1. Find the number of incongruent roots modulo 13 of each of the following polynomials:
   Hint: All of these can be done without actually finding any roots of the polynomials.

   (a) $x^2 + 1$

   Since 13 is prime, this polynomial has two roots if -1 is a quadratic reside mod 13 and zero roots otherwise. Since $13 \equiv 1 \mod 4$, we know that -1 is a quadratic residue mod 13 and so there are two roots to $x^2 + 1$ mod 13. Alternatively, we could compute the Legendre symbol

   $$\left(\frac{12}{13}\right) = \left(\frac{4}{13}\right)\left(\frac{3}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$$

   to see that 12 is a quadratic residue mod 13.

   (b) $x^2 - 5$

   Again, there are two roots here if 5 is a quadratic residue mod 13 and zero roots otherwise. We compute the Legendre symbol

   $$\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$$

   and so $x^2 - 5$ has zero roots mod 13.

   (c) $x^6 - 1$

   Since 6 is a divisor of $12 = 13 - 1$ and since 13 is prime, theorem 9.7 indicates that there are exactly 6 roots of $x^6 - 1$ mod 13.

2. Find a complete set of incongruent primitive roots of 13.

We first claim that 2 is a primitive root mod 13. To see this, note the following powers of 2:

$$\begin{aligned} 2^1 &\equiv 2 \mod 13 \\ 2^2 &\equiv 4 \mod 13 \\ 2^3 &\equiv 8 \mod 13 \\ 2^4 &\equiv 3 \mod 13 \\ 2^6 &\equiv 12 \mod 13 \end{aligned}$$

Since the possible orders of 2 are 1,2,3,4,6, and 12 and the above computations indicate that the order of 2 is not 1,2,3,4, or 6, we see that the order of 2 must be 12 and hence, 2 is a primitive root mod 13. Corollary 9.4.1 now indicates that the other primitive roots have the form 2^x for $x \in (\mathbb{Z}/12\mathbb{Z})^\times$. Hence, the other primitive roots are:

$$\begin{aligned} 2^1 &\equiv 2 \mod 13 \\ 2^5 &\equiv 6 \mod 13 \\ 2^7 &\equiv 11 \mod 13 \\ 2^{11} &\equiv 5 \mod 13 \end{aligned}$$

3. Show that if p is prime and $p \equiv 1 \mod 4$, then there is an integer x with $x^2 \equiv -1 \mod p$.
Hint: What does $p \equiv 1 \mod 4$ say about there being elements of order 4 mod p?

Since $p \equiv 1 \mod 4$, we know that $4 \mid p-1$ and by theorem 9.8, there are two integers of order 4 modulo p. Let a be an integer of order 4 mod p. Then a^2 is a square root of 1 because $(a^2)^2 \equiv a^4 \equiv 1 \mod p$. Since p is prime, the only square roots of 1 are $\pm 1 \mod p$. However, $a^2 \not\equiv 1 \mod p$ because the order of a is 4. Hence, we must have $a^2 \equiv -1 \mod p$, so -1 is a quadratic residue mod p.

4. Suppose that n is a positive integer and a and b are integers relatively prime to n.

   (a) Show that if $ab \equiv 1 \mod n$, then for any positive integer r, $a^r \equiv 1 \mod n$ if and only if $b^r \equiv 1 \mod n$. Conclude that $\text{ord}_n(a) = \text{ord}_n(b)$.

   Suppose that $ab \equiv 1 \mod n$. First suppose that $a^r \equiv 1 \mod n$. Then we must have

   $$b^r \equiv a^r b^r \equiv (ab)^r \equiv 1^r \equiv 1 \mod n$$

   By a symmetric argument, if $b^r \equiv 1 \mod n$, then $a^r \equiv 1 \mod n$. Therefore, $a^r \equiv 1 \mod n$ if and only if $b^r \equiv 1 \mod n$. As a result, the order of a mod n (which is the minimal exponent x so that $a^x \equiv 1 \mod n$) must be equal to the order of b.

