The structure of unit groups

1. Compute the following orders by hand. Show your work. Hint: the fact that \( \text{ord}_m(x) \mid \phi(m) \) may save you some work.
   
   (a) \( \text{ord}_{11}(3) \)
   
   (b) \( \text{ord}_{17}(2) \)
   
   (c) \( \text{ord}_{21}(10) \)
   
   (d) \( \text{ord}_{25}(9) \)

2. Fact: 2 is a primitive root modulo 701, and 695 \( \equiv 2^{80} \equiv 701 \). Use this to compute \( \text{ord}_{701}(695) \) by hand. Show your work.

3. Fact: 25 has order 323 modulo 647, and 104 \( \equiv 25^{17} \equiv 647 \). Use this to compute \( \text{ord}_{647}(104) \) by hand. Show your work.

4. Show that \( \mathbb{Z}/20\mathbb{Z} \) has no primitive roots.

5. Find a primitive root for \( (\mathbb{Z}/m\mathbb{Z})^* \) for each of the following values of \( m \): \( m = 10 \), \( m = 17 \), and \( m = 18 \).

6. Suppose \( \alpha, \beta \in (\mathbb{Z}/m\mathbb{Z})^* \) have relatively prime orders: i.e., \( (\text{ord}(\alpha), \text{ord}(\beta)) = 1 \). Prove that \( \text{ord}(\alpha \cdot \beta) = \text{ord}(\alpha) \cdot \text{ord}(\beta) \).

7. Given an explicit example of a modulus \( m \), and units \( \alpha, \beta \in (\mathbb{Z}/m\mathbb{Z})^* \) such that \( \text{ord}(\alpha \cdot \beta) \neq \text{ord}(\alpha) \cdot \text{ord}(\beta) \).

8. Let \( \alpha \in (\mathbb{Z}/m\mathbb{Z})^* \).
   
   (a) Prove that \( \text{ord}(\alpha) = \text{ord}(\alpha^{-1}) \).
   
   (b) Prove that \( \alpha \) is a primitive root if and only if \( \alpha^{-1} \) is a primitive root.

9. Let \( m > 2 \) be a modulus. Show that if there exists an \( \alpha \neq -1 \in (\mathbb{Z}/m\mathbb{Z})^* \) with \( \text{ord}(\alpha) = 2 \), then \( (\mathbb{Z}/m\mathbb{Z})^* \) does not have a primitive element. Hint: use the structure theorem for modular rings that contain primitive roots.

10. Suppose \( m = rs \) with \( (r, s) = 1 \) and \( r, s > 2 \).
    
    (a) Use the CRT to show that there are at least 4 distinct elements \( x \in \mathbb{Z}/m\mathbb{Z} \) satisfying \( x^2 = 1 \). Hint: look at solutions \( (x, y) \) to the system of congruences

        \[
        x^2 \equiv 1 \pmod{r} \quad \text{and} \quad y^2 \equiv 1 \pmod{s}.
        \]
(b) Using the previous problem, prove that \((\mathbb{Z}/m\mathbb{Z})^*\) has no primitive roots.

(c) Show that if \(m > 2\) is not of the form \(m = p^r\) or \(m = 2p^r\) with \(p\) an prime, then \((\mathbb{Z}/m\mathbb{Z})^*\) has no primitive roots. Hint: start by writing down what the prime factorization of \(m\) looks like in this case.

(Note: you can also show that if \(r > 1\), then the ring \(\mathbb{Z}/2^r\mathbb{Z}\) has exactly four elements \(x\) with \(x^2 = 1\). Thus if \(m = 2^r\) for \(r > 1\), then \((\mathbb{Z}/m\mathbb{Z})^*\) has no primitive roots. This narrows the possible moduli admitting primitive roots to moduli of the form \(m = 2\), \(m = p^r\) and \(m = 2p^r\).)