 = (1+2i)(1-2i) = [i(1+2i)]\ [-i(1-2i)] = (-2+i)(-2-i)$

All this happens already in $\mathbb{Z}$:
$15 = (-3)\times(-5) = 3\times 5$
$-15 = (-3)\times 5 = 3\times(-5)$
$= (-1)\times 3\times 5$
where the last form is the normalized one.

Normalized form. We can enforce uniqueness by choosing a representative among the associates. For example, we may always choose the associate belonging to the first quadrant of the complex plane (including the positive real axis and excluding the imaginary axis). This means $\pi = x + iy$ where $x > 0$ and $y \geq 0$. Then we can write the prime factorization as:

$$\alpha = \mu\pi_1\pi_2\cdots\pi_k \tag{2}$$

where μ is a unit and the factorization is unique up to the order of factors.

Example 1.7. $5 = -i(1+2i)(2+i)$

1.3 Gaussian primes

We seek a more explicit characterization of the Gaussian primes and their relationship to prime numbers in $\mathbb{Z}$. So we construct a useful map from one ring to the other: the norm of Gaussian integers.

This algebraic norm does not satisfy the axioms of a vector space norm for $\mathbb{C}$ or $\mathbb{R}^2$. Therefore, we do not use the notation $||\alpha||$.

Definition 1.8. The norm $N(\alpha)$ of a Gaussian integer $\alpha = x + iy$ is defined as:

$$N(\alpha) = x^2 + y^2 \tag{3}$$

Check the lemma!

Lemma 1.9. *The norm $N(\alpha)$ maps the ring $\mathbb{Z}[i]$ into the ring $\mathbb{Z}$, and it holds that:*

(i) The norm is multiplicative, $N(\alpha\beta) = N(\alpha)N(\beta)$ for all Gaussian integers α, β.

(ii) The norm maps zero (and only zero) in $\mathbb{Z}[i]$ to zero in $\mathbb{Z}$.

(iii) The norm maps units to units. More specifically, $N(\mu) = 1$ for all units μ.

(iv) The norm maps non-units to non-units.

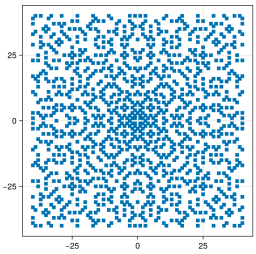


Figure 3: All Gaussian primes $\pi = x + iy$ with $|x| \leq 40$ and $|y| \leq 40$.

From this, we deduce immediately: *If $N(\alpha) = p$ is a prime number in $\mathbb{Z}$, then α is a Gaussian prime.* However, the converse does not hold since $N(\alpha)$ is neither surjective nor injective. Thus, this criterion alone does not capture all Gaussian primes. To proceed further, we need *Fermat's theorem on sums of two squares*. Using it, the following can be proved:

Theorem 1.10. *An element $\alpha = x + iy$ is a Gaussian prime if and only if either*

- *x and y are both non-zero and $N(\alpha)$ is a prime number in $\mathbb{Z}$; or*
- *one of x or y is zero and the absolute value $z = |x + y|$ of the other one is a prime number in $\mathbb{Z}$ and $z \equiv 3 \pmod 4$.*

1.4 *Gaussian prime factorization*

Finding the factorization of a Gaussian number α is possible in the usual recursive way:

(i) Your list of factors is empty.
(ii) If α is a unit, put it in front of your list, and you are finished.
(iii) If not, find a factor $\pi \mid \alpha$. Add it to your list of factors.
(iv) Set $\alpha \leftarrow \alpha/\pi$. Go to step (ii).

Finding a factor of α can be reduced to the problem of finding a factor of $N(\alpha)$:

(i) If $2 \mid N(\alpha)$, then $1+i \mid \alpha$. For prime factors $p > 2$:
(ii) If $p \mid N(\alpha)$ and $p \equiv 3 \pmod 4$, then $p + 0i \mid \alpha$.
(iii) If $p \mid N(\alpha)$ and $p \equiv 1 \pmod 4$, then p has a unique decomposition $p = x^2 + y^2$ as sum of two squares, and we have $x + iy \mid \alpha$ or $y + ix \mid \alpha$.

