Needed for Exercise 3.14 Group 1

~~Proof~~ To prove: $1+2+3+\dots n = \frac{1}{2}n(n+1)$

Proof (By PMI 1):

Fix n in $\mathbb{N}$.

Let $P(n) = 1+2+3+\dots+n = \frac{1}{2}n(n+1)$

Let $S = \{n \text{ in } \mathbb{N} \mid P(n) \text{ is true}\}$

So, $P(1) = \frac{1}{2} 1 (1+1) = 1 = 1$

So $P(1)$ is true.

Suppose $(P(i)$ is true.

Then $P(i) = 1+2+3 \dots + i = \frac{1}{2} i(i+1)$

Consider $P(i+1)$:

$$P(i+1) = P(i) + (i+1) = 1+2+3 \dots + i + i+1$$

$$= \frac{1}{2} i(i+1) + i + 1$$

$$= \frac{i^2+i+2i+2}{2}$$

$$= \frac{i^2+3i+2}{2}$$

$$= \frac{1}{2}(i+i)(i+2)$$

Then $P(i+1)$ is true.

So, $P(n)$ is true for all n in $\mathbb{N}$.

Ex: 3.1.4.

To prove: If n is odd in $\mathbb{N}$, then
$1+2+3+\dots+(n-1) \equiv 0 \pmod{n}$.

Proof: (Direct): Fix n an odd in $\mathbb{N}$.
Then from the proof above:
$1+2+3+\dots(n-1) = \frac{1}{2}(n-1)n$.
~~since~~ Since n is odd, $2 \mid n-1$.
Let $n-1 = 2q$.
Since $\frac{1}{2}(n-1)n = qn$, $n \mid qn = 1+2+3+\dots n-1$.

Thus $1+2+3+\dots n-1 \equiv 0 \pmod{n}$

Done.

Group 3 Theorem 3.9 (if)

fix a, b in $\mathbb{Z}$; n in $\mathbb{N}$, with $aX \equiv b \pmod{n}$, and $d = (a, n)$.

Let x_0 be a solution to $aX \equiv b \pmod{n}$.

Then $n \mid ax_0 - b$, and $ax_0 - b = ny$, for some y in $\mathbb{Z}$.

So $ax_0 + n(-y) = b$.

Thus the linear diophantine equation $aX + nY = b$ has a solution, and, by theorem 2.2, $(a, n) \mid b$. Therefore $d \mid b$ #

<u>Exercise</u> : Consider the system of congruences

$$S = \left\{ \begin{array}{l} X \equiv a_1 \pmod{n_1} \\ X \equiv a_2 \pmod{n_2} \end{array} \right\}.$$

The system has a solution iff $(n_1, n_2) \mid a_1 - a_2$.

<u>Proof</u> (if) (direct) We know $n_1 Y - n_2 Z = a_1 - a_2$ has a solution, call it y, z.

So $n_1 y - n_2 z = a_1 - a_2$, or $a_1 - n_1 y = a_2 - n_2 z$.

Let $x = a_1 - n_1 y = a_2 - n_2 z$.

Note $x \equiv a_1 - n_1 y \equiv a_1 - 0 \equiv a_1 \pmod{n_1}$.

Further $x \equiv a_2 - n_2 z \equiv a_2 - 0 \equiv a_2 \pmod{n_2}$.

So x is a solution to the system of congruences.

Proof (Direct): (Group 4)

Assume S has a solution, call it x.

Let $d = (n_1, n_2)$.

Since $d \mid n_1$ and $n_1 \mid x - a_1$, $d \mid x - a_1$; and

similarly, $d \mid x - a_2$.

That is, $dq = x - a_1$ and $dr = x - a_2$ for q and r in $\mathbb{Z}$.

So $dq + a_1 = dr + a_2 = x$. And $dr - dq = a_1 - a_2$.

Thus $d(r-q) = a_1 - a_2$, and $d \mid (a_1 - a_2)$.

$\blacksquare$