MATH 4573: FINAL EXAM

INSTRUCTOR: TYLER GENAO

Print name: _____

OSU name.# : _____

Before you start this exam, please read the following:

- There are **five questions** on this exam, and **two bonus questions.**
  - For the first four problems, **you must show the correct work to receive credit.** Partial credit may be given for these.
  - The fifth problem is a series of True/False questions. You are not required to show your work for them, as no partial credit will be given.
  - You must show work for bonus problem $B1$ to receive credit for it. Note that there is less opportunity for partial credit on this problem.
- This is a closed notes exam. All personal electronic devices, including smart watches and cell phones, must be silenced and stored in a bag. **Basic calculators will be provided by the instructor.**
- There is a statements page and scratch paper at the back of this exam; feel free to remove them. If you need more paper, please let me know. Scratch paper must be submitted with the exam; **however, work on scratch paper will not be graded unless you ask me to do so in your normal answer space.**
- There are a **total of** 152 **possible points** on this exam. However, this exam will be weighted out of 100, and any earned points over 100 will count as extra credit.

Problem:	**1**	**2**	**3**	**4**	**5**	**B1**	**B2**	**Total**
Points:	30	30	25	20	25	20 (/0)	2 (/0)	100

I will be academically honest in all my academic work and will not tolerate academic dishonesty of others.

Signed: _____ Date: _____

Date: May 1, 2026.

Problem 1. In the following problem, you can assume that each starting modulus is prime.

a) (6 points each) Determine with proof whether each of the following congruences **has a solution.**
   i) $x^2 \equiv 22 \pmod{101}$.
   ii) $x^2 - 37 \equiv 0 \pmod{73}$.
   iii) $x^3 \equiv 3 \pmod{19}$.

b) (6 points each) Determine with proof the **number of solutions** to each of the following congruences.
   i) $x^7 \equiv 2 \pmod{29}$.
   ii) $x^4 \equiv 6 \pmod{997}$.

Problem 2.

a) (6 points each) Determine with proof whether each of the following lines have integral points. If they do, then give a complete description of them.

i) $L_1 : 12x + 30y = 39$.

ii) $L_2 : 5x + 20y = 15$.

iii) $L_3 : 8x + (n^2 - 1)y = 28$, where $n \in \mathbb{Z}$ is odd.

b) (6 points each) Consider the superelliptic curve

$$C : y^5 = x^4 - 2x^2 + 4.$$

i) Prove that C has no singular points in $\mathbb{R}^2$.

ii) Determine whether C has points at infinity; if it does, then calculate them.

Problem 3.

a) (10 points) Prove that the hyperbola

$$C : 12x^2 - 7y^2 = 3$$

has no integral points. (*Hint:* use modular arithmetic.)

b) (10 points) Prove that the hyperbola in part a) has infinitely many rational points. (*Hint:* find at least one rational point.)

c) (5 points) Explain why for any $a, b, c \in \mathbb{Q}$ with $ab > 0$, the conic

$$C_{a,b,c} : ax^2 + by^2 = c$$

always has finitely many integral points.

Problem 4. Consider the elliptic curve

$$E : y^2 + xy = x^3 + x^2 - 2x.$$

Some points on E include $P := (-2, 2), Q := (-1, -1), R := (8, 20)$ and $S := (0, 0)$.

a) (10 points) Prove that $P \oplus Q = R$.

b) (10 points) Prove that $2S = O$, where $O := [0 : 1 : 0]$.

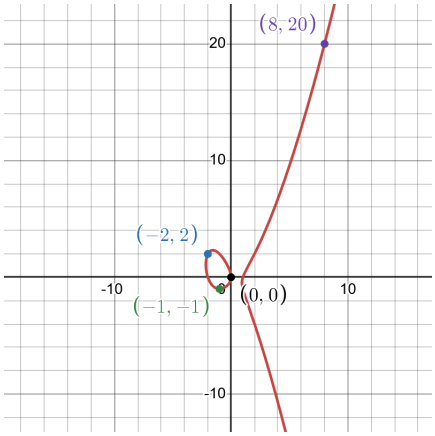

FIGURE 1. The elliptic curve $E : y^2 + xy = x^3 + x^2 - 2x$.

Problem 5. (5 points each) Determine whether the following statements are True or False.

*****You do not need to show your work for this problem.*****

a) The ring $\mathbb{Z}/57\mathbb{Z}$ is a field.

b) If g is a primitive root modulo a prime p, then it is a primitive root mod p^k for all $k \geq 2$.

c) The congruence $x^7 \equiv 46 \pmod{23}$ has a solution.

d) The triple $(531, 708, 885)$ is a primitive Pythagorean triple.

e) The point at infinity $[1 : 1 : 0] \in \mathbb{P}^2(\mathbb{Q})$ lies on every vertical line.

