Solutions to Discrete Math Quiz on Number Theory

1. Find the prime factors of the following two numbers:
   (a) $252 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7 = 2^2 \cdot 3^2 \cdot 7$
   (b) 103 is prime and therefore its only prime factor is 103.

2. Compute $(n \bmod d)$ for the following n and d.
   - $(101 \bmod 3) = 2$ because $101 = 33 \cdot 3 + 2$
   - $(101 \bmod 5) = 1$ because $101 = 20 \cdot 5 + 1$
   - $(101 \bmod 7) = 3$ because $101 = 14 \cdot 7 + 3$
   - $(101^2 \bmod 3) = 1$ because $(101^2 \bmod 3) = ((101 \bmod 3)^2 \bmod 3) = (2^2 \bmod 3) = (4 \bmod 3) = 1$
   - $(101^2 \bmod 5) = 1$ because $(101^2 \bmod 5) = ((101 \bmod 5)^2 \bmod 5) = (1^2 \bmod 5) = (1 \bmod 5) = 1$
   - $(101^2 \bmod 7) = 2$ because $(101^2 \bmod 7) = ((101 \bmod 7)^2 \bmod 7) = (3^2 \bmod 7) = (9 \bmod 7) = 2$

3. Find, if it exists, $(n^{-1} \bmod d)$ (inverse of n modulo d) for the following n and d.
   - $(3^{-1} \bmod 7) = 5$ because $3 \cdot 5 = 15 = 2 \cdot 7 + 1$
   - $(4^{-1} \bmod 7) = 2$ because $4 \cdot 2 = 8 = 1 \cdot 7 + 1$
   - $(5^{-1} \bmod 6) = 5$ because $5 \cdot 5 = 25 = 4 \cdot 6 + 1$
   - $(3^{-1} \bmod 6)$ does not exist because $(n \cdot 3 \bmod 6)$ is either 0 or 3 for any integer n.

4. Compute $\varphi(n)$ for the following n.
   - $\varphi(17) = 17 - 1 = 16$
   - $\varphi(25) = \varphi(5^2) = 5^2 - 5^1 = 25 - 5 = 20$
   - $\varphi(35) = \varphi(5 \cdot 7) = \varphi(5)\varphi(7) = (5-1)(7-1) = 4 \cdot 6 = 24$
   - $\varphi(54) = \varphi(2 \cdot 27) = \varphi(2 \cdot 3^3) = \varphi(2)\varphi(3^3) = (2-1)(3^3 - 3^2) = 1 \cdot (27 - 9) = 18$

5. Compute $(n^k \bmod d)$ for the following n, k, and d.
   - $(2^{200} \bmod 3) = ((2^2)^{100} \bmod 3) = (4^{100} \bmod 3) = ((4 \bmod 3)^{100} \bmod 3) = (1^{100} \bmod 3) = 1$
   - $(100^{16} \bmod 17) = 1$ by Fermat's little Theorem because 17 is prime that is not a divisor of 100.
   - $(1001^8 \bmod 15) = 1$ by Euler's Theorem because $\gcd(1001, 15) = 1$ and
   $$\varphi(15) = \varphi(3 \cdot 5) = \varphi(3)\varphi(5) = (3-1)(5-1) = 2 \cdot 4 = 8$$

6. Find the greatest common divisors for the following set of numbers.
   - $\gcd(64, 81) = 1$ because the only divisors of 64 are powers of 2 while the only divisors of 81 are powers of 3.
   - $\gcd(18, 27, 45, 63) = 9$ because 9 divides these four numbers, 18 does not divide the other three numbers, and any number between 9 and 18 does not divide 18.

7. Find the least common multiply in the first part and answer the question in the second part.
   - $\operatorname{lcm}(18, 27, 45) = 9 \cdot 2 \cdot 3 \cdot 5 = 270$ because 9 divides 18, 27, and 45, and the other prime factors of these numbers are 2, 3, and 5.
   - $\operatorname{lcm}(6, 8) + 3 = 24 + 3 = 27$ is the smallest integer $n > 3$ for which $(n \bmod 6) = (n \bmod 8) = 3$.

8. Compute $10! \bmod 11$.

   $10! = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 10 \cdot (9 \cdot 5) \cdot (8 \cdot 7) \cdot (6 \cdot 2) \cdot (4 \cdot 3) = 10 \cdot 45 \cdot 56 \cdot 12 \cdot 12$

   $(10! \bmod 11) = (10 \bmod 11) \cdot (45 \bmod 11) \cdot (56 \bmod 11) \cdot (12 \bmod 11) \cdot (12 \bmod 11) = 10 \cdot 1 \cdot 1 \cdot 1 \cdot 1 = 10$