Quiz Questions: Number Theory

1. The multiplicative inverse of 3 modulo 7 is?
   a. -1
   b. -2
   c. -3
   d. -4

   Explanation: -2*3 modulo 7 = -6 modulo 7 = 1 modulo 7

2. If a, b are positive integers such that $a > b$ then
   a. $a > lcm(a, b) > b$
   b. $a > b > lcm(a, b)$
   c. $lcm(a, b) \geq a > b$
   d. none of the mentioned

   Explanation: $lcm(a, b)$ is always larger equal a, b. $lcm(a, b) = a > b$ if $b|a$, and $lcm(a, b) > a > b$ otherwise.

3. A number greater than 32 would require a minimum of how may bits in binary representation?
   a. 5
   b. 6
   c. 4
   d. 10

   Explanation: The binary representation of $32 = 2^5 = (100000)_2$, which has 6 bits. Any larger number has at least as many bits.

4. Suppose that *a* and *b* are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer *c* with $0 \leq c \leq 12$ such that $c \equiv 2a + 3b \pmod{13}$.
   a. 9
   b. 35
   c. 8
   d. 12

   Explanation: 2*4 mod 13 = 8 mod 13, 3*9 mod 13 = 27 mod 13 = 1 mod 13, (8 + 1) mod 13 = 9 mod 13

5. $LCM(a, b)$ is equal to
   a. $\frac{ab}{GCD(a,b)}$
   b. $\frac{a+b}{GCD(a,b)}$
   c. $\frac{GCD(a,b)}{ab}$
   d. none of the mentioned

   Explanation: ab = $\gcd(a, b) * lcm(a, b)$, therefore $lcm(a, b) = \frac{ab}{\gcd(a,b)}$

6. $(1010111011)_2$ to its octal expansion.
   a. 1273
   b. 1752
   c. 1276

d. 1656

Explanation: we can write the number as $(001\ 010\ 111\ 011)_2$ where $(011)_2 = 3_8, (111)_2 = (7)_8, (010)_2 = (2)_8, (001)_2 = (1)_8$

7. What is the prime factorization of 10!?
   a. $2^5 \cdot 3^6 \cdot 5^2 \cdot 7$
   b. $2^6 \cdot 3^4 \cdot 5^2 \cdot 7^2$
   c. $2^7 \cdot 3^3 \cdot 5^2 \cdot 7^2$
   d. $2^8 \cdot 3^4 \cdot 5^2 \cdot 7$

Explanation: Factors of 2 : 2 has 1 factor 2, 4 has 2 factors 2, 6 has 1 factor 2, 8 has 3 factors 2, 10 has 1 factor 2, Total :8 factors of 2. 4 factors of 3 from 3,6,9, 2 factors of 5 from 5, 10, 1 factor 7 from 7

8. Which of the following is correct?
   a. $6\ mod\ 13 = 19$
   b. $6 \equiv 13\ (mod\ 19)$
   c. $6\ mod\ 13 = 19\ mod\ 13$
   d. 6 (mod 13) ≡ 19 (mod 13)

Explanation:

$6\ mod\ 13 = 6 \neq 19$
$6 \equiv 13\ (mod\ 19)$ is not true
$6\ mod\ 13 = 6 = 19\ mod\ 13$
6 (mod 13) ≡ 19 (mod 13) this notation is not defined