Tutorial 3 - Week 4

John O'Sullivan

Problem 1. Find the general solution for the following Diophantine equation:

$$258x + 147y = 369 \tag{1}$$

Problem 2. Find the multiplicative inverse of each non-zero element in $\mathbb{Z}/11$ (remember the alternative notation $\mathbb{Z}/11\mathbb{Z}$).

Problem 3. Show the following:

$$13 \equiv 1 \bmod 2 \tag{2}$$
$$-2 \equiv 1 \bmod 3 \tag{3}$$
$$-3 \equiv 30 \bmod 11 \tag{4}$$
$$111 \equiv -9 \bmod 40 \tag{5}$$

Problem 4. Construct a table for addition modulo 6.

Problem 5. Construct a table for multiplication modulo 6. Which residue classes have multiplicative inverses?

Problem 6. Show that if $a \in \mathbb{Z}$ is odd, then:

$$a^2 \equiv 1 \bmod 8 \tag{6}$$

Problem 7. Use the extended Euclidean algorithm to find the inverse of 19 mod 81.

Idea: We want x:

$$19x \equiv 1 \bmod 81$$

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

$$\begin{aligned} &19x \equiv 1 \bmod 81 \\ \iff\ &81 | (19x - 1) \\ \iff\ &81k = 19x - 1 \text{ for some } k \in \mathbb{Z} \\ \iff\ &1 = 19x - 81k \\ \iff\ &1 = 19x + 81y \text{ for } k = -y \end{aligned} \tag{7}$$

This is 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 x that results (we don't need y).

Problem 8. Use the extended Euclidean algorithm to find the inverse of 23 mod 121.