Chapter 1: A Special Case of Fermat's Conjecture

Author: Meng-Gen Tsai
Email: plover@gmail.com

Exercise 1.1-1.9: Define $N : \mathbb{Z}[i] \to \mathbb{Z}$ by $N(a+bi) = a^2 + b^2$.

Exercise 1.1 *Verify that for all $\alpha, \beta \in \mathbb{Z}[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$, either by direct computation or using the fact that $N(a+bi) = (a+bi)(a-bi)$. Conclude that if $\alpha \mid \gamma$ in $\mathbb{Z}[i]$, then $N(\alpha) \mid N(\gamma)$ in $\mathbb{Z}$.*

Proof.

(1) *Direct computation.* Write $\alpha = a+bi, \beta = c+di$ where $a, b, c, d \in \mathbb{Z}$. Thus,

$$\begin{aligned} N(\alpha\beta) &= N((a+bi)(c+di)) \\ &= N((ac-bd)+(ad+bc)i) \\ &= (ac-bd)^2 + (ad+bc)^2 \\ &= (a^2c^2 - 2abcd + b^2d^2) + (a^2d^2 + 2abcd + b^2c^2) \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2, \\ N(\alpha)N(\beta) &= N(a+bi)N(c+di) \\ &= (a^2+b^2)(c^2+d^2) \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2. \end{aligned}$$

Therefore, $N(\alpha\beta) = N(\alpha)N(\beta)$. (Note that we also get the identity $(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$.)

(2) *Using the fact that $N(a+bi) = (a+bi)(a-bi)$,* or $N(\alpha) = \alpha\overline{\alpha}$ for any $\alpha \in \mathbb{Z}[i]$. Thus,

$$\begin{aligned} N(\alpha\beta) &= \alpha\beta\overline{\alpha\beta} \\ &= \alpha\beta\overline{\alpha}\,\overline{\beta} \\ &= \alpha\overline{\alpha}\beta\overline{\beta} \\ &= N(\alpha)N(\beta). \end{aligned}$$

(3) *Show that if $\alpha \mid \gamma$ in $\mathbb{Z}[i]$, then $N(\alpha) \mid N(\gamma)$ in $\mathbb{Z}$.* Write $\gamma = \alpha\beta$ for some $\beta \in \mathbb{Z}[i]$. So $N(\gamma) = N(\alpha)N(\beta) \in \mathbb{Z}$, or $N(\alpha) \mid N(\gamma)$ in $\mathbb{Z}$.

□

Exercise 1.2 *Let $\alpha \in \mathbb{Z}[i]$. Show that α is a unit iff $N(\alpha) = 1$. Conclude that the only unit are ± 1 and $\pm i$.*

Proof.

(1) ($\Longrightarrow$) Since α is a unit, there is $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta = 1$. By Exercise 1.1, $N(\alpha\beta) = N(1)$, or $N(\alpha)N(\beta) = 1$. Since the image of N is nonnegative integers, $N(\alpha) = 1$.

(2) ($\Longleftarrow$) By Exercise 1.1, $N(\alpha) = \alpha\overline{\alpha}$, or $1 = \alpha\overline{\alpha}$ since $N(\alpha) = 1$. That is, $\overline{\alpha} \in \mathbb{Z}[i]$ is the inverse of $\alpha \in \mathbb{Z}[i]$. (Or by (1), we solve the equation $N(\alpha) = a^2 + b^2 = 1$, and show that all four solutions (± 1 and $\pm i$) are unit.)

Conclusion: a unit $\alpha = a+bi$ of $\mathbb{Z}[i]$ is satisfying the equation $N(\alpha) = a^2+b^2 = 1$ by (1)(2). That is, the only unit of $\mathbb{Z}[i]$ are ± 1 and $\pm i$. □

Exercise 1.3 *Let $\alpha \in \mathbb{Z}[i]$. Show that if $N(\alpha)$ is a prime in $\mathbb{Z}$ then α is irreducible in $\mathbb{Z}[i]$. Show that the same conclusion holds if $N(\alpha) = p^2$, where p is a prime in $\mathbb{Z}$, $p \equiv 3 \pmod 4$.*

Proof.

(1) *Show that if $N(\alpha)$ is a prime in $\mathbb{Z}$ then α is irreducible in $\mathbb{Z}[i]$.* Write $\alpha = \beta\gamma$. Then $N(\alpha) = N(\beta)N(\gamma)$ is a prime in $\mathbb{Z}$. Since each integer prime is irreducible, $N(\beta) = 1$ or $N(\gamma) = 1$. So that β is unit or γ is unit by Exercise 1.2. Hence, α is irreducible.

(2) *Show that α is irreducible in $\mathbb{Z}[i]$ if $N(\alpha) = p^2$, where p is a prime in $\mathbb{Z}$, $p \equiv 3 \pmod 4$.* Assume $\alpha = \beta\gamma$ were not irreducible. Similar to (1), $N(\alpha) = N(\beta)N(\gamma) = p^2$. Since β and γ are proper factors of α,

$$N(\beta) = N(\gamma) = p.$$

Since any square $a^2 \equiv 0, 1 \pmod 4$, any $N(a + bi) = a^2 + b^2 \equiv 0, 1, 2 \pmod 4$. Especially, $N(\beta) \equiv 0, 1, 2 \pmod 4$, contrary to $N(\beta) = p \equiv 3 \pmod 4$ by the assumption. Therefore, α is irreducible in $\mathbb{Z}[i]$.

□

Supplement.

(1) The prime 2 is reducible in $\mathbb{Z}[i]$ (Exercise 1.4).

