18 Gaussian Integers

Definition: $\mathbb{Z}[i] \subseteq \mathbb{C} = \{a + ib : \ a, b \in \mathbb{Z}\}$

Elements of $\mathbb{Z}[i]$ are called Gaussian integers, which can be added, subtracted and multiplied. But we cannot divide in $\mathbb{Z}[i]$. For example, $\frac{1}{1+i} = \frac{1}{2}(1-i) \notin \mathbb{Z}[i]$. Note: if $\alpha\beta = 0 \Rightarrow \alpha = 0$ or $\beta = 0$. Define the norm

$$N : \mathbb{Z}[i] \to \mathbb{Z}_+$$

by

$$\alpha = a + bi \mapsto a^2 + bi = (a + bi)(c - bi) = \alpha\bar{\alpha}$$

The complex conjugation map $\alpha \mapsto \bar{\alpha}$ satisfies:

$$\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}, \ \overline{\alpha\beta} = \bar{\alpha} \cdot \bar{\beta}.$$

So

$$N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = N(\alpha)N(\beta)$$

Notice that in $\mathbb{C}$, $\alpha^{-1} = \frac{\bar{\alpha}}{N(\alpha)}$

Definition: α, β in $\mathbb{Z}[i]$. Say $\alpha|\beta$ **iff** $\beta = \alpha \cdot \gamma$, some $\gamma \in \mathbb{Z}[i]$.

Definition: A **unit** in $\mathbb{Z}[i]$ is an element α in $\mathbb{Z}[i]$ such that $\alpha\beta = 1$ for some $\beta \in \mathbb{Z}[i]$. If α is a unit in $\mathbb{Z}[i]$, say $\alpha\beta = 1$,

$$N(\alpha\beta) = N(1) = 1 = N(\alpha)N(\beta).$$

If $\alpha = a + bi, \ a, b \in \mathbb{Z}$,

$$(a^2 + b^2) = N(\beta) = 1$$

Hence

$$a = 0, \ b = \pm 1, \ \text{or } a = \pm 1, \ b = 0.$$

This means $\alpha = \pm 1$ or $\pm i$. Put

$$D = \{a + bi : a \geq 1, \ b \geq 0\}$$

$\alpha \sim \beta$ ("associated") **iff** $\alpha = u\beta$ for some unit u in $\mathbb{Z}[i]$.

If $\alpha \neq 0$, there is exactly one associate of α in D, the normalized associate.

$\pi \in \mathbb{Z}[i]$ is called a **Gaussian prime** if its only divisors are units and its associates.

Question: What are the Gaussian primes?

$(1+i)(1-i) = 2$ so $(1 \pm i)|2$. Hence 2 is **not** a Gaussian prime. $1+i$, $2+i$ are Gaussian primes, so is $1+2i$ because it is an associate of $2+i$. (*Conjecture*: $a+ib$ is Gaussian prime iff $(a,b)=1$.)

Unsolved Problem: If you are allowed only steps of bounded size, is it possible to walk to ∞ stepping only on Gaussian primes?

Euclidean algorithm: Recall the norm function

$$\begin{aligned} N : \mathbb{Z}[i] &\to \mathbb{Z} \\ a+bi &\mapsto a^2+b^2 \\ \alpha &\mapsto \alpha\bar{\alpha}, \end{aligned}$$

which is multiplicative, i.e.,

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

Given $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$, $\exists$ [unique] $\rho, \kappa \in \mathbb{Z}[i]$ such that $\alpha = \kappa\beta + \rho$ **and** $0 \neq N(\rho) \leq \frac{N(\beta)}{2}$.

Proof: $\forall x \in \mathbb{R}$, let round(x) = closest integer to x. Then $|x - \text{round}(x)| \leq \frac{1}{2}$. Choose round$(\frac{1}{2}) = 1$ and let round$(x+iy)$ = round(x)+$i$round(y).

Let $z = \frac{\alpha}{\beta} = \mathbb{C}$.

Let $\kappa = \text{round}(z)$.

$$\begin{aligned} N(z-\kappa) &= N(z - \text{round}(z)). \\ &= N((x - \text{round}(x)) + i(y - \text{round}(y))) \\ &= (x - \text{round}(x))^2 + (y - \text{round}(y))^2 \leq \frac{1}{2} \end{aligned}$$

$$\text{Since } \frac{\alpha}{\beta} = \kappa + \left(\frac{\alpha}{\beta} - \kappa\right),$$

$$\alpha = \beta\kappa + \rho,$$

$$\text{with } \rho = (\alpha - \beta\kappa),\ 0 \leq N(\rho).$$

$$\text{Then } z - \kappa = \frac{\alpha}{\beta} - \kappa = \frac{\alpha - \kappa\beta}{\beta},\ \text{and}$$

$$N(z-\kappa) = \frac{N(\alpha - \kappa\beta)}{N(\beta)} = \frac{N(\rho)}{N(\beta)} \leq \frac{1}{2}.$$

Corollary: The ring $\mathbb{Z}[i]$ has unique factorization into Gaussian primes.

