UH - Math 3330 - Dr. Heier - Spring 2014
HW 5 - Solutions to *Selected* Homework Problems
by Angelynn Alvarez

2. (Section 2.5, Problem 17) Find a solution $x \in \mathbb{Z}$ $0 \leq x < n$, for the following congruence.

$$25x \equiv 31(\text{mod}7)$$

Solution. Because $\gcd(25, 7) = 1$, we know there exists $s, t \in \mathbb{Z}$ such that $1 = 25s + 7t$. Using the Division Algorithm yields

$$25 = 7(3) + 4, \;\; 7 = 4(1) + 3, \;\; 4 = 3(1) + 1, \;\; 3 = 1(3)$$

Thus,

$$4 = 25 - 7(3), \;\; 3 = 7 - 4(1), \;\; 1 = 4 - 3(1)$$

When we substitute, we get

$$\begin{aligned} 1 &= 4 - 3(1) \\ &= 4 - (7 - 4(1))(1) \\ &= 4(2) + 7(-1) \\ &= (25 - 7(3))(2) + 7(-1) \\ &= 25(2) + 7(-7) \end{aligned}$$

So $1 = 25(2) + 7(-7)$. Multiplying by 31 gives us

$$31 = 25(62) + 7(-217)$$

Therefore, $31 \equiv (25)(62)(\text{mod}7)$, so $x = 62$ is a solution. Note that we need $0 \leq x < 7$. Because $[62]_7 = [6]_7$, we have that $\boxed{x = 6}$ is the solution.

3. (Problem 2.5, Section 32) Prove or disprove that if n is odd, then $n^2 \equiv 1(\text{mod}8)$.

Solution. This statement is indeed **true.**

Proof. Assume n is odd. So $\exists\, k \in \mathbb{Z}$ such that $n = 2k + 1$. Therefore

$$n^2 - 1 = (2k + 1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k^2 + 4k = 4k(k + 1)$$

Consider two cases: (1) k is odd, and (2) k is even. If k is odd, then $k + 1$ is even. Thus, $k(k + 1)$ is even. If k is even, then $k + 1$ is odd. Thus $k(k + 1)$ is again even. Thus, in both cases, $k(k + 1)$ is even. Therefore, $\exists\, m \in \mathbb{Z}$ such that $k(k + 1) = 2m$. Hence, $n^2 - 1 = 4k(k + 1) = 4(2m) = 8m$. Therefore, $8 \mid (n^2 - 1)$ and $n^2 \equiv 1(\text{mod}8)$. □

4. (Section 2.5, Problem 53b) Solve the following system of congruences.

$$x \equiv 4(\text{mod}5)$$

$$x \equiv 2(\text{mod}3)$$

Solution. From the first congruence, $x \equiv 4(\text{mod}5)$, we have that $\exists\, k \in \mathbb{Z}$ such that $x = 4+5k$. Substituting this into the second congruence yields

$$4 + 5k \equiv 2(\text{mod}3) \Leftrightarrow 1 + 2 \equiv 2(\text{mod}3) \Leftrightarrow 2k \equiv 2 - 1(\text{mod}3) = 1(\text{mod}3)$$

Hence, $k = 2(\text{mod}3)$. Therefore, $x = 4 + 5(2) = 14$, and $\boxed{x \equiv 14(\text{mod}5 \cdot 3)}$ gives all solutions to the system of congruences.

6. (Section 2.5, Problem 53g) Solve the following system of congruences.

$$x \equiv 2(\text{mod}3)$$
$$x \equiv 2(\text{mod}5)$$
$$x \equiv 4(\text{mod}7)$$
$$x \equiv 3(\text{mod}8)$$

Solution. From the first congruence, $x \equiv 2(\text{mod}3)$, we know that $\exists\ k \in \mathbb{Z}$ such that $x = 2 + 3k$. Substituting this for x into the second congruence, $x \equiv 2(\text{mod}5)$, gives us

$$2 + 3k \equiv 2(\text{mod}5) \Leftrightarrow 3k \equiv 0(\text{mod}5) \Leftrightarrow k \equiv 0(\text{mod}5)$$

