Week 1 Group Work

Objective: To explore concepts related to Euler's theorem and to foreshadow some ideas that will arrive in chapter 9.

1. Find the least nonnegative residue of 7^{2022} modulo 10.

2. Use Euler's theorem to find the inverse for 3 modulo 14. Hint: begin with the fact that $3^6 \equiv 1 \mod 14$.

3. Here, we will explore the equation $a^x \equiv 1 \mod m$ for three different values of m: one where m is prime, and two where m is composite.

   (a) Show that for every a not divisible by 11, $a^{10} \equiv 1 \mod 11$. (Yes, this is meant to be easy)

   (b) Find an a so that $a^x \not\equiv 1 \mod 11$ whenever $1 \leqslant x < 10$. We're later going to call every such a a <u>primitive root</u>.

   (c) Show that for every integer a with $(a, 10) = 1$, $a^4 \equiv 1 \mod 10$. (Yes, this is meant to be easy)

(d) Does there exist an integer a with $(a, 10) = 1$ and $a^x \not\equiv 1 \mod 10$ whenever $1 \leqslant x < 4$?

(e) Show that for every integer a with $(a, 8) = 1$, $a^4 \equiv 1 \mod 8$. (Yes, this is meant to be easy)

(f) Does there exist an integer a with $(a, 8) = 1$ so that $a^x \not\equiv 1 \mod 11$ whenever $1 \leqslant x < 4$?

4. Suppose that a and m are positive integers with $(a, m) = (a-1, m) = 1$. Show that

$$1 + a + a^2 + \cdots + a^{\varphi(m)-1} \equiv 0 \mod m$$

Hint: use the fact that $(1 + x + x^2 + \cdots + x^k)(x-1) = x^{k+1} - 1$