MATH 4573: HOMEWORK 10

INSTRUCTOR: TYLER GENAO

Due: April 17, 2026.

This homework has two sections: the first section has the assigned problems that you will turn in to Gradescope for credit. The second section contains recommended and bonus problems, either from myself, the textbook or other sources. These latter problems are not graded for credit, but you may find them to be useful practice and/or interesting!

For any assigned problem in this homework, **you must show all of your work in order to receive full credit. Your solutions can only cite up to the first corollary of §5.8 of our notes. Everything else must be proven.**

1. Problems to Submit

Exercise 1. This exercise will describe the 2-torsion and 3-torsion points on an elliptic curve $E/\mathbb{Q}$ in Weierstrass form. Recall that for an integer $n > 0$, a point $P \in E$ is **n-torsion** if $nP = O$.

First, assume that E is given in general Weierstrass form:

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

a) Prove that the 2-torsion points on E are precisely the points with vertical tangent lines.
b) Prove that the 3-torsion points are precisely the flex points of E.

For parts c) and d), assume that E is in short Weierstrass form:

$$E : y^2 = x^3 + Ax + B.$$

c) Show that the order two points on E are precisely the points $(\alpha, 0)$ where $\alpha \in \mathbb{C}$ is a root of $x^3 + Ax + B$.
d) Use part c) to prove that if $x^3 + Ax + B$ has a root over $\mathbb{Q}$, then $\#E(\mathbb{Q})[\text{tors}]$ is even.

Exercise 2. This exercise shows there are no integral points on the elliptic curve $E : y^2 = x^3 + 7$, using elementary techniques.

a) For the sake of contradiction, assume that $(a, b) \in E(\mathbb{Q})$ is an integral point. Show that a must be odd.
b) Show that $b^2 + 1 = (a + 2)(a^2 - 2a + 4)$.
c) Show that $a^2 - 2a + 4$ is congruent to 3 modulo 4. Then explain why there exists a prime divisor $p \mid (a^2 - 2a + 4)$ congruent to 3 modulo 4.
d) Reduce the original equation modulo p to derive a contradiction.

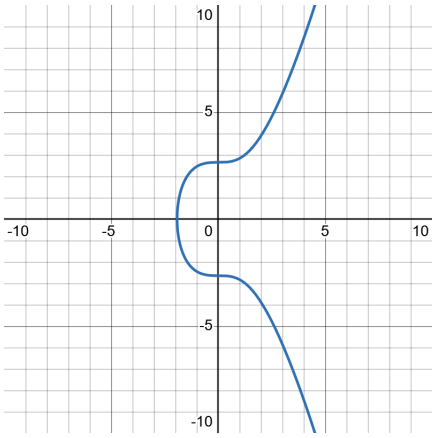

FIGURE 1. The elliptic curve $E : y^2 = x^3 + 7$.

Exercise 3. Consider the elliptic curve

$$E/\mathbb{Q} : y^2 = x^3 - 7x + 10,$$

which we did an example with in §5.7. We showed that for $P := (1, 2)$ and $Q := (3, 4)$, one has $P \oplus Q = (-3, 2)$ and $2P = (-1, -4)$. Compute $P \oplus' Q$ and $P \oplus' P$ in the group $(E(\mathbb{Q}), \oplus', Q)$, where Q is our new fixed identity.

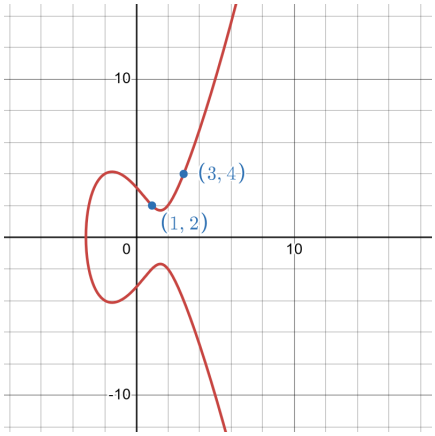

FIGURE 2. The elliptic curve $E : y^2 = x^3 - 7x + 10$.

