1. Find the smallest positive integer \( x \) such that \( x \cdot 4321 = 1 \mod 2007 \).

2. What is the value of \( 7^{2014} \mod 13 \)?

3. Given two positive integers \( a \) and \( n \), prove that \( a^{-1} \mod n \) exists if and only if \( \gcd(a, n) = 1 \).

4. Suppose that \( n = p \cdot q \) with \( p, q \) different primes. Suppose also that \( n = 4,386,607 \) and \( \phi(n) = 4,382,136 \). Find \( p, q \).

5. Find the smallest integer \( x > 0 \) such that \( 13 \cdot x = 4 \mod 99 \) and \( 7 \cdot x = 5 \mod 101 \) are satisfied simultaneously.

6. Given an integer \( n = p_1 \cdot p_2 \cdot p_3 \), where \( p_1, p_2, p_3 \) are prime numbers larger than 2, prove that there are exactly 8 integers \( x \in [1, n] \) satisfying \( x^2 = 1 \mod n \).

7. Let integer \( p \) be an odd prime number and \( p \) does not divide \( b \). Then prove the following statements

   (a) \( b \) is a quadratic residue of \( p \) if and only if \( b^{\frac{p-1}{2}} = 1 \mod p \).

   (b) \( b \) is a quadratic non-residue of \( p \) if and only if \( b^{\frac{p-1}{2}} = -1 \mod p \).

8. This question is about solving the quadratic congruence. Assume that \( p > 2 \) is a prime number and the positive integer \( a = x^2 \mod p \) for some unknown integer \( x \in [1, p-1] \). Prove the following statements

   (a) (5 points) There are only two solutions (i.e., two integers in \([1, p-1]\)) for equation \( a = x^2 \mod p \).

   (b) (5 points) If \( p = 3 \mod 4 \), then \( x_1 = a^{\frac{p+1}{4}} \mod p \), and \( x_2 = p - x_1 \) are the only two solutions.

   (c) (5 points) If \( p = 5 \mod 8 \) and \( a^{\frac{p-1}{4}} = 1 \mod p \), then \( x_1 = a^{\frac{p+3}{4}} \mod p \), and \( x_2 = p - x_1 \) are the only two solutions.

   (d) (5 points) If \( p = 5 \mod 8 \) and \( a^{\frac{p-1}{4}} = -1 \mod p \), then \( x_1 = 2a \cdot (4a)^{\frac{p-5}{4}} \mod p \), and \( x_2 = p - x_1 \) are the only two solutions.

Hint: (1) notice that \( a^{\frac{p-1}{2}} = 1 \mod p \); (2) notice that 2 is a quadratic non-residue modulo \( p \), if \( p = 5 \mod 8 \), i.e., there is no integer \( t \) such that \( t^2 = 2 \mod p \) if \( p = 5 \mod 8 \); (3) an integer \( b \) is a quadratic residue modulo \( p \) iff \( b^{\frac{p-1}{2}} = 1 \mod p \).

9. An affine cipher encrypts a plaintext \( x \in [0, 255] \) as \( y = k_1 x + k_2 \mod 256 \). A key \((k_1, k_2)\) with \( 0 \leq k_1, k_2 \leq 255 \) is valid for an affine cipher if the function \( k_1 x + k_2 \mod 256 \) is an one-to-one mapping. How many different valid keys for this affine cipher?

10. Write a code to compute \( a^b \mod n \), when given integer \( a > 0 \), \( b > 0 \), and \( n > 0 \).

   Here the input integers could be up to 1000 bits. So your code should be able to take care of big integers.

   Use your code to find what is the last digit of the following number \( a^b \mod n \), when \( a = 2^{123} - 1 \), \( b = 2^{999} - 1 \), and \( n = 2^{345} + 1 \).