Tutorial 4 - Week 5

John O'Sullivan

In class on Wednesday, we solved:

$$7x \equiv 4 \bmod 9$$

by seeing (using **brute force**) that we could 'cancel' 7 from the left-hand side by multiplying both sides by the inverse of 7 mod 9, which is 4:

$$\begin{aligned} 7x &\equiv 4 \bmod 9 \\ \implies 4(7x) &\equiv 4(4) \bmod 9 \\ \implies 28x &\equiv 16 \bmod 9 \\ \implies 1x &\equiv 16 \bmod 9 \\ \implies x &\equiv 7 \bmod 9 \end{aligned}$$

When the numbers are too large to use the *brute force* approach, we need to follow the method below, in **Problem 1**:

Problem 1. This problem is carried over from Tutorial 3. It's important to be able to solve problems of the type $ax \equiv b \bmod n$. If we can find the inverse of a, mod n, we can then use it to 'cancel' a from the left-hand side, and thus solve for x in the equation. e.g.:

Solve the following equation:

$$19x \equiv 3 \bmod 81 \tag{1}$$

Idea:
Use the extended Euclidean algorithm to find the inverse of 19 mod 81.
Where $19 = a$, we want $\bar{a}$:

$$19\bar{a} \equiv 1 \bmod 81$$

Trying all possible $\bar{a}$'s $\in \{0, 1, 2, 3, \ldots 80\}$ is a lot of work. Thankfully we don't need to do this! We can relate this to a Diophantine equation. Note that:

$$\begin{aligned}
&19\bar{a} \equiv 1 \bmod 81 \\
&\iff 81|(19\bar{a} - 1) \\
&\iff 81k = 19\bar{a} - 1 \text{ for some } k \in \mathbb{Z} \\
&\iff 1 = 19\bar{a} - 81k \\
&\iff 1 = 19\bar{a} + 81y \text{ for } k = -y
\end{aligned}$$

This is just a **Diophantine** equation where we want to express $(19, 81) = 1$ as a linear combination of 19 and 81. We know how to do this using the **extended Euclidean algorithm**. We want the value of $\bar{a}$ that results (we don't need y, though we end up finding this too).

Next, we multiply equation (1) by $\bar{a}$:

$$\begin{aligned}
\bar{a}19x &\equiv \bar{a}3 \bmod 81 \\
\implies 1x &\equiv \bar{a}3 \bmod 81 \\
\implies x &\equiv \bar{a}3 \bmod 81
\end{aligned}$$

Note how we use $\bar{a}$ to 'cancel' 19 as we specifically found it to be congruent to 1 mod 81.

So all you need to do is **find** $\bar{a}$ and then the solution is:

$$\implies x \equiv \bar{a}3 \bmod 81$$

Problem 2. Now we know two methods to solve linear congruences: **brute force** or using the **extended Euclidean algorithm** to find the inverse needed.

But don't forget that we don't always have a solution, and sometimes we have more than one. Remember **Theorem 26**, which stated that $ax \equiv b \bmod n$ has solutions if and only if $(a, n) = c|b$. And if $c|b$, then there are exactly c incongruent solutions mod n. These solutions are generated by:

$$x = x_0 + \frac{n}{c}t \tag{2}$$

where x_0 is one particular solution, and $t \in \mathbb{Z}$. Let $t = 0, 1, 2, \dots$ to generate all solutions. Stop when you have found c solutions. (If you continue, you will just repeat the solutions, mod n.)

With this in mind, solve the following (or state if no solutions exist):

$$2x \equiv 5 \bmod 7 \tag{3}$$
$$3x \equiv 2 \bmod 7 \tag{4}$$
$$3x \equiv 6 \bmod 9 \tag{5}$$
$$6x \equiv 3 \bmod 9 \tag{6}$$
$$15x \equiv 9 \bmod 25 \tag{7}$$

Problem 3. Without using a calculator (you don't need one!) reduce the following expressions, mod n. The first is done as an example:

$$2^{32} \bmod 63 \tag{8}$$
$$2^{47} \bmod 15 \tag{9}$$
$$2^{200} \bmod 17 \tag{10}$$
$$3^{10} \bmod 82 \tag{11}$$
$$20^{40} \bmod 21 \tag{12}$$

Solution:

$$\begin{aligned} & 2^{32} \bmod 63 \\ \equiv\ & (2^6)^5 2^2 \bmod 63 \\ \equiv\ & (64)^5 2^2 \bmod 63 \\ \equiv\ & (1)^5 4 \bmod 63 \\ \equiv\ & 4 \bmod 63 \end{aligned}$$