Problem Set #7

Exercise 1: (⋆⋆) 4 points
Obtain three consecutive integers, each having a square factor.

Exercise 2: (⋆) 4 points
Show by induction that if \( n \) is a positive integer, then \( 4^n \equiv 1 + 3n \pmod{9} \).

Exercise 3: (⋆) 4 points
Determine which integers \( a \), where \( 1 \leq a \leq 14 \), have an inverse modulo 14, and find the inverse of each of these integers modulo 14.

Exercise 4: (⋆) 4 points
Show that if \( p \) is an odd prime and \( a \) is a positive integer not divisible by \( p \), then the congruence \( x^2 \equiv a \pmod{p} \) has either no solution or exactly two incongruent solutions.

Exercise 5: (⋆) 4 points

1. Let \( a \) be an integer, \( u, v, n, m \) natural numbers. We assume that \( m \) and \( n \) are relatively prime, that \( a^u \equiv 1 \pmod{m} \) and that \( a^v \equiv 1 \pmod{n} \). Show that \( a^{\text{lcm}(u,v)} \equiv 1 \pmod{mn} \).

2. Let \( a \) be an integer relatively prime to 63. Show that \( a^{36} \equiv 1 \pmod{63} \).

3. Using question (a), show that we can improve the result in (b), by proving that for any integer relatively prime to 63, \( a^6 \equiv 1 \pmod{63} \).

---

\(^1\) (⋆) = easy, (⋆⋆) = medium, (⋆⋆⋆) = challenge