Solutions to Exercise Sheet 1

We provide at least one solution to each problem. Other approaches are also possible for some problems.

Solution 1.1. *Review of highest common factors.*

(1) Using Euclidean algorithm, we have

$$\begin{aligned}
963 &= 657 \times 1 + 306; \\
657 &= 306 \times 2 + 45; \\
306 &= 45 \times 6 + 36; \\
45 &= 36 \times 1 + 9; \\
36 &= 9 \times 4 + 0.
\end{aligned}$$

Hence we know $\mathrm{hcf}(963, 657) = 9$ which is the last non-zero remainder. Then we go backwards to find a linear combination which gives 1.

$$\begin{aligned}
9 &= 45 - 36 \\
&= 45 - (306 - 45) \\
&= 45 \times 7 - 306 \\
&= (657 - 306) - 306 \\
&= 657 \times 7 - 306 \times 15 \\
&= 657 \times 7 - (963 - 657) \times 15 \\
&= 657 \times 22 - 963 \times 15.
\end{aligned}$$

So $m = -15$ and $n = 22$ is one solution.

(2) Since $d = \mathrm{hcf}(a, b)$, there exist some $m, n \in \mathbb{Z}$, such that $d = am + bn$. (For example, the Euclidean algorithm can always give such a pair of (m, n).) By substituting, we get $d = da'm + db'n$, hence $1 = a'm + b'n$. If $\mathrm{hcf}(a', b') = k$, then $k \mid a'$ and $k \mid b'$, thus $k \mid a'm + b'n = 1$, which implies $\mathrm{hcf}(a', b') = 1$.

Solution 1.2. *Examples of arithmetic functions.*

(1) We factor $360 = 2^3 \times 3^2 \times 5^1$. By the formulas in Proposition 1.19, Definition 1.20 and Proposition 1.29, we have

$$\begin{aligned}
\nu(360) &= (3+1)(2+1)(1+1) = 24;\\
\sigma(360) &= \frac{2^4-1}{2-1} \times \frac{3^3-1}{3-1} \times \frac{5^2-1}{5-1} = 15 \times 13 \times 6 = 1170;\\
\mu(360) &= 0 \qquad \text{since 360 is not square-free;}\\
\phi(360) &= 360 \times (1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5}) = 96.
\end{aligned}$$

Similarly we have $429 = 3 \times 11 \times 13$. Therefore

$$\begin{aligned}
\nu(429) &= (1+1)(1+1)(1+1) = 8;\\
\sigma(429) &= \frac{3^2-1}{3-1} \times \frac{11^2-1}{11-1} \times \frac{13^2-1}{13-1} = 4 \times 12 \times 14 = 672;\\
\mu(429) &= (-1)^3 = -1 \qquad \text{since 429 is square-free;}\\
\phi(429) &= 429 \times (1-\frac{1}{3})(1-\frac{1}{11})(1-\frac{1}{13}) = 240.
\end{aligned}$$

(2) There are two different proofs. We show one of them here. The other proof will be given together with part (3). We consider two separate cases: if n has any odd prime factor p, then by Remark 1.30, $\phi(n)$ has a factor $p-1$ hence is even; if n has no odd prime factor, then we can write $n = 2^a$ for some $a \geqslant 2$, which implies $\phi(n) = 2^{a-1}$ by the same formula hence is even.

(3) Let $S = \{m \in \mathbb{Z} \mid 1 \leqslant m \leqslant n, \mathrm{hcf}(m,n) = 1\}$. When $n = 2$, the only element in S is 1, hence it is clear that the statement holds. From now on we assume $n \geqslant 3$. For every integer k with $k \leqslant \frac{n}{2}$, we consider the pair of integers $\{k, n-k\}$.

Let $m = \mathrm{hcf}(k,n)$ and $m' = \mathrm{hcf}(n-k,n)$. Then $m \mid k$ and $m \mid n$, hence $m \mid n-k$, which implies $m \mid m'$. A similar argument shows $m' \mid m$. Therefore $m = m'$, which implies either k and $n-k$ are both in S, or neither is in S.

The two integers k and $n-k$ in a pair are distinct unless $k = \frac{n}{2}$, which happens when n is even. However in such a case $\frac{n}{2} \notin S$ because $\mathrm{hcf}(n, \frac{n}{2}) = \frac{n}{2} > 1$. We conclude that S can be divided into pairs of distinct integers of the form $\{k, n-k\}$, which proves the number of elements in S, i.e. $\phi(n)$, is even. Moreover the sum of the two integers in a pair is n, and there are precisely $\frac{\phi(n)}{2}$ pairs in S (since there are $\phi(n)$ elements in S). This implies the sum of all elements in S is $n \cdot \frac{\phi(n)}{2}$, as required.

