Department of Mathematics, University of Wisconsin-Madison

Math 567 — Final Exam — Spring 2025

NAME : (as it appears on Canvas)

EMAIL: @wisc.edu

PROFESSOR: Mikhail Ivanov

INSTRUCTIONS:

Time: **120 minutes**

- This exam contains 9 questions some with multiple parts, 9 pages (including the cover) for the total of 60 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	Total
Points:	5	5	5	5	5	5	8	5	17	60
Score:										

1. (5 points) Solve the system of congruences

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

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

3. (5 points) How many zeroes are there at the end of the decimal representation of 2025!?

4. (5 points) Express number $(-\sqrt{5})$ as a continuous fraction.

5. (5 points) Find all primes p such that $p^4 - 606$ is prime.

6. (5 points) Which numbers of the form 6^k, $k \in \mathbb{Z}$ are congruence numbers?

7. Given an elliptic curve E over $\mathbb{Z}_{29}$ and the base point $P = (8, 10)$:

$$E: \quad y^2 = x^3 + 4x + 20 \bmod 29.$$

The order of this curve is known to be $|E| = 37$. Furthermore, an additional point $Q = 15 \cdot P = (14, 23)$ on this curve is given. **How to determine** the result of the following point additions/multiplications by using as few group operations as possible, i.e., make smart use of the known point Q?

(a) (2 points) $16 \cdot P$

(b) (2 points) $38 \cdot P$

(c) (2 points) $14 \cdot P + 4 \cdot Q$

(d) (2 points) $4 \cdot P + 9 \cdot Q$

8. (5 points) Let k and r be integers, $k > 1$, $r > 1$. Show that there is a prime number whose representation in base r has exactly k digits.

9. Consider equation $y^2 = x^3 - 4$.

   (a) (5 points) Find all integer solutions with $|x| \leq 6$ by brute force.

(b) (6 points) Find all integer solutions with odd x.

(c) (6 points) Find all integer solutions with even x.

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