Week 6 Group Work

1. True or false?

   (a) **True** or **False**? $20 \equiv 38 \mod 4$

   This is false because $20 - 38 = -18$ which is not divisible by 4.

   (b) **True** or **False**? $-9 \equiv -5 \mod 4$

   This is true because $-9 - (-5) = -4$ which is divisible by 4.

   (c) **True** or **False**? $15 \equiv 2 \mod 0$

   This is false because $15 - 2 \neq 0$ and 0 does not divide any nonzero integer.

   (d) **True** or **False**? $81 \equiv -92 \mod 1$

   This is true because 1 divides every integer.

2. Prove the following statements about congruences

   (a) For all $a \in \mathbb{Z}$, $a \equiv a \mod m$

   Note that $m \mid 0 = a - a$, so $a \equiv a \mod m$

   (b) For all $a, b \in \mathbb{Z}$, $a \equiv b \mod m$ if and only if $b \equiv a \mod m$

   Suppose that $a \equiv b \mod m$. Then $m \mid a - b$, so there exists $k \in \mathbb{Z}$ so that $mk = a - b$. Observe then that $b - a = m(-k)$, so $m \mid b - a$ and hence, $b \equiv a \mod m$.

   Now suppose that $b \equiv a \mod m$. Then the previous argument with the roles of a and b reversed shows that $a \equiv b \mod m$. Therefore, $a \equiv b \mod m$ if and only if $b \equiv a \mod m$.

   (c) For all $a, b, c \in \mathbb{Z}$, if $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$

   Suppose that $a \equiv b \mod m$ and $b \equiv c \mod m$. Then there exist $k, j \in \mathbb{Z}$ so that $a - b = mk$ and $b - c = mj$. Then
   $$a - c = (a - b) + (b - c) = mk + mj = m(k + j)$$
   and hence, $m \mid a - c$, so $a \equiv c \mod m$.

   (d) If $a \equiv b \mod m$, then $a + c \equiv b + c \mod m$

   Suppose that $a \equiv b \mod m$ so that there exists $k \in \mathbb{Z}$ with $mk = a - b$. Then
   $$(a + c) - (b + c) = a - b = mk$$
   so $m \mid (a + c) - (b + c)$ and hence, $a + c \equiv b + c \mod m$.

   (e) If $a \equiv b \mod m$, then $ac \equiv bc \mod m$

   Suppose $a \equiv b \mod m$. Then there exists $k \in \mathbb{Z}$ so that $mk = a - b$. Then
   $$ac - bc = c(a - b) = cmk$$
   so $m \mid ac - bc$, which implies that $ac \equiv bc \mod m$.

3. Is it true that if $ac \equiv bc \mod m$ then $a \equiv b \mod m$?

   The claim is untrue. Take $m = 10$, $a = 5$, $b = 4$, and $c = 100$. Then $ac = 500$ and $bc = 400$, which are congruent mod 10. But 4 and 5 are not congruent mod 10.

4. Find all solutions to the diophantine equation $102x + 1001y = 1$. If there are none, modify the equation appropriately so that there is at least one solution and classify all solutions to that equation.

   We apply the extended Euclidean algorithm with $r_0 = 1001$, $r_1 = 102$, $r_j = q_{j+1}r_{j+1} + r_{j+2}$, $s_0 = 1$, $s_1 = 0$, $s_{j+2} = s_j - q_{j+1}s_{j+1}$, $t_0 = 0$, $t_1 = 1$, and $t_{j+2} = t_j - q_{j+1}t_{j+1}$. Whew.

	$s_0 = 1$	$t_0 = 0$
	$s_1 = 0$	$t_1 = 1$
$1001 = 9 \cdot 102 + 83$	$s_2 = 1$	$t_2 = -9$
$102 = 1 \cdot 83 + 19$	$s_3 = -1$	$t_3 = 10$
$83 = 4 \cdot 19 + 7$	$s_4 = 5$	$t_4 = -49$
$19 = 2 \cdot 7 + 5$	$s_5 = -11$	$t_5 = 108$
$7 = 1 \cdot 5 + 2$	$s_6 = 16$	$t_6 = -157$
$5 = 2 \cdot 2 + 1$	$s_7 = -43$	$t_7 = 422$
$2 = 2 \cdot 1 + 0$		

   Observe now that $-43 \cdot 1001 + 422 \cdot 102 = 1$. Therefore, $(1001, 102) = 1$. Hence, by theorem 3.23, every solution has the form $x = -43 + 102k$ and $y = 422 + 1001k$ for some $k \in \mathbb{Z}$.

5. Let a and b be relatively prime positive integers and let n be a positive integer. A solution $(x, y) \in \mathbb{Z}^2$ of the linear diophantine equation $ax + by = n$ is nonnegative if both x and y are nonnegative. Show that whenever $n \geqslant (a-1)(b-1)$, there is a nonnegative solution of $ax + by = n$.

Suppose that $n \geqslant ab - a - b + 1$. Consider the numbers of the form $n - kb$ for $0 \leqslant k < a$.

We claim that the numbers of the form $n - kb$ for $0 \leqslant k < a$ are distinct mod a. Let $S = \{n - kb : 0 \leqslant k < a\}$. Pick two elements of S, say $n - kb$ and $n - jb$ and suppose that $n - kb \equiv n - jb \mod a$. Then $-kb \equiv -jb \mod a$. Since $-b$ is relatively prime to a, we can divide both sides by b and find that $k \equiv j \mod a$. Since $0 \leqslant k, j < a$ and $k \equiv j \mod a$, it must be the case that $k = j$. By contrapositive, we conclude that if $n - kb, n - jb \in S$ and $k \neq j$, then $n - kb \not\equiv n - jb \mod a$.

Since S has a elements in it and all are distinct mod a, S must be a complete set of residues modulo a. Hence, some element of S is congruent to $0 \mod a$. Suppose that $n - kb \equiv 0 \mod a$ for some $0 \leqslant k < a$. Then there exists $j \in \mathbb{Z}$ so that $n - kb = aj$, i.e. $n = aj + kb$.

We now argue that $j, k \geqslant 0$. Since $n - kb \in S$, we automatically have $k \geqslant 0$. Since $n \geqslant ab - a - b + 1$ and since $k \leqslant a - 1$, we have

$$\begin{aligned} n - kb &\geqslant ab - a - b + 1 - kb \\ &\geqslant ab - a - b + 1 - (a-1)b \\ &= 1 - a \end{aligned}$$

However, $n - kb$ is a multiple of a. The only multiples of a which are greater than or equal to $1 - a$ are $0, a, 2a, 3a, \ldots$, Hence, $n - kb$ must be a nonnegative multiple of a. Therefore, $j \geqslant 0$.

Hence, $ax + by = n$ has a nonnegative solution when $n \geqslant (a-1)(b-1)$.