Solution 1.3. *Applications of Möbius inversion.*

By Example 1.18, for every $n \in \mathbb{Z}^+$, we can write

$$\nu(n) = \sum_{d \mid n} 1;$$

$$\sigma(n) = \sum_{d \mid n} d.$$

Therefore we apply Theorem 1.26 for $f(n) = 1$ and $F(n) = \nu(n)$ to obtain

$$1 = \sum_{d \mid n} \mu(d)\nu\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right)\nu(d)$$

which is the first statement. For $f(n) = n$ and $F(n) = \sigma(n)$ we obtain

$$n = \sum_{d \mid n} \mu(d)\sigma\left(\frac{n}{d}\right) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right)\sigma(d)$$

which is the second statement.

Solution 1.4. *Unique factorisation in the ring of Gaussian integers.*

(1) The formula is in fact true for any complex numbers. For any $\alpha \in \mathbb{C}$, we have $\nu(\alpha) = \alpha\overline{\alpha}$. Hence for any $\alpha, \beta \in \mathbb{C}$, we have

$$\nu(\alpha\beta) = \alpha\beta \cdot \overline{\alpha\beta} = \alpha\overline{\alpha} \cdot \beta\overline{\beta} = \nu(\alpha)\nu(\beta).$$

(2) The commutative ring $\mathbb{Z}[i]$ does not have zero divisors because it is a subring of $\mathbb{C}$ in which there is no zero divisor. Now we check that ν is a Euclidean valuation.

Let $\alpha = a + bi$ and $\beta = c + di \neq 0$. We can divide α by β as complex numbers and write $\frac{\alpha}{\beta} = r + si$ where r, s are real numbers. Choose integers m, n such that $|r - m| \leqslant \frac{1}{2}$ and $|s - n| \leqslant \frac{1}{2}$ (the choice may not be unique). Set $\gamma = m + ni$, then $\gamma \in \mathbb{Z}[i]$ and $\nu(\frac{\alpha}{\beta} - \gamma) = (r - m)^2 + (s - n)^2 \leqslant \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$. Set $\delta = \alpha - \beta\gamma$, then $\delta \in \mathbb{Z}[i]$ and either $\delta = 0$ or $\nu(\delta) = \nu(\beta(\frac{\alpha}{\beta} - \gamma)) = \nu(\beta)\nu(\frac{\alpha}{\beta} - \gamma) \leqslant \frac{1}{2}\nu(\beta) < \nu(\beta)$. Hence ν defines a Euclidean valuation on $\mathbb{Z}[i]$, and $\mathbb{Z}[i]$ is a Euclidean domain.

(3) By Theorem 1.5 and Theorem 1.11, we know that a Euclidean domain is a UFD. Hence by part (2) we conclude that $\mathbb{Z}[i]$ is a UFD.

(4) Assume α is a unit, then there exists $\beta \in \mathbb{Z}[i]$, such that $ab = 1$. We apply the Euclidean valuation ν on both sides and use part (1) to get $\nu(\alpha)\nu(\beta) = \nu(1) = 1$. Since both $\nu(\alpha)$ and $\nu(\beta)$ are non-negative integer, the only possibility is $\nu(\alpha) = \nu(\beta) = 1$.

On the other hand, assume $\nu(\alpha) = 1$. Let $\alpha = a + bi$, then $a^2 + b^2 = 1$. This implies $(a + bi)(a - bi) = 1$. Since $a \pm bi \in \mathbb{Z}[i]$, we conclude that α divides 1, hence α is a unit.

To find all the units, we need to find all pairs of integers a, b such that $a^2 + b^2 = 1$. This is only possible when $a = \pm 1$ and $b = 0$, or $a = 0$ and $b = \pm 1$. In other words, $\alpha = \pm 1$ or $\pm i$.

(5) We prove by contradiction. Assume α is not irreducible. Then we can write $\alpha = \alpha_1\alpha_2$ where neither factor is zero or a unit. By part (4) we know $\nu(\alpha_1)$ and $\nu(\alpha_2)$ are both positive integers larger than 1. Therefore by part (1) we know $\nu(\alpha) = \nu(\alpha_1)\nu(\alpha_2)$ is composite, not a prime. Contradiction.

(6) We first show they are both irreducible factorisations of 5. We only need to check all factors are irreducible. This is true by part (5) because $\nu(2 \pm i) = \nu(1 \pm 2i) = 5$ is a prime integer.

We explain why this is consistent with unique factorisation. By Definition 1.10, unique factorisation means the number of irreducible factors agrees in two factorisations, and the corresponding factors are associated after reordering. In this example we have two irreducible factors in either factorisation. We can reorder the factors as $(2+i)(2-i) = 5 = (1-2i)(1+2i)$. Notice that $2+i = i\cdot(1-2i)$ and i is a unit in $\mathbb{Z}[i]$, so $2+i$ and $1-2i$ are associated. Similarly $2-i = (-i)\cdot(1+2i)$ implies that $2-i$ and $1+2i$ are also associated.