MATH 243 – Mathematical Structures
Selected Solutions for Problem Set 4

I. Let m, b be integers and consider the mapping $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = mx + b$.

(A) Prove that f is injective if and only if $m \neq 0$.

Solution: Since this is an "if and only if" statement, we must prove both implications.

$\Rightarrow$: Assume that f is an injective mapping. Then $x_1 \neq x_2$ in $\mathbb{Z}$ implies $f(x_1) = mx_1 + b \neq mx_2 + b = f(x_2)$. If $m = 0$, then this is a false statement because $f(x_1) = 0+b = 0+b = f(x_2)$. Hence f injective implies $m \neq 0$.

$\Leftarrow$: Assume that $m \neq 0$. If $f(x_1) = f(x_2)$, then we have $mx_1 + b = mx_2 + b$, so $mx_1 = mx_2$ and therefore $m(x_1 - x_2) = 0$. If $m \neq 0$, then the only way this can be true is for $x_1 - x_2 = 0$ and this shows $x_1 = x_2$. We have proved that f is injective (using the contrapositive form of the definition).

(B) Find conditions on m, b equivalent to saying f is surjective and prove your assertion.

Solution: Saying f is surjective means that for all $y \in \mathbb{Z}$, there must be some $x \in \mathbb{Z}$ such that $f(x) = mx + b = y$. We claim that this is true if and only if $m = \pm 1$.

$\Leftarrow$: If $m = \pm 1$, then we can solve the equation $mx + b = y$ for x and remain in the integers. Namely $x = \pm(y - b) \in \mathbb{Z}$. This shows that $m = \pm 1$ implies f is surjective.

$\Rightarrow$: Conversely, if f is surjective, then saying $f(x) = mx + b = y$ is solvable for all $y \in \mathbb{Z}$ says that $mx = y - b$ takes on every value in $\mathbb{Z}$ as x varies through $\mathbb{Z}$. In particular, this says $m\mathbb{Z} = \mathbb{Z}$ and that is true only when $m = \pm 1$.

II. Let b, c be integers and define $f : \mathbb{Z} \to \mathbb{Z}$ by $f(x) = x^2 + bx + c$.

(A) Show that f is *not injective*.

Solution: Recall the algebraic technique of completing the square in a quadratic function:

$$f(x) = x^2 + bx + c = (x + b/2)^2 + c - b^2/4$$

This shows that the graph $y = f(x)$ is a horizontally and vertically shifted version of the basic parabola $y = x^2$ (for $x \in \mathbb{Z}$). This shows the vertex is located at $(-b/2, c - b^2/4)$ but this may be a point whose coordinates are not integers. To show that $f(x)$ is not injective, it is enough to find two different x-values that give equal function values. Thinking of the shape of the parabola, we want two integer x-values the same distance away from $x = -b/2$, one to the left and one to the right. f will take the same value at both of them. Here, a direct computation shows that if $b \neq 0$, then

$$f(-b) = (-b)^2 + b \cdot -b + c = c = 0^2 + b \cdot 0 + c = f(0).$$

That is, $x = -b$ and $x = 0$ are located the same distance away from $x = -b/2$ on either side and give the same function value. On the other hand, if $b = 0$, then we can take $x = \pm 1$ and $f(-1) = 1 + c = f(1)$. This shows that f is not injective for any choice of b and c.

(B) Show that f is *not surjective.*

Solution: By the completion of the square done in part (A), note that $(x + b/2)^2 + c - b^2/4 \geq c - b^2/4$ for all $x \in \mathbb{Z}$. Hence the range of f contains no integer $y < c - b^2/4$ and f is not surjective.

III. For each of the following pairs of integers N, n, find the integer quotient q and remainder $0 \leq r < n - 1$ satisfying $N = qn + r$ as in Theorem 4.8.

(A) $N = 796$, $n = 26$

Solution: $796 = 30 \cdot 36 + 16$, so $q = 30$ and $r = 16$.

(B) $N = 1205$, $n = 37$

Solution: $1205 = 32 \cdot 37 + 21$, so $q = 32$ and $r = 21$.

(C) $N = -27$, $n = 7$.

Solution: $-27 = (-4) \cdot 7 + 1$, so $q = -4$ and $r = 1$.

From the Text:

Exercise 4.4.

(a) Let n and $n + 1$ be any two consecutive integers. Then

$$(n + 1)^2 - n^2 = n^2 + 2n + 1 - n^2 = 2n + 1.$$

Since n is an integer, this is odd.

(b) Let $N = (2k)^2$ be the square of an even integer $2k$. Then $N = 4k^2$, so N leaves a remainder of 0 on division by 4. On the other hand, if $N = (2\ell + 1)^2$ is the square of an odd integer $2\ell + 1$, then

$$N = 4\ell^2 + 4\ell + 1 = (\ell^2 + \ell) \cdot 4 + 1.$$

Since $\ell^2 + \ell \in \mathbb{Z}$ and $0 \leq 1 < 4$, the uniqueness of the quotient and remainder on division show that N leaves a remainder of 1 on division by 4 in this case.

