VE477

Introduction to Algorithms

Discussion

Manuel — UM-JI (Fall 2021)

Gaussian integers

- Practice exercises with chained questions
- Think further to design algorithms
- Work with mathematics

Gaussian integers appears in various setup such as cryptography of coding theory.

Ex. 1 — *Gaussian integers*

The subset of $\mathbb{C}$ consisting of the complex numbers $a + ib$, with a and b in $\mathbb{Z}$, is called the set of the *Gaussian integers*, and is denoted $\mathbb{Z}[i]$.

1. We define the norm of $\alpha \in \mathbb{Z}[i]$ is defined as $N(\alpha) = \alpha\bar{\alpha}$, where $\bar{\alpha}$ is the complex conjugate of a.
   a) Calculate the norm of $N(7 + 2i)$.
   b) Prove that for any $\alpha, \beta \in \mathbb{Z}[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$.
   c) Show that the only invertible elements of $\mathbb{Z}[i]$ are ± 1 and $\pm i$.
   d) Show that the norm of any Gaussian integer is an integer but that not every integer is the norm of a Gaussian integer.
2. We want to determine all the prime elements of $\mathbb{Z}[i]$.
   a) For $\alpha \in \mathbb{Z}[i]$, prove that if $N(\alpha)$ is prime in $\mathbb{Z}$, then α is prime in $\mathbb{Z}[i]$.
   b) Prove that a prime in $\mathbb{Z}$ is composite in $\mathbb{Z}[i]$, if and only if it can be written as a sum of two squares.
   c) Is the converse of 1. true? Explain.

For any $\alpha, \beta \in \mathbb{Z}[i]$, with $\beta \neq 0$, we say that β divides α if there exists $\gamma \in \mathbb{Z}[i]$ such that $\alpha = \beta\gamma$.

3. Divisibility of elements.
   a) Show that if β divides α in $\mathbb{Z}[i]$, then $N(\beta)$ divides $N(\alpha)$ in $\mathbb{Z}$.
   b) For $\alpha \in \mathbb{Z}[i]$, show that $N(\alpha)$ is even if and only if it is a multiple of $1 + i$.
   c) Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$.
   d) Prove the existence of q_1, q_2, r_1, r_2 such that $q_1, q_2 \in \mathbb{Z}$, $0 \leq |r_1|, |r_2| \leq \frac{1}{2}N(\beta)$, and

   $$\frac{\alpha}{\beta} = q_1 + q_2 i + \frac{r_1 + r_2 i}{N(\beta)}.$$

      i – Setting $\gamma = q_1 + q_2 i$, prove that $N(\alpha - \beta\gamma) \leq \frac{1}{2}N(\beta)$.
      ii – Conclude on the existence of $\gamma, \rho \in \mathbb{Z}[i]$, with $N(\rho) < N(\beta)$ and such that $\alpha = \beta\gamma + \rho$.
   e) Derive an algorithm taking as input $\alpha, \beta \in \mathbb{Z}[i]$ and returning $\gcd(\alpha, \beta)$.
   f) What is the complexity of this algorithm?
4. Applications.
   a) Compute $\gcd(32 + 9i, 4 + 11i)$.
   b) Show that $4 + 5i$ and $4 - 5i$ are coprime in $\mathbb{Z}[i]$.