5. Functions and bijections. Let $Y$ be a set and define $Y^2 = \{(y_1, y_2) \mid y_1, y_2 \in Y\}$. Define

$$F : Y^2 \to \text{Fun}(\mathbb{N}_2, Y)$$

by: for $(y_1, y_2) \in Y^2$, let $F(y_1, y_2) : 1 \mapsto y_1$ and $F(y_1, y_2) : 2 \mapsto y_2$. (Equivalently, $F(y_1, y_2)(1) = y_1$ and $F(y_1, y_2)(2) = y_2$.) Define

$$G : \text{Fun}(\mathbb{N}_2, Y) \to Y^2$$

by: for $f \in \text{Fun}(\mathbb{N}_2, Y)$, let $G(f) = (f(1), f(2))$. Prove that $G$ is the inverse of $F$.

Ans: Let $(y_1, y_2) \in Y^2$. Then $F(y_1, y_2) : 1 \mapsto y_1$ and $F(y_1, y_2) : 2 \mapsto y_2$. So

$$G(F(y_1, y_2)) = (F(y_1, y_2)(1), F(y_1, y_2)(2)) = (y_1, y_2).$$

Hence $G \circ F = I_{Y^2}$.

Next, we let $f \in \text{Fun}(\mathbb{N}_2, Y)$. Then $G(f) = (f(1), f(2))$. And $F(G(f)) = F(f(1), f(2)) \in \text{Fun}(\mathbb{N}_2, Y)$ is the function defined by

$$F(G(f)) : 1 \mapsto f(1),$$
$$F(G(f)) : 2 \mapsto f(2).$$

Thus $F(G(f)) = f$.

6. Linear diophantine equation.

(a) Find an integer solution $(m, n)$ to the equation $36m + 24n = 84$.

Ans: Dividing by gcd(36, 24) = 12, we obtain the equivalent equation

$$3m + 2n = 7.$$

$(1, 2)$ is a solution since $3 \cdot 1 + 2 \cdot 2 = 7$.

(b) Find all integer solutions $(m, n)$ such that $36m + 24n = 84$. In doing so, derive that this is the complete solution set (don’t just use a formula).

Ans: Since $(1, 2)$ is a solution, the equation is equivalent to

$$3(m - 1) = -2(n - 2).$$

Since gcd(3, 2) = 1, 2 divides $m - 1$. Hence there exists $k \in \mathbb{Z}$ such that $m - 1 = 2k$. This implies $3 \cdot 2k = -2(n - 2)$, so that $n - 2 = -3k$. That is,

$$m = 1 + 2k,$$
$$n = 2 - 3k, \text{ where } k \in \mathbb{Z}.$$

Conversely, $(m, n)$ of this form is a solution since then

$$3m + 2n = 3(1 + 2k) + 2(2 - 3k)$$
$$= 3 + 6k + 4 - 6k$$
$$= 7.$$
7. Division and the gcd. Let $a, b, c \in \mathbb{N}$. Let $g = \gcd(a, b)$. Prove that if $a$ divides $bc$, then $\frac{a}{g}$ divides $c$. \textbf{HINT:} Use a consequence of the Euclidean algorithm. \textbf{REMARK:} The case where $g = 1$ was a homework problem.

\textbf{Ans.} Since $g = \gcd(a, b)$, there exist $m, n, ma+nb = g$. Multiply this by $c$ to obtain $cma+cnb = cg$. Since $\frac{a}{g}$ and $\frac{b}{g}$ are integers, we may divide by $g$ to obtain the integer equation

$$c\frac{a}{g} + \frac{ncb}{g} = c.$$ 

Clearly $\frac{a}{g}$ divides the first term $c\frac{a}{g}$. On the other hand, $a$ divides $bc$, so that $\frac{a}{g}$ divides $\frac{ncb}{g}$. We conclude that $\frac{a}{g}$ divides the sum $c\frac{a}{g} + \frac{ncb}{g}$, that is, $\frac{a}{g}$ divides $c$.

8. The square root of a prime is irrational. Let $p$ be a prime number. Prove that $\sqrt{p}$ is irrational. \textbf{HINT:} You may use a consequence of Problem #7.