(c) Assume that n and m are not both even. This means that there are three cases to consider

(i) n even and m odd,

(ii) n odd and m even,

(iii) n and m both odd.

In case (i), we claim the equation $n^2 = 2m^2$ is impossible. Arguing by contradiction, suppose $n^2 = 2m^2$ was true. First, n^2 leaves a remainder of 0 on division by 4 by part (b). On the other hand, $2m^2$ would equal $2(2k+1)^2$ for some $k \in \mathbb{Z}$. But

$$2(2k+1)^2 = 8k^2 + 8k + 2 = 4(2k^2 + 2k) + 2.$$

Since $2k^2 + 2k \in \mathbb{Z}$ and $0 \leq 2 < 4$, the uniqueness of the quotient and remainder on division implies that $2m^2$ leaves a remainder of 2 on division by 4. This is a contradiction, so $n^2 \neq 2m^2$ in this case.

In case (ii), again we claim $n^2 = 2m^2$ is impossible. The reason is that n^2 leaves a remainder of 1 on division by 4, but $2m^2$ would leave a remainder of 0.

Finally in case (iii) we again claim $n^2 = 2m^2$ is impossible. This case is similar to (ii) since the left side would leave a remainder of 1 on division by 4, but the right side would leave a remainder of 2.

(Note: this is also closely related to the proof we did that $\sqrt{2}$ is not a rational number and the contrapositive statement "If $n^2 = 2m^2$, then n and m are both even" can be proved with exactly the same reasoning we used there.)

Exercise 4.5. (c) The tables the problem asked for look like this. For addition:

$+$	$r_2 = 0$	$r_2 = 1$
$r_1 = 0$	0	1
$r_1 = 1$	1	0

The only nontrivial one is the case with $r_1 = r_2 = 1$. Then we have $n_1 = 2q_1 + 1$ and $n_2 = 2q_2 + 1$. Hence $n_1 + n_2 = 2q_1 + 1 + 2q_2 + 1 = 2(q_1 + q_2 + 1) + 0$. Since $q_1 + q_2 + 1 \in \mathbb{Z}$, the remainder on division by 2 is 0 in this case.

The corresponding table for multiplication is:

$\cdot$	$r_2 = 0$	$r_2 = 1$
$r_1 = 0$	0	0
$r_1 = 1$	0	1

In words, remainder on division of $n_1 \cdot n_2$ in this case will just be the product of the two remainders: $r_1 \cdot r_2$.

Exercise 4.6. In formulas, the general pattern is that if $n_1 = 5q_1 + r_1$ and $n_2 = 5q_2 + r_2$, then

$$n_1 + n_2 = 5(q_1 + q_2) + (r_1 + r_2).$$

But $r_1 + r_2 \geq 5$ is possible, so we can also divide 5 into that integer to obtain

$$r_1 + r_2 = 5q + r$$

and then

$$n_1 + n_2 = 5(q_1 + q_2 + q) + r$$

and the remainder on division of $n_1 + n_2$ is *the remainder on division by* 5 *of the sum* $r_1 + r_2$.

Similarly, we have

$$n_1 \cdot n_2 = (5q_1 + r_1) \cdot (5q_2 + r_2) = 5(5q_1q_2 + q_1r_2 + q_2r_1) + r_1 \cdot r_2.$$

But again $r_1 \cdot r_2 \geq 5$ is possible so if we divide again $r_1 \cdot r_2 = 5q + r$, then

$$n_1 \cdot n_2 = 5(5q_1q_2 + q_1r_2 + q_2r_1 + q) + r$$

and the remainder on division of $n_1 \cdot n_2$ is *the remainder on division by* 5 *of the product* $r_1 \cdot r_2$.

The possibilities can also be described by giving tables like the ones from the last problem. (For simplicity we omit the $r_2 =$ from the column headings and the $r_1 =$ from the row headings, but the idea is the same.)

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

and

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Exercise 4.8. We want to show that the equations can be solved for $u, v \in \mathbb{Z}$ if and only if a, b are either both even or both odd.

$\Rightarrow$: Assume the equations have integer solutions $u, v \in \mathbb{Z}$. The equations $u+v = a$ and $u-v = b$ can be added to produce $2u = a+b$ and subtracted to produce $2v = a-b$. It follows that $a+b = 2u$ and $a - b = 2v$ are both even integers. This implies (by the addition table from Exercise 4.5) that a, b are either both even or both odd.

$\Leftarrow$: Conversely, assume that a, b are either both even or both odd. Then (again by the addition table from Exercise 4.5) it follows that $a + b$ and $a - b$ are both even integers. Hence $a + b = 2u$ for some $u \in \mathbb{Z}$ and $a - b = 2v$ for some $v \in \mathbb{Z}$. This shows that $u = \frac{a+b}{2}$ and $v = \frac{a-b}{2}$ are integer solutions of the original equations, since adding we get $2a = 2(u + v)$, so $u + v = a$, and similarly subtracting, $2b = 2(u - v)$, so $u - v = b$.