Proof: Similar to the proof in $\mathbb{Z}$, with $\gcd(\alpha, \beta)$ being defined using the Euclidean algorithm.

Now investigate what Gaussian primes look like.

$$N(3+i) = \underbrace{9+1}_{\text{[sum of squares]}} = 10 = 2 \cdot 5$$

[Notice relatioship to sums of squares!] So 3+i must be divisible by something of norm 2 and something of norm 5. $2+i$, $2-i$ has norm 5, while $1+i$ has norm 2.

$$(2+i)(1+i) = 2+3i-1 = 1+3i$$

$$(2-i)(1+i) = i+3$$

Theorem: Let p be a prime of $\mathbb{Z}$. If p is not a Gaussian prime then $p = \pi\overline{\pi}$, π, $\overline{\pi}$ Gaussian primes. ($\pi \not\sim \overline{\pi}$ if p is odd). Also, p has no other divisors. Moreover, p is not a Gaussian prime iff

$$p = 2 = (1+i)^2$$

or

$$p \equiv 1 \pmod 4.$$

Consequently if $p \equiv 3 \pmod 4$, p is a Gaussian prime.

Conversely, every Gaussian prime π is either a rational prime $\equiv 3$ (mod 4) or its norm is a rational prime $\not\equiv 3 \pmod 4$. In the latter case, $N(\pi) = 2$ iff $\pi \sim \overline{\pi}$.

Proof: By unique factorization, we may write $p = w\pi_1 \ldots \pi_m$, with w a unit, and the π_j's Gaussian primes.

$$N(p) = p\bar{p} = p^2 = \prod_{j=1}^{m} N(\pi_j).$$

Thus $\exists$ unique j such that $N(\pi_j) = p^2$. Then $m = 1$ and $p = w\pi_1$. Consequently, p is a Gaussian prime. So if $p \neq$ Gaussian prime, then none of the $N(\pi_j)$'s are p^2. So

$$p = \pi_1\pi_2$$

with π_1, π_2 Gaussian primes, $N(\pi_i) = p$. Since $\pi_1, \pi_2 \notin \mathbb{Z}$, and $\pi_1\pi_2 \in \mathbb{Z}$, $\pi_2 = \overline{\pi_1}$.

Assume p is odd. Then $\pi \sim \bar{\pi}$ means $\pi = a + bi \sim a - bi$. The associates of π are $\pm(a+ib)$ and $\pm(a+ib)$. This is because the units in $\mathbb{Z}[i]$ are ± 1, $\pm i$. Then $a - ib = \gamma(a + ib)$, where $\gamma \in \{1 - 1, i, -i\}$. If $\gamma = 1$, $p = a^2$, if $\gamma = -1$, $p = b^2$; and if $\gamma = \pm i$, $p = 2a^2$. None of these is a possibility as p is an odd prime. Thus π, $\bar{\pi}$ are not associates, and$p = \pi\bar{\pi}$, with π Gaussian prime of norm p. When $p = 2$, we have $2 = N(1 + i) = (1 + i)(1 - i)$, and $1 - i = -i(1 + i)$.

We have yet to show that an odd rational prime p is **not** a Gaussian prime precisely when $p \equiv 1 \pmod 4$. But we have just shown that p must be of the form $N(\pi)$ for a Gaussian prime π when p is not itself a Gaussian prime. Then $\exists x, y \in \mathbb{Z}$ such that

$$p = x^2 + y^2.$$

As we have seen in the previous section, this implies, as derived, that $p \equiv 1 \pmod 4$. But we can also check this directly. Modulo 4, the square of any integer must be 0 or 1. Then $p = x^2 + y^2$ must be 0 or 1 mod 4. Since p is odd, it must be 1 mod 4.

Now let π be any Gaussian prime, which is not in $\mathbb{Q}$. We have to show that $N(\pi) = p$ with $p \equiv 1 \pmod 4$ or $p = 2$. Since $N(\pi)$ is an integer ≥ 1, and since $N(\pi)$ cannot be 1 as π is not a unit, there must be some (rational) prime q dividing $N(\pi)$. Write $N(\pi) = q_1q_2 \ldots q_r$, with each q_j a rational prime. Now since $N(\pi) = \pi\bar{\pi}$, and since π is a Gaussian prime, viewing $\pi\bar{\pi} = q_1q_2 \ldots q_r$ as an equation in $\mathbb{Z}[i]$, we see that π must divide some q_j, call it p. By what we proved above, p must be the norm of some Gaussian prime π_1. Then π divides $p = \pi_1\overline{\pi_1}$. So π must divide π_1 or $\overline{\pi_1}$, say it divides π_1. Then $\pi \sim \pi_1$, and we will have $p = u\pi\bar{\pi}$, for some unit u. But both p and $\pi\bar{\pi}$ are real and positive, so u must be 1. The rest is clear.