2 *The Gaussian prime walk*

Our doctor (or helpful partner) suggests daily exercises. So we will go for a walk on the $\mathbb{Z}[i]$ lattice. Here are the rules:

(i) Steps are possible in four directions: to the east (from α to $\alpha+1$), west ($\alpha \to \alpha-1$), north ($\alpha \to \alpha + i$) or south ($\alpha \to \alpha - i$).
(ii) The walk begins at some number α_0 and our initial step is always to the east.
(iii) We walk straight keeping our direction until we meet a Gaussian prime. At a prime, we make a 90° turn to the left.
(iv) Our daily exercise is completed if we come back to α_0 *and* the next step would again be eastward.

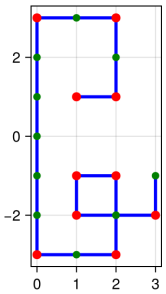
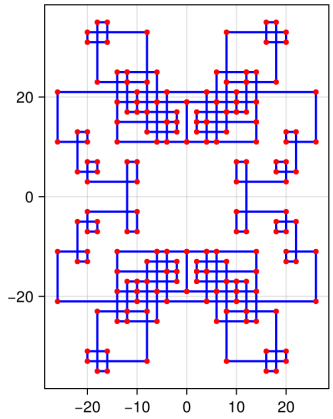


Figure 4: A walk of 20 steps starting at $\alpha_0 = 1 + i$. Primes in red.

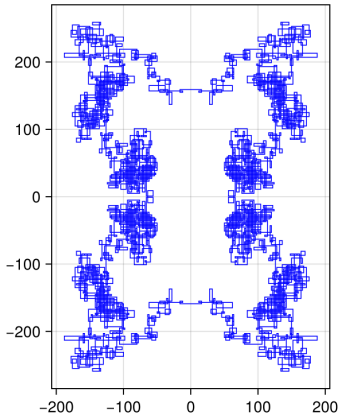
We try a different starting point every day and make some observations:

- It seems that we can always complete the walk, we never escape to infinity.[1]
- The length of the walk varies immensely. Often the walk has some bizarre almost symmetric form.

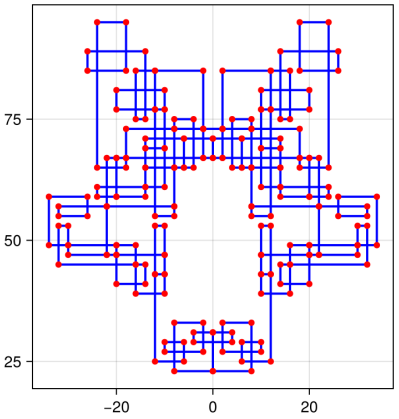
[1] *No proof or counterexample for this statement is known.*



(a) $\alpha_0 = 13 + 3i$, length=1316



(b) $\alpha_0 = 60 + i$, length=39212



(c) $\alpha_0 = 5 + 23i$, length=1536

Figure 5: Some Gaussian prime walks

3 Coding tasks

(i) Use only the `Primes.jl` package and some plotting package for the coding tasks.

(ii) You may define your own data type for Gaussian integers; or use something like:

```
const Gauss = Complex{Int64}
N(α::Gauss) = α.re^2 + α.im^2
```

(iii) Write a function to check if a Gaussian integer is a Gaussian prime. You may use the `isprime(n)` function of the `Primes.jl` module for primality tests in $\mathbb{Z}$.

(iv) Write a function that generates all Gaussian primes $a = x + iy$ in the region $|x| \leq n$ and $|y| \leq n$. Use this function to generate plots similar to Fig. 3.

(v) Write a function that generates a Gaussian prime walk. It should return the path as a list of Gaussian integers.

(vi) Write a function that uses the above function to generate plots similar to Fig. 5.

(vii) Write a function that factorizes Gaussian integers, with output similar to the output of:

```
using Primes
factors(n::Integer) = factor(Vector, n)
factors(-90)
```

(viii) *Bonus:* Study the dependency of the length of the prime walks on the start point.