School of Mathematics and Statistics
MT4517 Rings & Fields
Exercises 1

Exercise 1.1. Find $\gcd(a, b)$ and integers x, y such that $xa + yb = \gcd(a, b)$ for the following pairs of natural numbers a and b

(i) $a = 55$ and $b = 21$;

(ii) $a = 127$ and $b = 44$;

(iii) $a = 442$ and $b = 90$.

Exercise 1.2. Prove that if $a \in \mathbb{N}$ is a prime and if $a|b_1b_2 \cdots b_n$ for some $b_1, b_2, \ldots, b_n \in \mathbb{Z}$, then $a|b_i$ for some i. [Hint: use induction on n.]

Exercise 1.3. The lowest common multiple (lcm) of two integers a, b is the smallest (in absolute value) integer divisible by both a and b. Prove that

$$ab = \gcd(a, b)\text{lcm}(a, b).$$

[Hint: write a and b as products of primes.]

Exercise 1.4. Let $a, b \in \mathbb{Z}$. Prove that

(i) if $2 \mid a$ and $2 \mid b$, then $\gcd(a, b) = 2\gcd(a/2, b/2)$;

(ii) if $2 \mid a$ and $2 \nmid b$, then $\gcd(a, b) = \gcd(a/2, b)$.

Exercise 1.5. Let $x, y \in \mathbb{Z}$ such that $3|x^2 + y^2$. Prove that $3|x$ and $3|y$. [Hint: if $3 \nmid x$, then x can be given in the form $3t - 1$ or $3t + 1$. Likewise with y.]

Exercise 1.6. Find the remainder of 2^{340} modulo 341.

Exercise 1.7. Use modular arithmetic to prove that $233 \cdot 577 \neq 135441$.

Exercise 1.8. Find $x, y \in \mathbb{Z}$ such that $89x + 55y = 1$ and find all the integer solutions x to

$$89x \equiv 7 \pmod{55}.$$

Exercise 1.9. What is the smallest odd natural number that leaves a remainder of 2 when divided by 3 and a remainder of 3 when divided by 5?

Exercise 1.10. Solve the following system of equations

$$\begin{aligned} x &\equiv 17 \pmod{504} \\ x &\equiv -4 \pmod{35} \\ x &\equiv -33 \pmod{16} \end{aligned}$$

for x.

Exercise 1.11. Let $a, b \in \mathbb{Z}$ such that there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Prove that a and b are coprime.

Exercise 1.12. Let $x, y, z \in \mathbb{Z}$ such that $5 \mid x^2 + y^2 + z^2$. Prove that $5|x$ or $5|y$ or $5|z$.

Exercise 1.13. Prove that there are infinitely many primes of the form $4k + 3$ and $6k + 5$.

Exercise 1.14. Let $a, b, x, y \in \mathbb{Z}$ such that $ax + by = d$ and where $x > 0$. Prove that there exist $x', y' \in \mathbb{Z}$ such that

$$ax' + by' = d$$

and where $0 \leqslant y' < a$.

Exercise 1.15. Let $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$. Prove that $\gcd(a^m, b^n) = 1$ for all $m, n \in \mathbb{N}$.

Exercise 1.16. Let $x \in \mathbb{Z}/(60)$, let $x \equiv a \pmod{3}$, let $x \equiv b \pmod{4}$, and let $x \equiv c \pmod{5}$. Prove that

$$x \equiv 40a + 45b + 36c \pmod{60}.$$