due Feb 14 | Homework Set 5 (section 2.1 – 2.3) | Name: _____

1. Let a, b, and $n > 0$ be integers. Prove that $a \equiv b \bmod n$ if and only if a and b leave the same remainder when divided by n.

Let a, b, and n be positive integers. Suppose $a \equiv b \bmod n$. By the Division Algorithm, $a = nq_1 + r_1$ and $b = nq_2 + r_2$ where q_1, q_2, r_1, and r_2 are integers and $0 \le r_1, r_2 < n$. Then $a - c = (nq_1 + r_1) - (nq_2 + r_2) = nq_1 + (r_1 - (nq_2 + r_2))$
$= nq_1 + ((r_1 - nq_2) - r_2) = nq_1 + ((-nq_2 + r_1) - r_2) = nq_1 + (-nq_2 + (r_1 - r_2)) = (nq_1 - nq_2) + (r_1 - r_2)$
$= n(q_1 - q_2) + (r_1 - r_2)$. Since n divides $a - c$ by definition, we know that n must divide $r_1 - r_2$. Hence there is an integer k such that $r_1 - r_2 = nk$. Then $r_1 = r_2 + nk$. If $k \ge 1$, then $r_1 \ge n$. If $k \le -1$, then $r_1 < 0$. Neither of these situations can occur. Thus, $k = 0$, which implies that $r_1 = r_2$.

Conversely, suppose $a = nq_1 + r$ and $b = nq_2 + r$ for some integers q_1, q_2, and r with $0 \le r < n$. Then $a - b = (nq_1 + r) - (nq_2 + r) = nq_1 - nq_2 = n(q_1 - q_2)$. By definition, $a \equiv b \bmod n$.

2. Let a, b, and $n > 0$ be integers. If $ab = 0$ in $\mathbb{Z}_n$, then either prove or disprove that either $a = 0$ or $b = 0$. What about in $\mathbb{Z}_p$ where p is prime?

If n is not a prime, the statement is false. Consider: $2 \cdot 3 = 0$ in $\mathbb{Z}_6$.

Suppose p is prime. Let $a, b, n > 0$ be integers and $ab = 0$ in $\mathbb{Z}_p$. By Theorem 2.3, $ab \equiv 0 \bmod p$. By definition, there is an integer k such that $ab = pk$. By definition, p divides ab. Apply Theorem 1.8 to get that p divides a or b. This is equivalent to $a \equiv 0 \bmod p$ or $b \equiv \bmod p$. Apply Theorem 2.3 to get that $a = 0$ or $b = 0$ in $\mathbb{Z}_p$.

3. Write out the addition and multiplication tables for $\mathbb{Z}_8$.

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

•	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

4. Let a, b, and $n > 1$ be integers. If $[a]x = [b]$ has a solution in $\mathbb{Z}_n$, prove that the $\gcd(a, n)$ divides b. (Hint: if $x = [r]$ is a solution, then $[ar] = [b]$ implying that $ar - b = nk$ for some integer k. Be sure to give the reasons why all of these statements are true.)

Let a, b, and $n>1$ be integers such that $[a]x=[b]$ has a solution in $\mathbb{Z}_n$. Let $x=[r]$ be a solution. Then $[b]=[a]x=[a][r]=[ar]$. By Theorem 2.3, $ar \equiv b \bmod n$. By definition, $ar-b=nk$ for some integer k. Rearranging terms yields $b = ar-nk$.

Let $d=\gcd(a,n)$. Then by definition there exist integers t and s such that $a=dt$ and $n=ds$.

Then $b = ar-nk = (dt)r - (ds)k = d(tr)-d(sk) = d(tr-sk)$.

Thus, d divides b by definition.

5. Answer the following computational questions. Show all necessary work.
   a. For which a does $ax = 1$ have a solution in $\mathbb{Z}_8$? You may assume that $0 \leq a < 8$.

For $a=1, 3, 5$, and 7, the equation $ax=1$ will have a solution in $\mathbb{Z}_8$.

   b. Compute: $(x+2)^5$ in $\mathbb{Z}_5$

$$(x+2)^5 = x^5 + 5x^4(2) + 10x^3(2)^2 + 10x^2(2)^3 + 5x(2)^4 + (2)^5$$
$$= x^5 + 2^5 = x^5 + 32$$
$$= x^5 + 2 \quad \text{in } \mathbb{Z}_5$$

   c. Compute: $(x+2)(x+3)$ in $\mathbb{Z}_5$

$$(x+2)(x+3) = x^2 + 5x + 6 = x^2 + 1 \quad \text{in } \mathbb{Z}_5$$