Chapter 1: Unique Factorization

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

Exercise 1.10. *Suppose that* $(u, v) = 1$*. Show that* $(u+v, u-v)$ *is either* 1 *or* 2*.*

Each case is possible:

(1) $u = 3, v = 2$. $(u, v) = 1$ and $(u + v, u - v) = 1$.

(2) $u = 3, v = 1$. $(u, v) = 1$ and $(u + v, u - v) = 2$.

Proof (Exercise 1.6). Since $(u, v) = 1$, there is $m, n \in \mathbb{Z}$ such that $mu + nv = 1$ (Exercise 1.4). So

$$\begin{aligned} mu + nv = 1 &\Longleftrightarrow 2mu + 2nv = 2 \\ &\Longleftrightarrow ((u + v) + (u - v))m + ((u + v) - (u - v))n = 2 \\ &\Longleftrightarrow (m + n)(u + v) + (m - n)(u - v) = 2, \end{aligned}$$

or $(x, y) = (m + n, m - n)$ is an integer solution to $(u + v)x + (u - v)y = 2$. So $2 \mid (u + v, u - v)$ (Exercise 1.6). Hence $(u + v, u - v) = 1$ or 2. □

Exercise 1.11. *Show that* $(a, a + k) \mid k$*.*

Proof (Exercise 1.6). The equation $ax + (a + k)y = k$ has solution $(x, y) = (-1, 1) \in \mathbb{Z}^2$. Hence $(a, a + k) \mid k$ (Exercise 1.6). □

Exercise 1.31. *Show that* 2 *is divided by* $(1 + i)^2 \in \mathbb{Z}[i]$*.*

$1 + i$ is irreducible in $\mathbb{Z}[i]$.

The ring morphism $\mathbb{Z} \to \mathbb{Z}[i]$ corresponds to a map of schemes $f : \mathrm{Spec}(\mathbb{Z}[i]) \to \mathrm{Spec}(\mathbb{Z})$. Suppose (p) is a prime ideal of $\mathbb{Z}$. Might find the points of $f^{-1}(p) \in \mathrm{Spec}(\mathbb{Z}[i])$.

Proof. $(1 + i)^2 = 2i \in \mathbb{Z}[i]$. Thus $2 \mid (1 + i)^2 \in \mathbb{Z}[i]$. □

Exercise 1.34. *Show that* 3 *is divided by* $(1 - \omega)^2 \in \mathbb{Z}[\omega]$*.*

Proof. $(1-\omega)^2 = 1 - 2\omega + \omega^2 = (1 + \omega + \omega^2) - 3\omega = -3\omega \in \mathbb{Z}[\omega]$. Thus $3 \mid (1-\omega)^2 \in \mathbb{Z}[\omega]$. $\square$