Bonus Problem B1. Only attempt this problem if you have attempted all previous problems, and have double-checked your work. There will be less partial credit here, and it can be trickier than the previous questions!

Consider the elliptic curve

$$E : y^2 = x^3 - 4x^2 + 5x.$$

a) (**extra credit,** 10 points) Explain why the three points $P := (0,0), Q := \left(\frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2}\right)$ and $R := \left(\frac{1-\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right)$ on E add together to $O := [0:1:0]$.

b) (**extra credit,** 10 points) Determine with proof all 2-torsion points in $E(\mathbb{C})$.

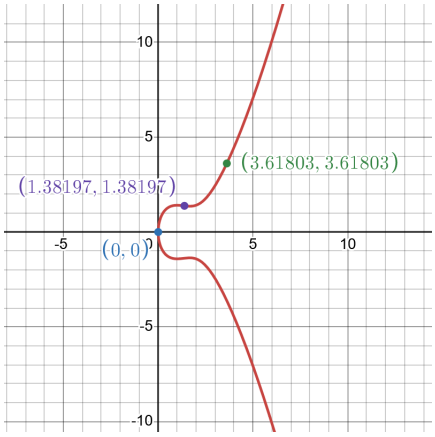

FIGURE 2. The elliptic curve $E : y^2 = x^3 - 4x^2 + 5x$.

Bonus Problem B2. (**extra credit,** 2 points) What was your favorite topic that you learned in this course?

Statements

Here are some statements for reference.

1. **(Formula for adding two points on an elliptic curve in general Weierstrass form):** Consider an elliptic curve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$. Then for two points $P = (x_1, y_1), Q = (x_2, y_2) \in E(\mathbb{Q})$ which are not collinear, if m denotes the slope of the line between P and Q, then one has

$$P \oplus Q = (x_3, -a_1x_3 - a_3 - y_3)$$

where

$$(x_3, y_3) = P * Q = (m^2 + a_1m - a_2 - x_1 - x_2, m(x_3 - x_1) + y_1).$$

2. **(Euler's Criterion for n'th Power Residues)** Let a, n and p be integers with p prime and $p \nmid a$. Then the congruence

$$x^n \equiv a \pmod{p}$$

has a solution if and only if

$$a^{\frac{p-1}{\gcd(n,p-1)}} \equiv 1 \pmod{p}.$$

In this case, it has exactly $\gcd(n, p-1)$ solutions.

3. **(The Linear Diophantine Theorem)** Fix integers a, b and c where $a \neq 0$ or $b \neq 0$. Then the line

$$L : ax + by = c$$

has an integral solution if and only if $\gcd(a, b) \mid c$. When this happens, the line has infinitely many integral points. Furthermore, if $(x_1, y_1) \in \mathbb{Z}^2$ is any solution, then all other integral solutions are of the form

$$(x_2, y_2) = \left(x_1 + k \cdot \frac{b}{\gcd(a,b)}, y_1 - k \cdot \frac{a}{\gcd(a,b)}\right)$$

where $k \in \mathbb{Z}$.

4. **(Quadratic Reciprocity and its supplemental laws for the Jacobi symbol)** Let m and n be odd, positive, coprime integers. Then one has

$$\begin{aligned}\left(\frac{m}{n}\right) &= \left(\frac{n}{m}\right) \cdot (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} \\ &= \begin{cases} \left(\frac{n}{m}\right) & \text{if } m \equiv 1 \pmod 4 \textbf{ or } n \equiv 1 \pmod 4 \\ -\left(\frac{n}{m}\right) & \text{if } m \equiv 3 \pmod 4 \textbf{ and } n \equiv 3 \pmod 4. \end{cases}\end{aligned}$$

Furthermore, one has

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} = \begin{cases} 1 & \text{if } m \equiv 1 \pmod 4 \\ -1 & \text{if } m \equiv -1 \pmod 4 \end{cases}$$

and

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} = \begin{cases} 1 & \text{if } m \equiv \pm 1 \pmod 8 \\ -1 & \text{if } m \equiv \pm 3 \pmod 8. \end{cases}$$

5. **(Definition of a torsion point)** For an elliptic curve $E/\mathbb{Q}$, a point $P \in E(\mathbb{C})$ is a *torsion point* if P has finite order in $E(\mathbb{C})$, i.e., if there exists $n \in \mathbb{Z}^+$ with $nP = O$. In this case, we say that P is an *n-torsion point.*

6. **(Structure theorem for the Mordell-Weil group of an elliptic curve)** For an elliptic curve $E/\mathbb{Q}$, one has

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})[\text{tors}]$$

for some integer $r := r(E, \mathbb{Q}) \geq 0$ and some finite abelian group $E(\mathbb{Q})[\text{tors}]$.

-Scratch paper-