Indian Institute of Technology Kharagpur
Department of Computer Science and Engineering

CS60094 Computational Number Theory **Spring 2026**

Quiz 1 **9th of February 2026, 9:35 AM – 9:55 AM** **Marks: 10 × 1.5 = 15**

Please write your answers in the space provided. Do not mark in the question ittself.

---

1. Suppose we use Toom-4 method to multiply two n-digit integers in base B. How many multiplications of $n/4$-digit integers are required?

   A. 7

   B. 10

   C. 16

   D. 8

2. Let a, b, c, x, y be arbitrary integers. Which one of the following is incorrect?

   A. For $p \in \mathbb{P}$, if $p|a_1a_2 \cdots a_n$, then $p|a_i$ for some $i \in [n]$.

   B. If $a|bc$ and $\gcd(a, b) = d$, then $a|dc$.

   C. If $a|b$ and $b|c$, then $a|(bx + cy)$.

   D. If $a|b$, $b|c$, then $a = \pm c$.

3. What is the intermediate result after 3rd iteration of square-and-multiply method for modular multiplication while computing $6^{13} \mod 23$? Assume the bits of the exponent are processed in left-to-right order.

   A. 9

   B. 6

   C. 21

   D. 12

4. Consider the polynomial $f(x) = 2x^3 - 7x^2 + 189$. We want to find roots of $f(x) \equiv 0 \pmod{675}$. Roots of $f(x)$ modulo 5^2 are

   A. 0,8,13

   B. 18

   C. 0,9,17,18

   D. 13

5. Which one of the following linear congruences is solvable?

   A. $14x_1 + 10x_2 \equiv 7 \pmod{28}$

   B. $4x \equiv 7 \pmod{11}$

   C. $7x \equiv 4 \pmod{14}$

   D. $21x \equiv 17 \pmod{60}$

6. Let $p \in \mathbb{P}$ and $a, b \in \mathbb{Z}$. Which of the following is correct?

A. if $a^{p^r} + b^{p^r} \equiv a + b \pmod{p}$ then $a \equiv b \pmod{p}$

B. $(p-1)! \equiv 1 \pmod{p}$

C. $(a+b)^p \equiv 0 \pmod{p}$

D. $\binom{p}{k} \equiv 0 \pmod{p}$ **for all** $k = 1, 2, \ldots, p-1$

7. Let p be a prime of the form $4k+1$, let $a, b \in \mathbb{Z}^+$ with a odd and $a^2 + b^2 = p$. Then $\left(\frac{a}{p}\right)$ is

A. 1

B. $\left(\frac{b}{p}\right)$

C. -1

D. 0

8. Let $m \in \mathbb{N}$, $h = \mathrm{ord}_m a$, $k = \mathrm{ord}_m b$ and let $l \in \mathbb{Z}$. Identify which of the following statements is incorrect.

A. $\mathrm{ord}_m a^l = h/\gcd(h, l)$

B. If $a^l \equiv 1 \pmod{m}$**, then** $l|h$**.**

C. If $\gcd(h, k) = 1$, then $\mathrm{ord}_m(ab) = hk$

D. $\mathrm{ord}_m(ab) | \mathrm{lcm}(a, b)$

9. Let $p \in \mathbb{P} \setminus \{2\}$ and let $a \in \mathbb{Z}_p^*$ be a quadratic residue modulo p. Which of the following assertions is true?

A. If $p \equiv 5 \pmod{8}$ and $a^{(p-1)/4} \equiv 1 \pmod{p}$, then $a^{(p-5)/8} \pmod{p}$ is a modular squareroot of a

B. If $p \equiv 3 \pmod{4}$, then $a^{(p-3)/4} \pmod{p}$ is a modular squareroot of a.

C. If $p \equiv 5 \pmod{8}$ **and** $a^{(p-1)/4} \equiv 1 \pmod{p}$**, then** $a^{(p+3)/8} \pmod{p}$ **is a modular squareroot of** a

D. If $p \equiv 5 \pmod{8}$ and $a^{(p-1)/4} \equiv -1 \pmod{p}$, then $a^{(p+3)/8} \pmod{p}$ is a modular squareroot of a

10. Running time of the algorithm for finding solutions to t simultaneous linear congruences using Chinese Remainder Theorem (with pairwise coprime modulii $m_1, m_2, \ldots, m_t$) is

A. $O(t \log^2 \prod_i m_i)$

B. $O(t^2 \log^2(\max_i m_i))$

C. $O(t \log(\max_i m_i))$

D. $O(t^2 \log \prod_i m_i)$