Department of Mathematics, University of Wisconsin-Madison

Math 567 — Midterm Exam 1 — Spring 2025

NAME :   (as it appears on Canvas)

EMAIL: @wisc.edu

PROFESSOR: Mikhail Ivanov

INSTRUCTIONS:

Time: **90 minutes**

- This exam contains 10 questions some with multiple parts, 7 pages (including the cover) for the total of 50 points. Read the problems carefully and budget your time wisely.

- **NO CALCULATORS** or other electronic devices are to be used. Turn off your phone so as to not disturb others.

- Please present your solutions in a clear manner. Cross out any writing that you do not wish to be graded.

- Justify your steps.

- If you use an additional page for a particular problem, be sure to **CLEARLY** indicate this on the problem's page so I know to look further.

- Please write your name on every page.

- You can safely assume that all unknown quantities in this exam, e.g. a, b, c, n, x, y, are always the integers.

Question:	1	2	3	4	5	6	7	8	9	10	Total
Points:	5	5	5	5	5	5	5	5	5	5	50
Score:											

1. (5 points) Solve the system of congruences

$$\begin{cases} x \equiv 11 \pmod 2 \\ x \equiv 22 \pmod 3 \\ x \equiv 33 \pmod 5 \end{cases}$$

2. (5 points) Find the greatest common divisor of numbers 81 and 30 and linear representation of it.

3. (5 points) Find last 2 digits of 7^{2025}.

4. (5 points) Find all prime numbers p such that $p^2 + 4$ and $p^2 + 6$ are prime.

5. (5 points) Solve congruence
$$16x \equiv 4 \pmod{22}.$$

6. (5 points) Verify that $4 \cdot 29! + 5!$ is divisible by 31.

7. (5 points) Alice and Bob establish Diffie–Hellman key exchange with $p = 29$ and $g = 2$. Alice generate number 5 and receive number 7 from Bob. Which number Alice should send to Bob and what is their joint secret key?

8. (5 points) Solve the system of congruences

$$\begin{cases} x \equiv 20 \pmod{30} \\ x \equiv 24 \pmod{48} \end{cases}$$

9. (5 points) Find all positive integers n such that $\varphi(n) = 2$.

10. (5 points) We consider the group $(\mathbb{Z}/53\mathbb{Z})^*$. What are the possible element orders? How many elements exist for each order?

SCRATCH PAPER - DO NOT REMOVE FROM YOUR EXAM.
SCRATCH WORK WILL NOT BE GRADED