Therefore, $x \equiv 2(\text{mod}15)$ solves the first two congruences. Now we pair the solution with congruence (3). So our system of congruences becomes

$$x \equiv 2(\text{mod}15)$$
$$x \equiv 4(\text{mod}7)$$

From the solution to the first two congruences, we know that $\exists\, l \in \mathbb{Z}$ such that $x = 2 + 15l$. Substituting this into the third congruence gives us

$$2 + 15l \equiv 4(\text{mod}7) \Leftrightarrow 15l \equiv 2(\text{mod}7) \Leftrightarrow l \equiv 2(\text{mod}7)$$

Hence $x = 2 + 15(2) = 32$, and $x \equiv 32(\text{mod}7 \cdot 15)$ solves the first three congruences. Finally, pairing this solution with the last congruence, $x \equiv 3(\text{mod}8)$, gives us

$$x \equiv 32(\text{mod}7 \cdot 15)$$
$$x \equiv 3(\text{mod}8)$$

From the solution to the first three congruences, we know that $\exists\ m \in \mathbb{Z}$ such that $x = 32 + 105m$. Substituting this into the fourth congruence yields

$$32 + 105k \equiv 3(\text{mod}8) \Leftrightarrow 0 + k \equiv 3(\text{mod}8)$$

Hence, $x = 32 + 105(3) = 347$. Therefore, $\boxed{x \equiv 347(\text{mod}840)}$ solves the system of congruences.

7. (Section 2.6, Problem 11) Solve the following system of equations in $\mathbb{Z}_7$.

$$[2][x] + [y] = [4], \quad [2][x] + [4][y] = [5]$$

Solution. Subtracting the top equation from the bottom equation results in us eliminating $[x]$ and the equation

$$[4][y] - [y] = [5] - [4]$$

which simplifies to $[3][y] = [1]$.
Thus $y = [1][3]^{-1}$. Now we must find that $[3]^{-1}$ is in $\mathbb{Z}_7$. To do so, we use the Division Algorithm on the numbers 3 and 7. This gives us

$$7 = 3(2) + 1, \quad 3 = 3(1)$$

Solving for the nonzero remainder yields $1 = 7 - 3(2) = 3(-2) + 7$. Thus, $[3][-2] = [1]$, and $[3]^{-1} = [-2] = [5]$ in $\mathbb{Z}_7$. Thus, $y = [1][3]^{-1} = [1][5] = [5]$.

Now we must solve for $[x]$. Substituting $[y] = [5]$ into the first equations yields

$$[2][x] + [5] = [5] \Longleftrightarrow [2][x] = [4] - [5] = [-1] = [6]$$

Thus, $x = [2]^{-1}[6]$. Because $[2]^{-1} = [4]$ in $\mathbb{Z}_7$, we have that $x = [2]^{-1}[6] = [4][6] = [24] = [3]$ Therefore, the solution to the system is $\boxed{[x] = [3] \text{ and } [y] = [5]}$.

9. (Section 2.6, Problem 20) Let p be a prime integer. Prove that $[1]$ and $[p-1]$ are the only elements in $\mathbb{Z}_p$ that are their own multiplicative inverses.

Proof. Assume p is a prime integer. Then

$$[1][1] = [1], \text{ and } [p-1][p-1] = [-1][-1] = [1]$$

in $\mathbb{Z}_p$, Thus $[1]$ and $[p-1]$ are their own inverses.

Now we must show that these two are the *only* elements that are their own inverses. Let $x \in \mathbb{Z}_p$. Assume that x is its own inverse—that is,

$$[x][x] = [x^2] = [1]$$

Thus,

$$[x^2] - 1 = [0] \Leftrightarrow [x^2 - 1] = [0] \Leftrightarrow [(x+1)(x-1] = [0] \Leftrightarrow [x+1][x-1] = [0]$$

Because p is prime, $\mathbb{Z}_p$ has no zero divisors. Thus, if $[x+1][x-1] = [0]$, then either $[x+1] = [0]$ or $[x-1] = 0$. So $[x] = [-1] = [p-1]$ or $[x] = [1]$. Hence, the only elements in $\mathbb{Z}_p$ which are their own multiplicative inverses are $[1]$ and $[p-1]$. $\square$