Department of Mathematics, University of Wisconsin-Madison

Math 567 — Midterm Exam 2 — Solutions — Spring 2025

NAME : (as it appears on Canvas)

EMAIL: @wisc.edu

PROFESSOR: Mikhail Ivanov

INSTRUCTIONS:

Time: **90 minutes**

- This exam contains 9 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	Total
Points:	5	5	5	5	5	5	5	5	10	50
Score:										

1. (5 points) Find the Legendre symbol $\left(\frac{15}{101}\right)$.

Solution:

$$\left(\frac{15}{101}\right) = \left(\frac{101}{15}\right) = \left(\frac{11}{15}\right) = -\left(\frac{15}{11}\right) - \left(\frac{4}{11}\right) = -1$$

2. (5 points) Express $-\frac{19}{51}$ as the finite simple continuous fraction.

Solution:

$$\frac{-19}{51} = -1 + \frac{32}{51} = -1 + \cfrac{1}{1 + \cfrac{19}{32}} = -1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{13}{19}}} = -1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{6}{13}}}}$$

$$= -1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{6}}}}} = [-1, 1, 1, 1, 2, 6].$$

3. (5 points) Show that for every prime p there is $n \in \mathbb{Z}$ such that $(n^2-2)(n^2-3)(n^2-6) \equiv 0 \pmod{p}$.

Solution: For $p = 2, 3$ we can take $n = 0$. If $p > 3$ we have Legendre symbols $\left(\frac{2}{p}\right)$, $\left(\frac{3}{p}\right)$, $\left(\frac{6}{p}\right)$. If one symbol is equal to 1, then corresponding term of our product can be 0 modulo p. But all three cannot be equal to -1, because $\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{6}{p}\right)$.

4. (5 points) Evaluate the infinite simple continuous fraction $[0, \overline{1, 2, 1}]$.

Solution: Let $\alpha = [\overline{1, 2, 1}] = [1, 2, 1, \alpha] = \frac{4\alpha+3}{3\alpha+2} \Rightarrow 3\alpha^2 + 2\alpha = 4\alpha + 3$, $\alpha > 0$, so $\alpha = \frac{1+\sqrt{10}}{3}$. Now answer is $[0, \alpha] = \frac{1}{\alpha} = \frac{\sqrt{10}-1}{3}$.

5. (5 points) Find all integer solutions for equation

$$x^2 + y^2 = 2z^2.$$

Solution: $(0,0,0)$ is a only solution with $z = 0$, now we can divide by z^2. Let's consider $a = \frac{x}{z}$, $b = \frac{y}{z}$, $a^2 + b^2 = 2$, $a, b \in \mathbb{Q}$. Now we have one rational solution $(1,1)$ any rational line will intersect circle in second rational point and line through $(1,1)$ and rational point will have rational coefficients. So, for $t \in \mathbb{Q}$,

$$\begin{cases} b = t(a-1) + 1 \\ a^2 + b^2 = 2 \end{cases}$$

will have 2 solutions: $(1,1)$ and $\left(\dfrac{t^2 - 2t - 1}{t^2 + 1}, \dfrac{-t^2 - 2t + 1}{t^2 + 1}\right)$, Second formula generate all points including $(1,1)$ (for $t = -1$, tangent line), excluding $(1,-1)$ (for $t = \infty$). Now we need to recover x, y and z. Let $t = \frac{p}{q}$, $\gcd(p,q) = 1$.

$$(a,b) = \left(\frac{x}{z}, \frac{y}{z}\right) = \left(\frac{p^2 - 2pq - q^2}{p^2 + q^2}, \frac{-p^2 - 2pq + q^2}{p^2 + q^2}\right)$$

Numerators and denominator are relatively prime, so

$$x = s(p^2 - 2pq - q^2), \quad y = s(-p^2 - 2pq + q^2), \quad z = s(p^2 + q^2).$$

for some integers p, q, s.

Solution: Suppose $\gcd(x,y,z) = 1$. We have $4z^2 = 2x^2 + 2y^2 = (x+y)^2 + (x-y)^2$, so $(x+y)$, $x-y$, $2z$ are Pythagorean triple. $\gcd(x+y, x-y, 2z) = 2$, so $\frac{x+y}{2}$, $\frac{x-y}{2}$, z is primitive. We don't know which one os even, but we can change the sign of y, if we needed.

$$\frac{x+y}{2} = t^2 - s^2, \quad \frac{x-y}{2} = 2ts, \quad z = t^2 + s^2$$

so, adding $\pm$ for y and adding $a = \gcd(x,y,z)$ we have

$$x = a(t^2 + 2ts - s^2), \quad y = \pm a(t^2 - 2ts - s^2), z = a(t^2 + s^2).$$

6. (5 points) Find all integer solutions for equation

$$x^2 + y^2 = 3z^2.$$

Solution: Consider equation modulo 3. LHS$\in 0, 1, 2$, so LHS$\equiv 0 \pmod 3$, so $x \equiv y \equiv 0 \pmod 3$, so $z \equiv 0 \pmod 3$ and $x_1 = x/3$, $y_1 = y/3$, $z_1 = z/3$, $x_1^2 + y_1^2 = 3z_1^2$ for smaller numbers. For non-zero numbers we cannot continue to do it unlimited amount of times, so $x = y = z = 0$.

First Name: ______________________ Last Name: ______________________

7. (5 points) Suppose that N is a nonzero integer and d is non-square positive integer. Prove that if $x^2 - dy^2 = N$ has one integer solution, then it has infinitely many.

Solution: We know that equation $x^2 - dy^2 = 1$ has infinitely many questions, let's call them $a_k + b_k\sqrt{N}$. If there is one pair $x + y\sqrt{N}$ such that $x^2 - dy^2 = N$, then any number of the form $(x + y\sqrt{N})(a_k + b_k\sqrt{N})$ will be a solution too.

8. (5 points) Let α be irrational number with partial convergents $\frac{p_n}{q_n}$. Use the relation

$$\alpha = \frac{r_{n+1}p_n + p_{n-1}}{r_{n+1}q_n + q_{n-1}}$$

to show that

$$\left|\alpha - \frac{p_n}{q_n}\right| < \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right|.$$

Solution:

$$\alpha r_{n+1}q_n + \alpha q_{n-1} = r_{n+1}p_n + p_{n-1}$$

$$r_{n+1}(\alpha q_n - p_n) = p_{n-1} - \alpha q_{n-1}$$

$$r_{n+1}q_n\left|\alpha - \frac{p_n}{q_n}\right| = q_{n-1}\left|\frac{p_{n-1}}{q_{n-1}} - \alpha\right|$$

Now $r_{n+1} > 1$ nd $q_n > q_{n-1}$, so

$$\left|\alpha - \frac{p_n}{q_n}\right| < \left|\frac{p_{n-1}}{q_{n-1}} - \alpha\right|$$

9. Let E be the elliptic curve

$$y^2 = x^3 + 2x + 4 \pmod 5.$$

(a) (5 points) Write down all the points of $E(\mathbb{Z}/5\mathbb{Z})$.

Solution: $E(\mathbb{Z}/5\mathbb{Z}) = \{(0, \pm 2), (2, \pm 1), (-1, \pm 1), \mathcal{O}\}$, $|E(\mathbb{Z}/5\mathbb{Z})| = 7$.

(b) (5 points) Suppose $P = (0, 2)$. Find coordinates of $6P$.

Solution: $6P = -P = (0, -2) = (0, 3)$.

First Name: ____________ Last Name: ____________

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