   (b) Now suppose that $\text{ord}_n(a)$ and $\text{ord}_n(b)$ are relatively prime. Show that

   $$\text{ord}_n(ab) = \text{ord}_n(a) \cdot \text{ord}_n(b)$$

   Observe first that

   $$(ab)^{\text{ord}_n(a)\,\text{ord}_n(b)} \equiv \left(a^{\text{ord}_n(a)}\right)^{\text{ord}_n(b)} \left(b^{\text{ord}_n(b)}\right)^{\text{ord}_n(a)} \equiv 1^{\text{ord}_n(b)} \cdot 1^{\text{ord}_n(a)} \equiv 1 \mod n$$

   Hence, the order of ab must divide $\text{ord}_n(a)\,\text{ord}_n(b)$. Since $\text{ord}_n(a)$ and $\text{ord}_n(b)$ are relatively prime, we can write $\text{ord}_n(ab) = d_1 d_2$ where $d_1 \mid \text{ord}_n(a)$ and $d_2 \mid \text{ord}_n(b)$. Since $\text{ord}_n(a)$ and $\text{ord}_n(b)$ are relatively prime, we find that d_1 is relatively prime to $\text{ord}_n(b)$ and d_2 is relatively prime to $\text{ord}_n(a)$. We can conclude that

   $$1 = (ab)^{\text{ord}_n(ab)} = (ab)^{d_1 d_2} \equiv a^{d_1 d_2} b^{d_1 d_2} \mod n$$

   By part (a), we know that the order of $a^{d_1 d_2}$ is equal to the order of $b^{d_1 d_2}$. But by theorem 9.4, we have

   $$\text{ord}_n(a^{d_1 d_2}) = \frac{\text{ord}_n(a)}{(d_1 d_2, \text{ord}_n(a))} = \frac{\text{ord}_n(a)}{d_1}$$
   $$\text{ord}_n(b^{d_1 d_2}) = \frac{\text{ord}_n(b)}{d_1 d_2, \text{ord}_n(b)} = \frac{\text{ord}_n(b)}{d_2}$$

   Hence, $\frac{\text{ord}_n(a)}{d_1} = \frac{\text{ord}_n(b)}{d_2}$ which implies that $d_2\,\text{ord}_n(a) = d_1\,\text{ord}_n(b)$. But since $\text{ord}_n(a)$ and $\text{ord}_n(b)$ are relatively prime, we must have $d_2 = \text{ord}_n(b)$ and $d_1 = \text{ord}_n(a)$. Therefore, $\text{ord}_n(ab) = d_1 d_2 = \text{ord}_n(a)\,\text{ord}_n(b)$.

5. Let p be prime and suppose that $p-1 = q_1^{e_1} \cdots q_g^{e_g}$ where $q_1, \ldots, q_g$ are distinct primes and $e_1, \ldots, e_g \geqslant 1$. In this problem, we construct a primitive root mod p

   (a) Show that there are integers $a_1, a_2, \ldots, a_g$ so that $\operatorname{ord}_p(a_i) = q_i^{e_i}$ for each $1 \leqslant i \leqslant g$

   Each $q_i^{e_i}$ is a divisor of $p-1$ and by theorem 9.8, there is an integer of order $q_i^{e_i}$.

   (b) Use the previous exercise to show that $a_1 a_2 \cdots a_g$ is a primitive root modulo p

   Since $q_1, \ldots, q_g$ are distinct primes, $q_1^{e_1}, \ldots, q_g^{e_g}$ are pairwise relatively prime. Hence, the orders of $a_1, \ldots, a_g$ are pairwise relatively prime and by part (b) of the previous problem,

   $$\operatorname{ord}_p(a_1 \cdots a_g) = \operatorname{ord}_p(a_1) \cdots \operatorname{ord}_p(a_g) = q_1^{e_1} \cdots q_g^{e_g} = p-1$$

   Since $a_1 \cdots a_g$ has order $p-1$, it must be a primitive root mod p.

(c) Use this procedure to find a primitive root mod 29.

Note that $29-1 = 28 = 2^2 \cdot 7$. So we first try to find elements of orders 4 and 7. Search around for a bit and you'll find that 12 has order 4 and 16 has order 7. So by the previous part, $12 \cdot 16 \equiv 18 \mod 29$ is a primitive root.