Discrete Mathematics - CSCE 531 Fall 2018
In-Class Exercises, Day 5 (17 Oct 18)
Congruences

From Section 4.4

1. (Inspired by Problem 3) By testing possible candidates, find a multiplicative inverse of $4 \bmod 9$, i.e. find an $x \in \{0, 1, \ldots 8\}$ such that $4x \bmod 9 = 1$.

$$\begin{aligned}
&x = 0?\, 4 \cdot 0 \bmod 9 = 0 \neq 1 \\
&x = 1?\, 4 \cdot 1 \bmod 9 = 4 \neq 1 \\
&x = 2?\, 4 \cdot 2 \bmod 9 = 8 \neq 1 \\
&x = 3?\, 4 \cdot 3 \bmod 9 = 12 \bmod 9 = 3 \neq 1 \\
&x = 4?\, 4 \cdot 4 \bmod 9 = 16 \bmod 9 = 7 \neq 1 \\
&x = 5?\, 4 \cdot 5 \bmod 9 = 20 \bmod 9 = 2 \neq 1 \\
&x = 6?\, 4 \cdot 6 \bmod 9 = 24 \bmod 9 = 6 \neq 1 \\
&x = 7?\, 4 \cdot 7 \bmod 9 = 28 \bmod 9 = 1
\end{aligned}$$

Thus, $\overline{4} = 7 \bmod 9$.

2. (Inspired by Problem 5a) Find an inverse of $4 \bmod 9$ using the Euclidean algorithm and the method of Bezout's coefficients as shown in Example 2 (page 276). Obviously, you should get the same answer as you did for the previous exercise (up to equivalence under the modulus).

To apply the Euclidean algorithm, we begin by writing $9 = 2 \cdot 4 + 1$ (i.e. $9 \bmod 4 = 1$), and then $4 = 4 \cdot 1 + 0$ (i.e. $4 \bmod 1 = 0$), which terminates the algorithm.

The last step with nonzero remainder is $9 = 2 \cdot 4 + 1$, which we rearrange to isolate the remainder

$$1 = 9 - 2 \cdot 4 = 1 \cdot 9 - 2 \cdot 4$$

and then write as a congruence in the modulus of interest

$$\begin{aligned}
1 &\equiv -2 \cdot 4 (\bmod 9) \\
1 &\equiv 7 \cdot 4 (\bmod 9).
\end{aligned}$$

The last statement implies the solution

$$\overline{4} = 7 (\bmod 9).$$

3. (Inspired by Problem 5b) Find an inverse of 19 modulo 141 using the Euclidean algorithm and the method of Bezout's coefficients. That is, find x such that $x \cdot 19 \equiv 1 \pmod{141}$.

Euclidean algorithm:

$$141 = 7 \cdot 19 + 8$$
$$19 = 2 \cdot 8 + 3$$
$$8 = 2 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

Isolate last non-zero remainder:

$$1 = 3 - 1 \cdot 2$$
$$1 = 3 - 1 \cdot (8 - 2 \cdot 3) = -1 \cdot 8 + 3 \cdot 3$$
$$1 = -1 \cdot 8 + 3 \cdot (19 - 2 \cdot 8) = 3 \cdot 19 - 7 \cdot 8$$
$$1 = 3 \cdot 19 - 7 \cdot (141 - 7 \cdot 19) = -7 \cdot 141 + 52 \cdot 19$$

Rewrite as a congruence:

$$1 \equiv -7 \cdot 141 + 52 \cdot 19 \pmod{141}$$
$$1 \equiv 52 \cdot 19 \pmod{141}$$

Identify multiplicative inverse:

$$\overline{19} \equiv 52 \pmod{141}$$

4. (Inspired by Problem 9) Solve the congruence $4x \equiv 5 \pmod 9$ using the inverse of $4 \bmod 9$ found previously.

If we were doing algebra over the reals, we would divide both sides by 4, which is the same thing as multiplying by the multiplicative inverse of 4. So,

$$\overline{4} \cdot (4x) \equiv \overline{4} \cdot (5) \pmod 9$$
$$\left(\overline{4} \cdot 4\right)x \equiv \left(\overline{4} \cdot 5\right) \pmod 9$$
$$\left(\overline{4} \cdot 4\right)x \equiv (7 \cdot 5) \pmod 9$$
$$(1)x \equiv (35) \pmod 9$$
$$x \equiv 8 \pmod 9$$