(2) Every prime $p \equiv 1 \pmod 4$ is reducible in $\mathbb{Z}[i]$ (Exercise 1.8).

Exercise 1.4 *Show that $1-i$ is irreducible in $\mathbb{Z}$ and that $2 = u(1-i)^2$ for some unit u.*

Proof.

(1) *$1-i$ is irreducible.* Since $N(1-i) = 2$ is a prime in $\mathbb{Z}$, $1-i$ is irreducible by Problem 1.3.

(2) $2 = i(1-i)^2$ where i is unit in $\mathbb{Z}$.

□

Exercise 1.5 *Notice that $(2+i)(2-i) = 5 = (1+2i)(1-2i)$. How is this consistent with unique factorization?*

Proof. Since $2+i = i(1-2i)$ and $2-i = (-i)(1+2i)$, the factorization is unique up to order and multiplication of primes by units. □

Exercise 1.6 *Show that every nonzero, non-unit Gaussian integer α is a product of irreducible elements, by induction on $N(\alpha)$.*

Proof. Induction on $N(\alpha)$.

(1) $n = 2$. Given $\alpha \in \mathbb{Z}[i]$ with $N(\alpha) = 2$. Since $N(\alpha) = 2$ is a prime in $\mathbb{Z}$, α is irreducible (Exercise 1.3).

(2) *Suppose the result holds for $n \leq k$.* Given $\alpha \in \mathbb{Z}[i]$ with $N(\alpha) = k+1$. There are only two possible cases.

   (a) *α is irreducible.* Nothing to do.

   (b) *α is reducible.* Write $\alpha = \beta\gamma$ where neither factor is unit. Since $N(\alpha) = N(\beta)N(\gamma)$ and neither factor is unit,

$$2 \leq N(\beta), N(\gamma) \leq k.$$

   By the induction hypothesis, each factor of α (β and γ) is a product of irreducible elements. So that α again is a product of irreducible elements.

   In any cases, α is a product of irreducible elements.

By induction, the result is established. □

Exercise 1.7 *Show that $\mathbb{Z}[i]$ is a principal ideal domain (PID); i.e., every ideal I is principal. (As shown in Appendix 1, this implies that $\mathbb{Z}[i]$ is a UFD.)*

Suggestion: Take $\alpha \in I - \{0\}$ such that $N(\alpha)$ is minimized, and consider the multiplies $\gamma\alpha$, $\gamma \in \mathbb{Z}[i]$; show that these are the vertices of an infinite family of squares which fill up the complex plane. (For example, one of the squares has vertices 0, α, $i\alpha$, and $(1+i)\alpha$; all others are translates of this one.) Obviously I contains all $\gamma\alpha$; show by a geometric argument that if I contains anything else then minimality of $N(\alpha)$ would be contradicted.

Proof (without geometric intuition). Define N on $\mathbb{Q}[i]$ by $N(a+bi) = a^2 + b^2$ where $a + bi \in \mathbb{Q}[i]$ as usual.

(1) *Show that $\mathbb{Z}[i]$ is a Euclidean domain.* Given $\alpha = a + bi \in \mathbb{Z}[i]$ and $\gamma = c + di \in \mathbb{Z}[i]$ with $\gamma \neq 0$. It suffices to show there exist δ and ρ such that the identity $\alpha = \gamma\delta + \rho$ holds and either $\rho = 0$ or $N(\rho) < N(\gamma)$.

(a) *Pick $\delta \in \mathbb{Z}[i]$. (Intuition: Pick the 'integer part' of $\frac{\alpha}{\gamma}$ as we did in integer numbers.)* Write $\frac{\alpha}{\gamma} = r + si \in \mathbb{Q}[i]$. Then we pick $\delta = m + ni \in \mathbb{Z}[i]$ such that $|r - m| \leq \frac{1}{2}$ and $|s - n| \leq \frac{1}{2}$. Therefore,

$$\begin{aligned} N\left(\frac{\alpha}{\gamma} - \delta\right) &= (r-m)^2 + (s-n)^2 \\ &\leq \frac{1}{4} + \frac{1}{4} \\ &= \frac{1}{2}. \end{aligned}$$

(b) *Pick $\rho \in \mathbb{Z}[i]$.* Clearly we can pick $\rho = \alpha - \gamma\delta \in \mathbb{Z}[i]$. Therefore, $\rho = 0$ or

$$\begin{aligned} N(\rho) &= N(\alpha - \gamma\delta) \\ &= N\left(\gamma\left(\frac{\alpha}{\gamma} - \delta\right)\right) \\ &= N(\gamma)N\left(\frac{\alpha}{\gamma} - \delta\right) \\ &\leq \frac{1}{2}N(\gamma) \\ &< N(\gamma). \end{aligned}$$

(2) *Show that every Euclidean domain R is a PID.* Given any ideal I of R. Take $\alpha \in I - \{0\}$ such that $N(\alpha)$ is minimized.

(a) $R\alpha \subseteq I$ clearly.

(b) Conversely, for any $\beta \in I$, there are $\delta, \rho \in R$ such that $\beta = \alpha\delta + \rho$, where either $\rho = 0$ or $N(\rho) < N(\alpha)$. Since $\rho = \beta - \alpha\delta \in I$, we cannot have $N(\rho) < N(\alpha)$ by the minimality of $N(\alpha)$. Therefore, $\rho = 0$ and $\beta = \alpha\delta \in R\alpha$, or $R\alpha \supseteq I$.

By (1)(2), $\mathbb{Z}[i]$ is a PID. $\square$

Exercise 1.9 *Describe all irreducible elements in* $\mathbb{Z}[i]$.