MATH 4573: FINAL EXAM

INSTRUCTOR: TYLER GENAO

Print name: _____

OSU name.# : _____

Before you start the exam, please read this:

- There are **six questions** on this exam.
  - For the first four, **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.
- **This exam will be weighted out of** 100 **points on Carmen.** In particular, if you receive more than 100 points on this exam, it will count as extra credit.
- This is a closed notes exam. All personal electronic devices, including smart watches and cell phones, must be silenced and stored in a bag. Calculators are not permitted, and aren't necessary.
- There is a blank page after each proof-based problem, for more space for your answer. There is also scratch paper at the back of the midterm. If you need more, 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.**

Problem:	**1**	**2**	**3**	**4**	**5**	**6**	**Total**
Points:	30	25	24	24	25	2	130
Score:							

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

Signed: _____ Date: _____

-Page left intentionally blank-

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

a) **(6 points each)** Determine with proof whether each of the following congruences **has a solution.**
   i) $x^2 \equiv -5 \pmod{229}$.
   ii) $x^2 - 10 \equiv 0 \pmod{127}$.
   iii) $x^5 \equiv 3 \pmod{17}$.

b) **(6 points each)** Determine with proof the **number of solutions** to each of the following congruences.
   i) $x^4 \equiv -1 \pmod{1019}$.
   ii) $x^{15} \equiv 8 \pmod{73}$.

-This is extra space to work on-

Problem 2.

a) **(10 points)** Prove that for each integer $n > 0$, one has

$$\mu(n) \cdot \mu(n+1) \cdot \mu(n+2) \cdot \mu(n+3) = 0,$$

where $\mu\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ denotes the Möbius function.

b) **(15 points)** Show that

$$\sum_{d|n} |\mu(d)| = 2^{\omega(n)},$$

where $\omega\colon \mathbb{Z}^+ \to \mathbb{Z}_{\geq 0}$ counts the number of distinct positive primes dividing n.

-This is extra space to work on-

Problem 3.

a) **(6 points each)** Determine whether each of the following linear equations have integral solutions. If they do, give a complete description of them.

i) $14x - 7y = 22$.

ii) $(n^2 - 1)x + 8y = 16$, where $n \geq 1$ is an odd integer.
(*Hint:* what do we know about n^2 modulo 8?)

b) **(12 points)** Show that the Diophantine equation

$$x^2 + 2y^2 = 8z + 5$$

has no integral solutions $(x, y, z) \in \mathbb{Z}^3$.

(*Hint:* Assume that such a solution exists, and determine the parity of x. Then reduce the original equation modulo 8.)

-This is extra space to work on-

Problem 4. Consider the elliptic curve

$$E_{/\mathbb{Q}} : y^2 = x^3 + 9.$$

Some of its points include $P_1 := (-2, -1)$, $P_2 := (0, 3)$ and $P_3 := (6, -15)$.

a) **(12 points)** Prove that

$$P_1 \oplus P_2 = P_3.$$

b) **(12 points)** Prove that

$$3P_2 = O,$$

where $3P_2 := P_2 \oplus P_2 \oplus P_2$ and $O := [0 : 1 : 0]$ is the point at infinity on E.

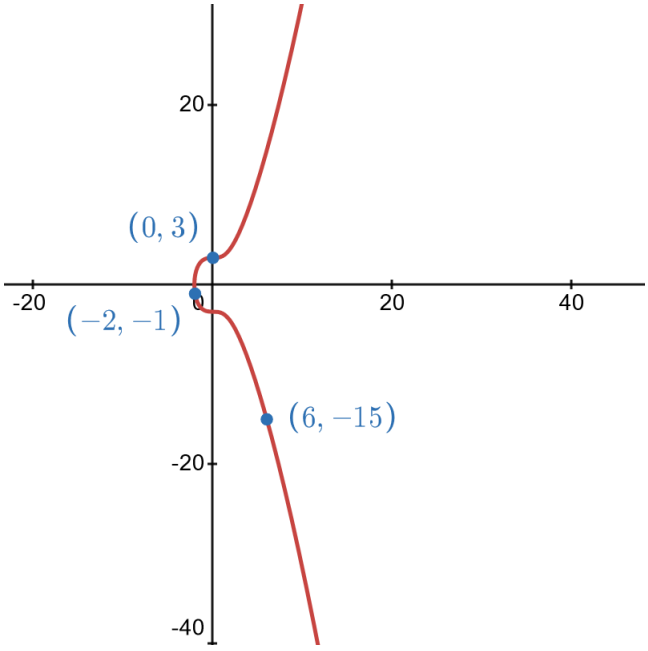

FIGURE 1. The elliptic curve $E : y^2 = x^3 + 9$.

-This is extra space to work on-

Problem 5. (5 points each) Say whether the following statements are True or False. **You do not need to show your work for this problem.**

a) 2 is a primitive root modulo 81.

b) $(6, 8, 10)$ is a primitive Pythagorean triple.

c) Since $\left(\frac{2}{15}\right) = 1$, the congruence $x^2 \equiv 2 \pmod{15}$ has a solution.

d) The ellipse $C_1 : 2x^2 + 3y^2 = 5$ has infinitely many rational solutions.

e) The plane curve $C_2 : x^{12} = 2 + 13y$ has integral solutions.

Problem 6. (2 points) What is your favorite topic that we covered in this class?

-This is an extra page for scratchwork-

-This is an extra page for scratchwork-

Statements

Here are some statements for reference that will be included on the final exam.

1. **(Quadratic reciprocity):** if p, q are distinct odd primes, then

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

2. **(Euler's criterion for n'th power residues):** for $n, a, p \in \mathbb{Z}^+$ with p prime: if $\gcd(p, a) = 1$, 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 which case it has $\gcd(n, p-1)$ solutions.
3. **(Formula for point sum):** let $E_{/\mathbb{Q}} : y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve (in "normal Weierstrass form"). Then given two points $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\mathbb{Q})$, if $x_1 \neq x_2$ then one has

$$P_1 \oplus P_2 := (x_3, y_3) = (m^2 - a - x_1 - x_2, -y_1 - m(x_3 - x_1)),$$

where m is the secant slope between P_1 and P_2.