Solutions to Discrete Math Quiz on Modular Arithmetic

1. Compute \((n \mod d)\) for the following \(n\) and \(d\).
   - \((29 \mod 3) = 2\) because \(29 = 9 \cdot 3 + 2\)
   - \((29 \mod 5) = 4\) because \(29 = 5 \cdot 5 + 4\)
   - \((29 \mod 7) = 1\) because \(29 = 4 \cdot 7 + 1\)
   - \((29^2 \mod 3) = 1\) because \((29^2 \mod 3) = ((29 \mod 3)^2 \mod 3) = 2^2 \mod 3 = (4 \mod 3) = 1\)
   - \((29^2 \mod 5) = 1\) because \((29^2 \mod 5) = ((29 \mod 5)^2 \mod 5) = 4^2 \mod 5 = (16 \mod 5) = 1\)
   - \((29^2 \mod 7) = 1\) because \((29^2 \mod 7) = ((29 \mod 7)^2 \mod 7) = 1^2 \mod 7 = (1 \mod 7) = 1\)

2. Find, if it exists, \((n^{-1} \mod d)\) (inverse of \(n\) modulo \(d\)) for the following \(n\) and \(d\).
   - \((3^{-1} \mod 5) = 2\) because \(3 \cdot 2 = 6 = 1 \cdot 5 + 1\)
   - \((4^{-1} \mod 5) = 4\) because \(4 \cdot 4 = 16 = 3 \cdot 5 + 1\)
   - \((3^{-1} \mod 4) = 3\) because \(3 \cdot 3 = 9 = 2 \cdot 4 + 1\)
   - \((2^{-1} \mod 4)\) does not exist because \((n \cdot 2 \mod 4)\) is either 0 or 2 for any integer \(n\).

3. Compute \(\varphi(n)\) for the following \(n\).
   - \(\varphi(11) = 11 - 1 = 10\)
   - \(\varphi(9) = \varphi(3^2) = 3^2 - 3^1 = 9 - 3 = 6\)
   - \(\varphi(10) = \varphi(5) \varphi(2) = (5 - 1)(2 - 1) = 4 \cdot 1 = 4\)
   - \(\varphi(36) = \varphi(3^2 \cdot 2^2) = \varphi(3^2) \varphi(2^2) = (3^2 - 3^1)(2^2 - 2^1) = 6 \cdot 2 = 12\)

4. Compute \((n^k \mod d)\) for the following \(n, k,\) and \(d\).
   - \((2^{20} \mod 3) = ((2^2)^{10} \mod 3) = (4^{10} \mod 3) = ((4 \mod 3)^{10} \mod 3) = (1^{10} \mod 3) = 1\)
   - \((11^{12} \mod 13) = 1\) by Fermat’s little Theorem because 13 is a prime number that is not a divisor of 11.
   - \((1001^2 \mod 6) = 1\) by Euler’s Theorem because \(\gcd(1001, 6) = 1\) and \(\varphi(6) = \varphi(3) \varphi(2) = (3 - 1)(2 - 1) = 2 \cdot 1 = 2\)

5. Find the greatest common divisors for the following set of numbers.
   - \(\gcd(16, 27) = 1\) because the only divisors of 16 are powers of 2 while the only divisors of 27 are powers of 3.
   - \(\gcd(14, 21, 35, 42) = 7\) because 7 divides these four numbers, 14 does not divide the other three numbers, and any number between 7 and 14 does not divide 14.

6. Find the least common multiply in the first part and answer the question in the second part.
   - \(\text{lcm}(14, 21, 35) = 7 \cdot 2 \cdot 3 \cdot 5 = 210\) because 7 divides 14, 21, and 35, and the other prime factors of these numbers are 2, 3, and 5.
   - \(\text{lcm}(4, 6) + 2 = 12 + 2 = 14\) is the smallest integer \(n > 2\) for which \((n \mod 4) = (n \mod 6) = 2\).