MATH 4573: PRACTICE FINAL EXAM PROBLEMS

INSTRUCTOR: TYLER GENAO

Here is a list of topics we have covered in class or on the homework, after Lagrange's Theorem from §2.11 and up to some of §5.8 on elliptic curves. Any of these topics can appear on the final exam. Note that this list is not necessarily exhaustive.

- §2.11: Groups, Rings and Fields.
  - The definition of rings, their unit groups, and fields.
  - The definition of the direct products of groups and rings.
  - CRT for $\mathbb{Z}/m\mathbb{Z}$ and $(\mathbb{Z}/m\mathbb{Z})^\times$.
- §2.8: Primitive Roots and Power Residues.
  - The definition of a primitive root modulo m.
  - Lifting primitive roots mod p^2 to p^k for $k \geq 3$, including when one can lift a primitive root mod p to mod p^2.
  - The definition of an n'th power residue.
  - Euler's Criterion for n'th power residues modulo p.
    - Formula for solutions to $x^n - a$ modulo p. Involves the Linear Congruence Theorem!

  §3.1: Quadratic Residues.
  - Euler's Criterion when $n = 2$.
  - The definition of quadratic residues and non-residues modulo p.
  - The Legendre symbol and its basic properties.
- §3.2: Quadratic Reciprocity.
  - The statement of Quadratic Reciprocity.
  - The supplemental laws of Quadratic Reciprocity for computing $\left(\frac{2}{p}\right)$ and $\left(\frac{-1}{p}\right)$.
- §3.3: The Jacobi Symbol.
  - The definition of the Jacobi symbol, and its basic properties.
  - Quadratic Reciprocity and its supplemental laws for the Jacobi symbol.
- §5.0: A Dictionary for Diophantine Geometry.
  - The definition of a Diophantine equation.
  - The definition of integral, rational, real and complex solutions to a Diophantine equation.
  - The definition of a plane curve (over $\mathbb{R}$).
  - The technique of proving integral points do not exist on a Diophantine plane curve, via reducing the equation modulo suitably chosen integers.
- §5.1: The Equation $ax + by = c$.
  - The Linear Diophantine Theorem.

        - The associated algorithm to parametrize all integral solutions to a Diophantine line, using its "GCD line."
- §5.3: Pythagorean Triples.
  - The definition of Pythagorean triples, and primitive Pythagorean triples.
    - I will not ask you to memorize the characterization for positive primitive Pythagorean triples.
- §5.6: Rational Points on Curves.
  - The algorithm for parametrizing rational points on (nonsingular) conics.
  - The chord and tangent method for producing rational points on cubic curves.
  - The definition of (non)singular points, the projective plane, homogenization, points at infinity, and irreducibility.
    - The basic concepts of intersection multiplicity we covered in class (e.g., the tangent line to a curve at a nonsingular point has intersection multiplicity ≥ 2).
- §5.7: Elliptic Curves.
  - The definition of an elliptic curve.
  - The definition of a flex point.
  - The group law on an elliptic curve.
    - The formula for adding points on an elliptic curve in general Weierstrass form can speed up calculations.
  - The Collinearity Theorem for elliptic curves with a flex point identity.
- §5.8: Torsion, Rank and Reduction on Elliptic Curves.
  - The Structure Theorem for the Mordell-Weil group of an elliptic curve.
  - The definition of a torsion point on an elliptic curve, and an n-torsion point.
  - The definition of the rank of an elliptic curve.

Problem 1. Determine the number of solutions to the following congruences. You can assume that each modulus is prime. (For extra practice, determine the solutions to each part, if they exist.)

a) $x^{12} \equiv 16 \pmod{17}$.
b) $x^4 \equiv 1 \pmod{163}$.
c) $x^{20} \equiv 2 \pmod{29}$.
d) $x^2 \equiv 3 \pmod{997}$, where 997 is prime.
e) $x^2 \equiv -5 \pmod{1009}$, where 1009 is prime.

Problem 2. Parametrize all integral solutions to the following lines, if they exist.

a) $L_1 : 12x + 50y = 1$.

b) $L_2 : 15x + 7y = 111$.

Problem 3. This exercise concerns the arithmetic of the elliptic curve $E : y^2 = x^3 - 5x + 1$.

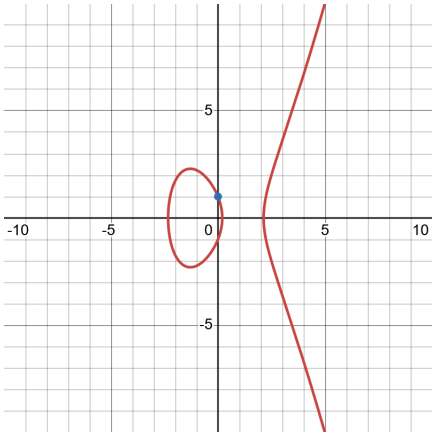

FIGURE 1. The elliptic curve $E : y^2 = x^3 - 5x + 1$.

a) We have the point $P = (0, 1) \in E(\mathbb{Q})$. Show that $2P = \left(\frac{25}{4}, \frac{117}{8}\right)$.
b) Suppose that $\alpha \in \mathbb{R}$ satisfies

$$\alpha^3 - 5\alpha + 1 = 0.$$

Then $Q := (\alpha, 0) \in E(\mathbb{R})$. Show that $2Q = O$, where $O := [0 : 1 : 0]$.

Problem 4. (Taken from the 2024 final exam.) 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 an integral solution.

1. Statements

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

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 $E(\mathbb{Q})[\text{tors}]$.