1. Solve the congruence \( x^2 \equiv 145 \pmod{256} \).

   [ANSWER: \( x \equiv 41, 87, 169, 215 \pmod{256} \).]

2. Let \( k \geq 3 \). Show that if \( a \) is odd, then the congruence \( a \equiv x^2 \pmod{2^k} \) is solvable if and only if \( a \equiv 1 \pmod{8} \), in which case there are four solutions mod \( 2^k \).

3. Let \( a \) be an integer not divisible by the odd prime \( p \) and suppose that the congruence \( x^2 \equiv a \pmod{p} \) is soluble. Prove that for each \( n \geq 2 \), the congruence \( x^2 \equiv a \pmod{p^n} \) has precisely two solutions.

4. Use CALC to prove that 5 is the least primitive root of the prime \( p = 10007 \).

5. (a) Given that 2 is a primitive root mod 61, solve the congruences
   \( i \) \( x^5 \equiv 32 \pmod{61} \); \( ii \) \( x^{35} \equiv 2^{35} \pmod{61} \).

   (Ans: (1) 2,18,40,55 (mod 61); (ii) 2,18,40,55 (mod 61).)

   (b) Also find the elements of order 4 mod 61. (Ans: 11, 50).

6. Let \( \Phi_p(x) = (x^p - 1)/(x - 1) \), where \( p \) is a prime. If \( q \) is a prime divisor of \( \Phi_p(n) \) for some \( n \in \mathbb{Z} \), prove that \( q = p \) or \( q \equiv 1 \pmod{p} \). Deduce that there are infinitely many primes of the form \( kp + 1 \).

7. Prove that 6 is the least primitive root modulo 109.

8. Let \( p \) be an odd prime and \( n \) a quadratic residue mod \( p \). Use the congruence \( n^{\frac{p-1}{2}} \equiv 1 \pmod{p} \) to deduce the following:

   (a) If \( p \equiv 3 \pmod{4} \), show that

   \[ \left( n^{\frac{1}{4}(p+1)} \right)^2 \equiv n \pmod{p}. \]

   (b) If \( p \equiv 5 \pmod{8} \), observe that \( n^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p} \) and show that

   \[ (i) \quad n^{(p-1)/4} \equiv 1 \pmod{p} \Rightarrow \left( n^{\frac{1}{8}(p+3)} \right)^2 \equiv n \pmod{p} \]
(ii) If \( b^2 \equiv -1 \pmod{p} \) show that
\[
n^{(p-1)/4} \equiv -1 \pmod{p} \Rightarrow \left( bn^{\frac{1}{8}(p+3)} \right)^2 \equiv n \pmod{p}.
\]

9. Let \( g \) be a Fibonacci primitive root \( \pmod{p} \). i.e. \( g \) is a primitive root \( \pmod{p} \) satisfying
\[
g^2 \equiv g + 1 \pmod{p}.
\]
(e.g. \( g = 8 \) if \( p = 11 \).)

Prove that
(a) \( g - 1 \) is also a primitive root \( \pmod{p} \);
(b) if \( p = 4k + 3 \), then
\[
(g - 1)^{2k+3} \equiv g - 2 \pmod{p}
\]
and deduce that \( g - 2 \) is also a primitive root \( \pmod{p} \).

10. Use the existence of a primitive root \( \pmod{p} \) to prove that
\[
1^n + 2^n + \ldots + (p - 1)^n \equiv \begin{cases} -1 \pmod{p} & \text{if } (p - 1) \mid n, \\ 0 \pmod{p} & \text{if } (p - 1) \nmid n. \end{cases}
\]

11. (*): If \( g_1, \ldots, g_{\phi(p-1)} \) are the primitive roots \( \pmod{p} \) in the range \( 1 < g \leq p - 1 \), prove that
\[
\sum_{i=1}^{\phi(p-1)} g_i \equiv \mu(p-1) \pmod{p}.
\]

12. Let \( r_1, \ldots, r_{\frac{p-1}{2}} \) be the quadratic residues in the range \( 1 \leq r \leq p - 1 \).

Show that
\[
r_1 r_2 \ldots r_{\frac{p-1}{2}} \equiv \begin{cases} 1 & \text{if } p \equiv -1 \pmod{4}, \\ -1 & \text{if } p \equiv 1 \pmod{4}. \end{cases}
\]

13. Use the existence of a primitive root \( \pmod{p} \) to prove that \(-3\) is a quadratic residue \( \pmod{p} \) if \( p \equiv 1 \pmod{3} \).

[Hint: Prove that an integer \( a \) of order 3 \( \pmod{p} \) exists and show that
\[
-3 \equiv (2a + 1)^2 \pmod{p}.]
\]
14. Use the existence of a primitive root (mod p) to prove that 5 is a quadratic residue mod p if \( p \equiv 1 \pmod{5} \).

[Hint: Prove that an integer \( a \) of order 5 (mod p) exists and show that if \( x = a + a^4 \), then
\[
x^2 + x - 1 \equiv 0 \pmod{p}
\]
and deduce that
\[
5 \equiv (2x + 1)^2 \pmod{p}.
\]
]

15. Let \( p \equiv 3 \pmod{4} \) be a prime.

(a) If \( p|\left(x^2 + y^2\right) \), \( x, y \in \mathbb{Z} \), prove that \( p|x \) and \( p|y \).

(b) Deduce that if \( n > 1 \) is the sum of two squares and \( p^a \| n \), where \( a \geq 1 \), then \( a \) is even.

16. Use Pocklington’s theorem and the fact that \( 2^{127} - 1 \) is prime, to prove that \( 180 \cdot (2^{127} - 1)^2 + 1 \) is a prime.

17. Use Proth’s theorem to prove that \( 81 \cdot 2^{89} + 1 \) and \( 3 \cdot 2^{209} + 1 \) are primes.