Solutions to Discrete Math Quiz on Number Theory

1. Find the prime factors of the following two numbers:
   (a) $264 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 11 = 2^3 \cdot 3 \cdot 11$
   (b) 101 is prime and therefore its only prime factor is 101.

2. Compute $(n \bmod d)$ for the following n and d.
   - $(92 \bmod 3) = 2$ because $92 = 30 \cdot 3 + 2$
   - $(92 \bmod 5) = 2$ because $92 = 18 \cdot 5 + 2$
   - $(92 \bmod 7) = 1$ because $92 = 13 \cdot 7 + 1$
   - $(92^2 \bmod 3) = 1$ because $(92^2 \bmod 3) = ((92 \bmod 3)^2 \bmod 3) = (2^2 \bmod 3) = (4 \bmod 3) = 1$
   - $(92^2 \bmod 5) = 4$ because $(92^2 \bmod 5) = ((92 \bmod 5)^2 \bmod 5) = (2^2 \bmod 5) = (4 \bmod 5) = 4$
   - $(92^2 \bmod 7) = 1$ because $(92^2 \bmod 7) = ((92 \bmod 7)^2 \bmod 7) = (1^2 \bmod 7) = (1 \bmod 7) = 1$

3. Find, if it exists, $(n^{-1} \bmod d)$ (inverse of n modulo d) for the following n and d.
   - $(2^{-1} \bmod 7) = 4$ because $2 \cdot 4 = 8 = 1 \cdot 7 + 1$
   - $(5^{-1} \bmod 7) = 3$ because $5 \cdot 3 = 15 = 2 \cdot 7 + 1$
   - $(3^{-1} \bmod 8) = 3$ because $3 \cdot 3 = 9 = 1 \cdot 8 + 1$
   - $(4^{-1} \bmod 8)$ does not exist because $(n \cdot 4 \bmod 8)$ is either 0 or 4 for any integer n.

4. Compute $\varphi(n)$ for the following n.
   - $\varphi(19) = 19 - 1 = 18$
   - $\varphi(49) = \varphi(7^2) = 7^2 - 7^1 = 49 - 7 = 42$
   - $\varphi(21) = \varphi(3 \cdot 7) = \varphi(3)\varphi(7) = (3-1)(7-1) = 2 \cdot 6 = 12$
   - $\varphi(48) = \varphi(16 \cdot 3) = \varphi(2^4 \cdot 3) = \varphi(2^4)\varphi(3) = (2^4 - 2^3)(3-1) = (16-8) \cdot 2 = 8 \cdot 2 = 16$

5. Compute $(n^k \bmod d)$ for the following n, k, and d.
   - $(2^{100} \bmod 3) = ((2^2)^{50} \bmod 3) = (4^{50} \bmod 3) = ((4 \bmod 3)^{50} \bmod 3) = (1^{50} \bmod 3) = 1$
   - $(100^{18} \bmod 19) = 1$ by Fermat's little Theorem because 19 is prime that is not a divisor of 100.
   - $(901^8 \bmod 15) = 1$ by Euler's Theorem because $\gcd(901, 15) = 1$ 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.
   - $\gcd(32, 25) = 1$ because the only divisors of 32 are powers of 2 while the only divisors of 25 are powers of 5.
   - $\gcd(22, 33, 55, 77) = 11$ because 11 divides these four numbers, 22 does not divide the other three numbers, and any number between 11 and 22 does not divide 22.

7. Find the least common multiply in the first part and answer the question in the second part.
   - $\operatorname{lcm}(22, 33, 55) = 11 \cdot 2 \cdot 3 \cdot 5 = 330$ because 11 divides 22, 33, and 55, and the other prime factors of these numbers are 2, 3, and 5.
   - $\operatorname{lcm}(6, 9) + 3 = 18 + 3 = 21$ is the smallest integer $n > 3$ for which $(n \bmod 6) = (n \bmod 9) = 3$.

8. Compute $10! \bmod 13$.

   $10! = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = (10 \cdot 4) \cdot (9 \cdot 3) \cdot (8 \cdot 5) \cdot (7 \cdot 2) \cdot 6 = 40 \cdot 27 \cdot 40 \cdot 14 \cdot 6$

   $(10! \bmod 13) = (40 \bmod 13) \cdot (27 \bmod 13) \cdot (40 \bmod 13) \cdot (14 \bmod 13) \cdot (6 \bmod 13) = 1 \cdot 1 \cdot 1 \cdot 1 \cdot 6 = 6$