\textbf{Ans.} Suppose that $\sqrt{p}$ is rational. Then there exist integers $a$ and $b$ with $\gcd(a, b) = 1$ and $\sqrt{p} = \frac{a}{b}$. Then

$$b^2p = a^2.$$ 

Since $p$ divides $a^2$, we have that $p$ divides $a$ (a standard result). Hence there exists $k \in \mathbb{Z}$ such that $a = kp$. So $b^2p = a^2k^2p^2$ and hence $b^2 = a^2k^2$. Thus $p$ divides $b^2$, which implies $p$ divides $b$. We conclude that $\gcd(a, b) \geq p \geq 2$, which is a contradiction.

9. Remainders and squaring. Let $r_6 : \mathbb{Z} \to \mathbb{Z}_6$ be the remainder map.

(a) Prove that if $a, b \in \mathbb{Z}$ satisfy $r_6(a) = r_6(b)$, then $r_6(a^2) = r_6(b^2)$. \textbf{HINT:} Use the equality $a^2 - b^2 = (a + b)(a - b)$.

\textbf{Ans.} Suppose $r_6(a) = r_6(b)$. Then 6 divides $(a - b)$, which implies 6 divides $(a + b)(a - b)$. Since $a^2 - b^2 = (a + b)(a - b)$, this implies 6 divides $(a^2 - b^2)$. Hence $r_6(a^2) = r_6(b^2)$.

(b) Prove that if $a \in \mathbb{Z}$, then there exists an integer $c$ with $0 \leq c < 6$ such that $r_6(a) = r_6(c)$.

\textbf{Ans.} Let $c = r_6(a)$. Since $r_6(a) \in \mathbb{Z}_6$, we have $0 \leq c < 6$. Since $0 \leq c < 6$, we have $r_6(c) = c = r_6(a)$.

(c) It is a fact that $r_6(0^2) = 0$, $r_6(1^2) = r_6(5^2) = 1$, $r_6(2^2) = r_6(4^2) = 4$, $r_6(3^2) = 3$. Using this, prove that if $a \in \mathbb{Z}$, then $r_6(a^2) \in \{0, 1, 3, 4\}$.

\textbf{Ans.} Let $a \in \mathbb{Z}$. Then

$$r_6(a^2) = r_6((r_6(a))^2) \in \{r_6(0^2), r_6(1^2), r_6(2^2), r_6(3^2), r_6(4^2), r_6(5^2)\} = \{0, 1, 3, 4\}.$$ 

(d) Prove that if $d = 6p + 2$ for some $p \in \mathbb{Z}$ or if $d = 6q + 5$ for some $q \in \mathbb{Z}$, then $d$ is not a perfect square.

\textbf{Ans.} Suppose $d = 6p + 2$ for some $p \in \mathbb{Z}$ or $d = 6q + 5$ for some $q \in \mathbb{Z}$. Then $r_6(d) \in \{2, 5\}$. Since $\{2, 5\} \cap \{0, 1, 3, 4\} = \emptyset$, there does not exist $a \in \mathbb{Z}$ such that $r_6(d) = r_6(a^2)$. In particular, there does not exist $a \in \mathbb{Z}$ such that $d = a^2$.

10. Modular arithmetic.

(a) Let $m \in \mathbb{N}$. Prove: If $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$, then $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$.

\textbf{Ans.} Suppose $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$. Then there exist $k, \ell \in \mathbb{Z}$ such that

$$a_1 - a_2 = km \quad \text{and} \quad b_1 - b_2 = \ell m.$$ 

2
Thus

\[(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)\]
\[= km + ℓm\]
\[= (k + ℓ) m.\]

(b) Prove, using the definition of congruence and using properties of division, that $15a \equiv 15b \pmod{39}$ if and only if $a \equiv b \pmod{13}$.

**Ans.** We have $15a \equiv 15b \pmod{39}$ if and only if $a \equiv b \pmod{\frac{39}{\gcd(15,39)}}$. Since $\frac{39}{\gcd(15,39)} = 13$, this is true if and only if $a \equiv b \pmod{13}$.

(c) Find all solutions to the equation $6x \equiv 21 \pmod{15}$. And, how many solutions are there modulo 15?

**Ans.** $6x \equiv 21 \pmod{15}$ if and only if $2x \equiv 7 \pmod{5}$ if and only if $2x \equiv 12 \pmod{5}$ if and only if $x \equiv 6 \pmod{5}$. Hence the solution set is \{6 + 5k : k \in \mathbb{Z}\}. So there are 3 solutions modulo 15. For example, a maximal set of incongruent solutions is \{6, 11, 16\}. 