Name: Solutions

Directions: Solve the following problems. Give supporting work/justification where appropriate.

1. In each part, give a direct proof or a contrapositive proof.

(a) **[4 points]** Let $x, y \in \mathbb{Z}$. Prove that if xy is even, then x is even or y is even.

We prove the contrapositive: If x is odd and y is odd, then xy is odd.

Suppose that x and y are odd. We have that $x = 2k+1$ and $y = 2\ell+1$ for some $k, \ell \in \mathbb{Z}$. We compute

$$xy = (2k+1)(2\ell+1) = 4k\ell + 2k + 2\ell + 1$$
$$= 2(2k\ell + k + \ell) + 1.$$

Since $2k\ell + k + \ell \in \mathbb{Z}$, it follows that xy is odd. ∎

(b) **[3 points]** Let $a, b \in \mathbb{Z}$. Use part (a) to show that if $b \mid 2a$ and b is odd, then $b \mid a$.

We give a direct proof. Suppose $b \mid 2a$ and b is odd. Since $b \mid 2a$, we have that $2a = bk$ for some $k \in \mathbb{Z}$. Since the product bk equals the even integer $2a$, it follows from part (a) that b or k is even. Since b is odd, it must be that k is even. Therefore $k = 2t$ for some $t \in \mathbb{Z}$, and so $2a = bk = b(2t) = 2bt$. Dividing both sides by 2 gives $a = bt$. Since $t \in \mathbb{Z}$, we have that $b \mid a$. ∎

2. **[3 points]** Let $a, a', b, b' \in \mathbb{Z}$ and let $m \in \mathbb{N}$. Show that if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then $a + a' \equiv b + b' \pmod{m}$.

Note: There is an error in the statement of this problem. As written, the statement is FALSE. To see this, take $a = a' = 0$, $b = b' = 1$, and $m = 5$ (say). Now the hypotheses ($0 \equiv 0 \pmod 5$, $1 \equiv 1 \pmod 5$) are met, but the conclusion fails: $a + a' = 0$, $b + b' = 2$, but $0 \equiv 2 \pmod 5$ is clearly false.

The problem should have stated: If $a \equiv a' \pmod m$ and $b \equiv b' \pmod m$, then $a + b \equiv a' + b' \pmod m$.

Pf. Suppose $a \equiv a' \pmod m$ and $b \equiv b' \pmod m$. Then by definition, we have $m \mid a - a'$ and $m \mid b - b'$, and so $a - a' = k_1 m$ and $b - b' = k_2 m$ for some $k_1, k_2 \in \mathbb{Z}$. Adding these gives

$$(a - a') + (b - b') = k_1 m + k_2 m$$

which becomes $(a+b) - (a'+b') = (k_1 + k_2) m$ after rearranging terms. Since $k_1 + k_2 \in \mathbb{Z}$, we have that $m \mid (a+b) - (a'+b')$ and so $a + b \equiv a' + b' \pmod m$ by definition. ∎