Department of Mathematics, University of Wisconsin-Madison

Math 567 — Final Exam — Solutions — 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

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

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

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?

Solution: Alice sends to bob $g^{k_A} = 2^7 \equiv 32 \cdot 4 \equiv \boxed{12} \pmod{29}$. Their shared secret key $(2^{k_B})^{k_A} \equiv 5^7 \equiv 5 \cdot 25 \cdot 25 \cdot 25 \equiv 5 \cdot (-4) \cdot (-4) \cdot (-4) \equiv -20 \cdot 16 \equiv -320 \equiv \boxed{28}$.

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

Solution: We know that $v_2(2025!) \geq v_5(2025!)$, so we number of zeroes is equal to the $v_5(2025!)$.

$$v_5(2025!) = \left\lfloor \frac{2025}{5} \right\rfloor + \left\lfloor \frac{2025}{5^2} \right\rfloor + \left\lfloor \frac{2025}{5^3} \right\rfloor + \left\lfloor \frac{2025}{5^4} \right\rfloor + \left\lfloor \frac{2025}{5^5} \right\rfloor + \ldots = 405+80+16+3+0 = \boxed{505}.$$

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

Solution:

$$-\sqrt{5} = -3 + (3 - \sqrt{5}) = -3 + \frac{1}{\frac{3+\sqrt{5}}{4}}$$

$$\frac{3+\sqrt{5}}{4} = 1 + \frac{\sqrt{5}-1}{4} = 1 + \frac{1}{\sqrt{5}+1}$$

$$\sqrt{5}+1 = 3 + (\sqrt{5}-2) = 3 + \frac{1}{\sqrt{5}+2}$$

$$\sqrt{5}+2 = 4 + (\sqrt{5}-2) = 4 + \frac{1}{\sqrt{5}+2}$$

We have cycle!

$$-\sqrt{5} = [-3, 1, 3, \overline{4}].$$

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

Solution: If $p \equiv \pm 1 \pm 2 \pmod 5$, then $p^4 - 606 \equiv 1 - 606 \equiv 0 \pmod 5$, so it is divisible by 5 and $p^4 - 606 > 5 \Leftrightarrow p > 5$, so not prime.

If $p = 2, 3$, then $p^5 - 606 < 0$, so not prime.

If $p = 5$, then $p^4 - 606 = 19$, so $\boxed{p = 5}$ is the answer.

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

Solution: We know that $n = 6$ is the congruence number. (It is area of triangle 3, 4, 5).

We know that $n = 1$ is not a congruence number. (it is equivalent to $x^4 + y^4 = z^4$.)

Now suppose n is a congruence number for triangle a, b, c, then $6^{2k}n$, $k \in \mathbb{Z}$,

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) $16 \cdot P$

Solution:

$$16 \cdot P = Q + P.$$

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

Solution:

$$38 \cdot P = 37 \cdot P + P = \mathcal{O} + P = P.$$

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

Solution:

$$14 \cdot P + 4 \cdot Q = 74 \cdot P = 2 \cdot 37 \cdot P = \mathcal{O}.$$

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

Solution:

$$4 \cdot P + 9 \cdot Q = (4 + 135) \cdot P = 139 \cdot P = 28 \cdot P = 2 \cdot (Q - P).$$

2 operations!

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.

Solution: Bertrand's postulate (Chebyshev Theorem) tell us that there is a prime number p such that

$$r^{k-1} < p < 2r^{k-1} \leq r^k.$$

Such prime will have exactly k r-digits.

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

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

Solution: $x < 2 \Rightarrow x^3 - 4 < 0$,
$x = 2 \Rightarrow x^3 - 4 = 4 \Rightarrow \boxed{(2, -2),\ (2, 2)}$,
$x = 3 \Rightarrow x^3 - 4 = 23$,
$x = 4 \Rightarrow x^3 - 4 = 60$,
$x = 5 \Rightarrow x^3 - 4 = 121 \Rightarrow \boxed{(5, -11),\ (5, 11)}$,
$x = 6 \Rightarrow x^3 - 4 = 212$,

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

Solution: Odd x give odd y. Now

$$x^3 = y^2 + 4 = (y + 2i)(y - 2i).$$

In the $\mathbb{Z}[i]$. $\gcd(y + 2i, y - 2i) = \gcd(y + 2i, 2i)$. $4i = -i(1 + i)^4$, $y + i \equiv y - 1 \equiv 1 \pmod{1 + i}$, so $\gcd(y + 2i, y - 2i) = 1$. Product of 2 coprime numbers is the cube, so each of them is cube times unit. All units on $\mathbb{Z}[i]$ are cubes themselves, so we have just cube. Integer x is odd, so cube is coprime with $1 + i$, i.e. a and b have different parity.

$$y + 2i = (a + bi)^3 = (a^3 - 3ab^2) + (3a^2b - b^3)i,$$

so $2 = b(3a^2 - b^2)$, so $b = \pm 1, \pm 2$, which, with parity, gives us $y + 2i = (\pm 1 - 2i)^3 = \pm 11 + 2i$, $\boxed{(5, \pm 11)}$

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

Solution: Even x give even y. Suppose $x = 2n$, $y = 2m$. Now

$$8n^3 = 4m^2 + 4 \Leftrightarrow 2n^3 = m^2 + 1$$

so m is odd and

$$2n^3 = (m+i)(m-i).$$

In the $\mathbb{Z}[i]$. $\gcd(m+i, m-i) = \gcd(m+2i, 2i)$. $2i = (1+i)^2$, $m+i \equiv m-1 \equiv 0 \pmod{1+i}$, so $\gcd(y+2i, y-2i) = 1+i$ (clearly $m+i$ is not divisible by 2). Now

$$n^3 = \Big(\frac{m+i}{1+i}\Big)\Big(\frac{m-i}{1-i}\Big).$$

Product of 2 coprime numbers is the cube, so each of them is cube times unit. All units on $\mathbb{Z}[i]$ are cubes themselves, so we have just cube. x is odd, so cube is coprime with $1+i$, i.e. a and b have different parity.

$$m + i = (1+i)(a+bi)^3 = ((a^3 - 3ab^2) + (3a^2b - b^3)i)(1+i),$$

so $1 = a^3 - 3ab^2 + 3a^2b - b^3 = (a-b)(a^2 + ab + b^2 + 3ab)$, so

$$\begin{cases} a - b = 1 \\ a^2 + 4ab + b^2 = 1 \end{cases} \quad \text{or} \quad \begin{cases} a - b = 1 \\ a^2 + 4ab + b^2 = 1 \end{cases}$$

which gives only tqo solutions $(a, b) \in \{(1, 0), (0, -1)\}$, means $m+i = (1+i)1^3 = 1+i$, or $m + i = (1+i)(-i)^3 = -1 + i$ $\boxed{(2, \pm 2)}$

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