Midterm

1. Suppose m and n are natural numbers. Prove that

   (a) any common divisor of m and n divides $\gcd(m, n)$

   (b) $\operatorname{lcm}(m, n)$ divides any common multiple of m and n

(i) By Bézout's theorem $\exists\, s, t \in \mathbb{Z}$ $d = sa + tb$

So any common divisor of a & b, divides d

(ii) Let $m = \operatorname{lcm}(a, b)$. Given a common multiple s of a & b

by the division algorithm $\exists!\, q, r \in \mathbb{Z}$ $s = qm + r$, $0 \le r < m$

Then $r = s - qm$ is a common multiple of a & b.

If $r > 0$, it contradicts the minimality of m. $\therefore r = 0$ $\therefore s = qm$ ☺

2. Use the extended Euclid's algorithm to find the multiplicative inverse of 17 modulo 37

$37 = 2 \cdot 17 + 3$ $\qquad 3 = 37 - 2 \cdot 17$

$17 = 5 \cdot 3 + 2$ $\qquad 2 = 17 - 5 \cdot 3$

$3 = 2 + 1$ $\qquad 1 = 3 - 2 = 3 - (17 - 5 \cdot 3) = -17 + 6 \cdot 3$

$= -17 + 6 \cdot (37 - 2 \cdot 17) = 6 \cdot 37 - 13 \cdot 17$

$\therefore 17^{-1} \equiv -13 \bmod 37 = 24 \bmod 37$

3. Determine for which natural numbers n we have $n! > 2^n$ and prove it by induction.

n	$n!$	2^n
0	1	1
1	1	2
2	2	4
3	6	8
4	24	16
5	120	32
6	720	64
...		

$n!$ grows faster than 2^n as $n \to \infty$, so we expect $n! > 2^n$ for large enough n. From computing some values it looks like it's for $n \geq 4$. Let's prove it.

(i) Basis: $n = 4$ $\quad 24 > 16$:)

(ii) Inductive step: for $n > 4$

$$n! = n(n-1)! > n2^{n-1} > 2 \cdot 2^{n-1} = 2^n$$:)

4. Prove that $\{1, -1\} \subseteq \mathbf{Z}$ is a multiplicative group and that it is isomorphic to $\mathbf{Z}_2$

$\cdot$	1	-1
1	1	-1
-1	-1	1

(i) Multiplication in $\mathbb{Z}$ is associative so $\{1,-1\}$ will inherit associativity

(ii) From the Cayley table we see closure, 1 is the identity of $\{1,-1\}$ and $1^{-1} = 1$, $(-1)^{-1} = -1$

$\therefore$ $\{1,-1\}$ is a group.

Define $f : \{1,-1\} \to \mathbb{Z}_2$ by

x	$f(x)$
1	0 mod 2
-1	1 mod 2

Then f is clearly bijective. To see that f is a hom. compute:

$\mathbb{Z}_2$:

+	0	1
0	0	1
1	1	0

$f(1 \cdot 1) = f(1) = 0 = 0 + 0 = f(1) + f(1)$

$f(1 \cdot (-1)) = f(-1) = 1 = 0 + 1 = f(1) + f(-1)$

$f((-1) \cdot 1) = f(-1) = 1 = 1 + 0 = f(-1) + f(0)$

$f((-1)(-1)) = f(1) = 0 = 1 + 1 \pmod 2 = f(-1) + f(-1)$

Alternately we can define $g: \mathbb{Z}_2 \to \{1, -1\}$ by $g(x) = (-1)^x$

y	$g(y)$
0 mod 2	1
1 mod 2	-1

g is well defined, since if x is even, then $(-1)^x = 1$

and if x is odd, $(-1)^x = -1$

It's easy to check that g is an isomorphism

In fact, f and g are compositional inverses ☺