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.

   Note that $(\mathbb{Z}/10\mathbb{Z})^\times = \{1,3,7,9\}$, so $\varphi(10) = 4$. Since $(7,10) = 1$, Euler's theorem indicates that $7^4 \equiv 1 \mod 10$ and we conclude that

$$7^{2022} \equiv 7^{4\cdot 505+2} \equiv (7^4)^{505} \cdot 7^2 \equiv 1^{505} \cdot 49 \equiv 9 \mod 10$$

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

   We have that $(\mathbb{Z}/14\mathbb{Z})^\times = \{1,3,5,9,11,13\}$ and so $\varphi(14) = 6$. Hence, by Euler's theorem,

$$3 \cdot 3^5 = 3^6 \equiv 1 \mod 14$$

   Hence, 3^5 is the inverse of 3 modulo 14. We can find 3^5 through the following computations:

$$\begin{aligned} &3^2 \equiv 9 \mod 14 \\ &3^4 \equiv 9^2 \equiv 81 \equiv 11 \mod 14 \\ &3^5 \equiv 3 \cdot 3^4 \equiv 3 \cdot 11 \equiv 33 \equiv 5 \mod 14 \end{aligned}$$

   Therefore, 5 is an inverse of 3 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)

   Since $a \not\equiv 0 \mod 11$, Fermat's Little Theorem implies that $a^{10} \equiv 1 \mod 11$.

   (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 primitive root.

   Note that the powers of 2 modulo 11 are as follows:

x	1	2	3	4	5	6	7	8	9	10
2^x	2	4	8	5	10	9	7	3	6	1

   Since the smallest (nonzero) power of 2 yielding 1 is $2^{10} \equiv 1 \mod 11$, 2 is a primitive root modulo 11.

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

   As noted in problem 1, $\varphi(10) = 4$. Hence, if $(a, 10) = 1$, Euler's theorem guarantees that $a^4 \equiv 1 \mod 10$

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

Note that the powers of 3 modulo 10 are

x	1	2	3	4
3^x	3	9	7	1

Since the smallest positive power of 3 giving $3^x \equiv 1 \mod 10$ is $x = 4 = \varphi(10)$, 3 is a primitive root modulo 10.

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

$$\left(\mathbb{Z}/8\mathbb{Z}\right)^\times = \{1, 3, 5, 7\}$$

so $\varphi(8) = 4$. Hence, Euler's theorem guarantees that any integer a with $(a, 8) = 1$ satisfies $a^4 \equiv 1 \mod 8$.

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

Note that the powers of 1, 3, 5, and 7 modulo 8 are

x	1	2	3	4
1^x	1	1	1	1
3^x	3	1	3	1
5^x	5	1	5	1
7^x	7	1	7	1

Since $a^2 \equiv 1 \mod 8$ for every integer a with $(a, 8) = 1$, there are no primitive roots modulo 8.

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 $(1 + x + x^2 + \cdots + x^k)(x-1) = x^{k+1} - 1$

First observe that since $(a, m) = 1$, $a^{\varphi(m)} \equiv 1 \mod m$. Hence, we can conclude that

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

i.e. m divides $(1 + a + a^2 + \cdots + a^{\varphi(m)-1})(a-1)$. However, since m is relatively prime to $a-1$, we can conclude that m divides $1 + a + a^2 + \cdots + a^{\varphi(m)-1}$, i.e.

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