NB: Please deposit your solutions in the appropriate box **by 4 p.m. on the due date**. Late assignments or assignments placed into incorrect boxes will not be marked. Use a mathematics department cover sheet: these are available from outside the Resource Centre.

1. Let $*$ be an operation on a set A.

(a) Show that if $*$ has an identity element, then it is unique.

(b) Suppose $*$ is associative and has an identity element e. Let $x \in A$. An *inverse* of x is an element y such that $x * y = y * x = e$. Show that if x has an inverse, then the inverse is unique (note that when this Assignment was handed out in lectures the word "associative" was omitted in error).

(c) Let F be the set of all functions from $\mathbb{Z}$ to $\mathbb{Z}$. Then $\circ$ is an operation on F, and $1_{\mathbb{Z}}$ is an identity element of F under $\circ$. Give an example of functions f and g such that $f \circ g = 1_{\mathbb{Z}}$ but $g \circ f \neq 1_{\mathbb{Z}}$. [Hint: f and g must not be bijections: if f is a bijection and $f \circ g = 1_{\mathbb{Z}}$ then $g = (f^{-1} \circ f) \circ g = f^{-1} \circ (f \circ g) = f^{-1}$, i.e. $g = f^{-1}$, so we also have $g \circ f = 1_{\mathbb{Z}}$.]

2. For any integers a and b we have $(-a) \cdot b = -(a \cdot b)$. Prove this **from the axioms given in the notes**. You may use the result proved in lectures that for any n we have $n \cdot 0 = 0$. At each step you should indicate which axiom you are using.

3. Let $a, b \in \mathbb{N}$. Put $g = \gcd(a, b)$ and $l = \operatorname{lcm}(a, b)$. Our goal is to prove that $ab = gl$.

Since g is a common divisor of a and b we have $p, q \in \mathbb{N}$ with $a = pg$, $b = qg$. Put $z = pb$. Also, we know that there exist $x, y \in \mathbb{Z}$ with $g = ax + by$. Since l is a common multiple of a and b there exist $m, n \in \mathbb{N}$ with $l = am = bn$.

(a) Show that $z = qa$.

(b) Deduce that $l \mid z$, so there is some $t \in \mathbb{N}$ with $z = lt$.

(c) Show that $zg = ab$.

(d) Deduce that $lg \mid ab$.

(e) Show that $gl = axbn + byam$ (note that this was misprinted as $gl = axbn + byan$ when this Assignment was handed out in lectures).

(f) Deduce that $ab \mid gl$.

(g) Deduce that $ab = gl$.

4. Use the modified version of Euclid's Algorithm to find $\gcd(a, b)$ and integers x and y with $\gcd(a, b) = ax + by$ for the following pairs of integers.

(a) 128 and 60.

(b) 42 and 16.

(c) 1230 and 153.