

Chapter 1: A Special Case of Fermat's Conjecture

Author: Meng-Gen Tsai

Email: plover@gmail.com

Exercise 1.1-1.9: Define $N : \mathbb{Z}[i] \rightarrow \mathbb{Z}$ 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 $N(\alpha) = \alpha\bar{\alpha}$ for any $\alpha \in \mathbb{Z}[i]$.* Thus,

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

(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) (\implies) 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) (\impliedby) By Exercise 1.1, $N(\alpha) = \alpha\bar{\alpha}$, or $1 = \alpha\bar{\alpha}$ since $N(\alpha) = 1$. That is, $\bar{\alpha} \in \mathbb{Z}[i]$ 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 $\pm i$. \square

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 $\mathbb{Z}[i]$.

\square

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 1.8. We will use the unique factorization in $\mathbb{Z}[i]$ to prove that every prime $p \equiv 1 \pmod{4}$ is a sum of two squares.

- (a) Use the fact that the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of integers mod p is cyclic to show that if $p \equiv 1 \pmod{4}$ then $n^2 \equiv -1 \pmod{p}$ for some $n \in \mathbb{Z}$.
- (b) Prove that p cannot be irreducible in $\mathbb{Z}[i]$. (Hint: $p \mid n^2 + 1 = (n+i)(n-i)$.)
- (c) Prove that p is a sum of two squares. (Hint: (b) shows that $p = (a + bi)(c + di)$ with neither factor a unit. Take norms.)

Proof of (a). Since the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of integers mod p is cyclic, $(\mathbb{Z}/p\mathbb{Z})^\times$ is generated by (a primitive root) $g \in \mathbb{Z}/p\mathbb{Z}$. $g^{p-1} = 1$, or

$$(g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1) = 0$$

since p is odd. Since $\mathbb{Z}/p\mathbb{Z}$ is an integral domain, $g^{\frac{p-1}{2}} - 1 = 0$ or $g^{\frac{p-1}{2}} + 1 = 0$. g cannot satisfy $g^{\frac{p-1}{2}} - 1 = 0$ since g is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. So,

$$g^{\frac{p-1}{2}} + 1 = 0.$$

Let $n = g^{\frac{p-1}{4}} \in \mathbb{Z}$ since $p \equiv 1 \pmod{4}$. So $n^2 + 1 = 0 \pmod{p}$. \square

Proof of (b). Since $n^2 + 1 \equiv 0 \pmod{p}$ by (a), $p \mid n^2 + 1 = (n+i)(n-i)$. If p were irreducible in $\mathbb{Z}[i]$, $p \mid (n+i)$ or $p \mid (n-i)$ by using the unique factorization in $\mathbb{Z}[i]$. Hence

$$\frac{n+i}{p} = \frac{n}{p} + \frac{1}{p}i \notin \mathbb{Z}[i], \frac{n-i}{p} = \frac{n}{p} - \frac{1}{p}i \notin \mathbb{Z}[i],$$

contrary to the assumption. Therefore, p is reducible in $\mathbb{Z}[i]$. \square

Proof of (c). Since p is reducible in $\mathbb{Z}[i]$ by (b), write $p = (a + bi)(c + di)$ with neither factor a unit. Take norms,

$$p^2 = N(p) = N(a + bi)N(c + di).$$

Since neither factor of p is unit, $N(a + bi) = p$, or $a^2 + b^2 = p$, or p is a sum of two squares. \square

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

Notice that α is irreducible if and only if $\bar{\alpha}$ is irreducible. (Write $\alpha = \beta\gamma$, then $\bar{\alpha} = \bar{\beta}\bar{\gamma}$. Besides, $\bar{\bar{\alpha}} = \alpha$.)

Proof. Show that all irreducible elements in $\mathbb{Z}[i]$ (up to units) are

- (1) $1 + i$.
- (2) $\pi = a + bi$ for each integer prime $p \equiv 1 \pmod{4}$ with $p = a^2 + b^2$.
- (3) p for each integer prime $p \equiv 3 \pmod{4}$.

Let α be any irreducible element in $\mathbb{Z}[i]$. Consider $N(\alpha) = \alpha\bar{\alpha}$. $N(\alpha) \neq 1$ since α is not unit. By the unique factorization theorem in \mathbb{Z} , $N(\alpha) \in \mathbb{Z}$ is a product of primes in \mathbb{Z} .

There are three possible cases.

- (a) $2 \mid N(\alpha)$. Write $(1+i)(1-i) \mid \alpha\bar{\alpha}$ in $\mathbb{Z}[i]$. Notice that $1+i$, $1-i$, α and $\bar{\alpha}$ are all irreducible (Exercise 1.4). By the unique factorization theorem in $\mathbb{Z}[i]$, $\alpha = 1+i$ (up to units).
- (b) $p \mid N(\alpha)$ for some prime $p \equiv 3 \pmod{4}$. Write $p \mid \alpha\bar{\alpha}$ in $\mathbb{Z}[i]$. Notice that p , α and $\bar{\alpha}$ are all irreducible (Exercise 1.3). By the unique factorization theorem in $\mathbb{Z}[i]$, $\alpha = p$ (up to units) or $\bar{\alpha} = p$ (up to units). So in any cases $\alpha = p$ (up to units). (Note that $\bar{p} = p$.)
- (c) $p \mid N(\alpha)$ for some prime $p \equiv 1 \pmod{4}$. For such p , there is an irreducible $\pi \in \mathbb{Z}[i]$ satisfying $p = \pi\bar{\pi}$ (Exercise 1.8). Now we write $\pi\bar{\pi} \mid \alpha\bar{\alpha}$ in $\mathbb{Z}[i]$. Notice that π , $\bar{\pi}$, α and $\bar{\alpha}$ are all irreducible. By the unique factorization theorem in $\mathbb{Z}[i]$, $\alpha = \pi$ or $\alpha = \bar{\pi}$. In any cases, $\alpha = a + bi$ for integer prime $p \equiv 1 \pmod{4}$ with $p = a^2 + b^2$.

□

Exercise 1.16-1.28: Let p be an odd prime, $\omega = e^{\frac{2\pi i}{p}}$.

Exercise 1.16. Show that

$$(1 - \omega)(1 - \omega^2) \cdots (1 - \omega^{p-1}) = p$$

by considering equation (2).

Equation (2). $t^p - 1 = (t - 1)(t - \omega)(t - \omega^2) \cdots (t - \omega^{p-1})$.

Proof. Note that $t^p - 1 = (t - 1)(t^{p-1} + t^{p-2} + \cdots + t + 1)$. Cancel out $t - 1$ of Equation (2),

$$t^{p-1} + t^{p-2} + \cdots + t + 1 = (t - \omega)(t - \omega^2) \cdots (t - \omega^{p-1}).$$

Put $t = 1$ to get $p = (1 - \omega)(1 - \omega^2) \cdots (1 - \omega^{p-1})$. \square

Exercise 1.30-1.32: R is an integral domain (commutative ring with 1 and no zero divisors).

Exercise 1.30. Show that two ideals in R are isomorphic as R -modules iff they are in the same ideal class.