Ahmedabad University
School of Arts and Sciences

Elementary Number Theory & Cryptography (MAT215) - Part B

Mid-Semester Examination, Date: 27 September 2025

Timing: up to 04:00 PM | Monsoon 2025 | Maximum points: 10

Instructions

- You are allowed to bring only the following items with you: a calculator, stationery, and one A4-sized sheet of paper with anything written on it, double-sided (this doesn't mean two sheets, it means only one sheet, and it has to be A4 size; anything is not permissible).
- Write clear proofs for full credit.
- You can do any combination of questions totaling 10 points. Anything above that will not be evaluated.
- Malpractice (including, but not limited to, bringing unauthorized things to the exam room, talking with others, prompting, and using electronic devices) will result in an immediate NP grade.

Best wishes

Questions

The quantities written in small letters, such as a, b, n, etc. will always be integers, unless otherwise mentioned.

Question 1 to 4 are worth 2 points each. Full details of the proofs are required.

1. Prove that, if p is an odd prime then
   (a) $1^{p-1} + 2^{p-1} + \cdots (p-1)^{p-1} \equiv -1 \pmod{p}$, and
   (b) $1^p + 2^p + \cdots (p-1)^p \equiv 0 \pmod{p}$.
2. Show that 31 divides $4 \cdot (29!) + 5!$.
3. Solve the linear congruence: $17x \equiv 9 \pmod{256}$ for x.
4. Give a proof of the infinitude of primes by assuming that there are only finitely many primes, say $p_1, p_2, \ldots, p_n$, and using the following integer to arrive at a contradiction:

$$N = p_2 p_3 \cdots p_n + p_1 p_3 \cdots p_n + \cdots + p_1 p_2 \cdots p_{n-1}.$$

Question 5 and 6 are worth 4 points each. Full details of the proofs are required.

5. Prove the following divisibility test for 7: an integer $n = a_1 a_2 \dots a_k$ is divisible by 7 iff 7 divides $a_1 a_2 \dots a_{k-1} - 2a_k$.

   For instance, if $n = 353535$, then we see that $35353 - 2 \cdot 5 = 35343$, now $3534 - 2 \cdot 3 = 3528$ and $352 - 2 \cdot 8 = 336$, and finally $33 - 2 \cdot 6 = 21$ which is divisible by 7, so $7|328$ which implies $7|3528$ and so on, culminating in $7|353535$.

   (Hint: Try to mimic the proof of the divisibility test for 9 shown in the lectures.)

6. Find the last two digits of 9^{9^9}.