Department of Mathematics, University of Wisconsin-Madison

Math 567 — Midterm Exam 1 — Solutions — 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

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

Solution: We are using CRT:

$$\begin{cases} x \equiv 11 \pmod 2 \\ x \equiv 22 \pmod 3 \\ x \equiv 33 \pmod 5 \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 1 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \pmod 6 \\ x \equiv 3 \pmod 5 \end{cases}$$

$$\Leftrightarrow \begin{cases} x \equiv 1, 7, 13, 19, 25 \pmod{30} \\ x \equiv 3, 8, 13, 18, 23, 28 \pmod{30} \end{cases} \Leftrightarrow \boxed{x \equiv 13 \pmod{30}}$$

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

Solution:

$$81 = 30 \cdot 2 + 21$$
$$30 = 21 \cdot 1 + 9$$
$$21 = 9 \cdot 2 + \boxed{3}$$
$$9 = 3 \cdot 3 + 0$$

$3 = 21 - 9 \cdot 2 = 21 - (30 - 21) \cdot 2 = 21 \cdot 3 - 30 \cdot 2 = (81 - 30 \cdot 2) \cdot 3 - 30 \cdot 2 = \boxed{81 \cdot 3 - 30 \cdot 8}$.

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

Solution: $7^4 \equiv 49^2 \equiv 2401 \equiv 1 \pmod{100}$, so

$$7^{2025} \equiv 7^1 \equiv \boxed{07} \pmod{100}.$$

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

Solution: If $p \equiv \pm 1 \pmod 5$, then $p^2 + 4 \equiv 0 \pmod 5$, so it is divisible by 5 and $p^2 + 4 > 5$, so not prime.

If $p \equiv \pm 2 \pmod 5$, then $p^2 + 6 \equiv 0 \pmod 5$, so it is divisible by 5 and $p^2 + 6 > 5$, so not prime.

If $p \equiv 0 \pmod 5$, then $p = 5$, $p^2 + 4 = 29$, $p^2 + 6 = 31$, so $\boxed{p = 5}$ is the answer.

5. (5 points) Solve congruence

$$16x \equiv 4 \pmod{22}.$$

Solution:

$16x \equiv 4 \pmod{22} \Leftrightarrow 8x \equiv 2 \pmod{11} \Leftrightarrow 4x \equiv 1 \pmod{11} \Leftrightarrow 12x \equiv \boxed{x \equiv 3 \pmod{11}}$

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

Solution: By Wilson Theorem $30! \equiv -1 \pmod{31}$, so $29! \equiv (-1) \cdot (30)^{-1} \equiv 1 \pmod{31}$. Now

$$4 \cdot 29! + 5! \equiv 4 \cdot 1 + 120 = 124 \equiv 0 \pmod{31}.$$

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?

Solution: Alice sends to bob $g^{k_A} = 2^5 \equiv \boxed{3} \pmod{29}$. Their shared secret key $(2^{k_B})^{k_A} \equiv 7^5 \equiv 7 \cdot 49 \cdot 49 \equiv 7 \cdot (-9) \cdot (-9) \equiv 7 \cdot 81 \equiv 7 \cdot (-6) \equiv \boxed{16}$.

8. (5 points) Solve the system of congruences

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

Solution: First equation gives $x \equiv 20 \equiv 2 \pmod{3}$, but second equation gives $x \equiv 24 \equiv 0 \pmod{3}$. Contradiction, so $\boxed{\text{no solutions}}$.

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

Solution: Suppose $n = p_1^{a_1} \dots p_k^{a_k}$ with $a_i > 0$. We have $\varphi(n) = p_1^{a_1-1}(p_1-1) \dots p_k^{a_k-1}(p_k-1)$, so all $p_i < 5$ and $a_i \leq 2$. It gives as the list of candidates: 1, 2, 3, 4, 6, 9, 12, 18, 36 (2 and 3 in powers no more than 2). test all of them and find answer $\boxed{3,\ 4,\ 6}$.

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?

Solution: 53 is prime, so $(\mathbb{Z}/53\mathbb{Z})^* \cong \mathbb{Z}/52\mathbb{Z}$. Cyclic group has elements with orders any divisors of 52, i.e. 1, 2, 4, 13, 26, 52. Number of elements of such order d is $\varphi(d)$ i.e.

1	2	4	13	26	52	total
1	1	2	12	12	24	52

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