Exercise 4. This exercise explores some arithmetic with an elliptic curve not in Weierstrass form.

Consider the cubic curve

$$E/\mathbb{Q} : x^3 + y^3 = 1.$$

a) Write down the homogenization E_H of E. Show that $O := [1 : -1 : 0]$ is the only real point at infinity on E. (Note that E has exactly three points at infinity over $\mathbb{C}$.)
b) Show that E_H is nonsingular. Assuming that E_H is irreducible, deduce that E_H is a projective elliptic curve.

c) Thus E is an elliptic curve over $\mathbb{Q}$; in particular $E(\mathbb{Q})$ is a group with identity $O := [1 : -1 : 0]$. Prove that for any point $P = (a, b) \in E(\mathbb{C})$ with $a \neq b$, the inverse of P is

$$-P = (b, a).$$

(You may assume that O is a flex point.)

d) For any point $P = (a, a) \in E$, show that P has order two.

e) (Extra credit) Explain why E has no positive rational points.

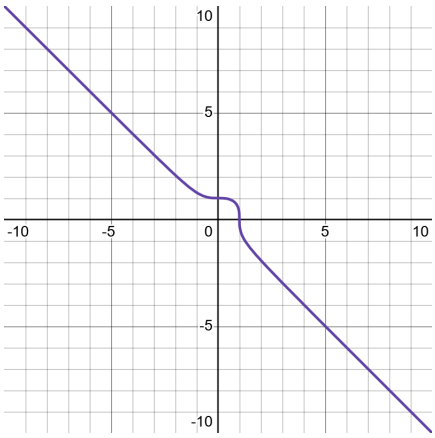

FIGURE 3. The elliptic curve $E : x^3 + y^3 = 1$.

Exercise 5. For this computational exercise, **you will need to submit your associated code as a text file onto Carmen.** In particular, your code must run without error if pasted into SageCell by the class grader, and *automatically* print the output you claim in your answer. Note that when you copy-paste your code into Carmen, it might mess some of the formatting up, so you may need to fix it. The deadline for submitting the code is the same as this HW.

This exercise investigates the behavior of the number of points on the elliptic curve

$$E/\mathbb{Q} : y^2 = x^3 + x$$

modulo primes p. You can use https://graui.de/code/elliptic2/ to graph elliptic curves modulo p, as well as compute tables of point additions on them.

For a prime p, we will write $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. As we will discuss in §5.8, we can realize E as an elliptic curve over $\mathbb{F}_p$ for almost all primes p, which also admits a group law via the chord and tangent method. We will use $E(\mathbb{F}_p)$ to denote the group of points on E modulo p, which are simply solutions $(x, y) \in \mathbb{F}_p^2$ to the congruence

$$y^2 \equiv x^3 + x \pmod{p},$$

which includes $O := [0 : 1 : 0]$ once you homogenize this congruence.

a) For primes $p = 3, 7, 11$, compute by hand the set of points $(x_0, y_0) \in \mathbb{F}_p^2$ with $y_0^2 \equiv x_0^3 + x_0 \pmod{p}$.

b) Prove that for any prime $p \equiv 3 \pmod 4$, one has

$$\#E(\mathbb{F}_p) = p + 1.$$

(*Hint:* if $y_0^2 \equiv x_0^3 + x_0 \pmod p$, then $x_0^3 + x_0$ is a square modulo p. However -1 is not a quadratic residue modulo p since $p \equiv 3 \pmod 4$.)

c) Create `Sage` code that does the following: given a prime p and an elliptic curve $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$ and $\Delta := -16(4A^3 + 27B^2) \not\equiv 0 \pmod p$, it returns the set of points in $E(\mathbb{F}_p)$, as well as the size of $\#E(\mathbb{F}_p)$ (you should include $[0 : 1 : 0]$). Run output for this for $E : y^2 = x^3 + x$ and $2 < p \leq 103$.

d) Based on your calculations in part c), make a conjecture for the size of $E(\mathbb{F}_p)$ when $E : y^2 = x^3 + x$ and $p \equiv 1 \pmod 4$. (One point)

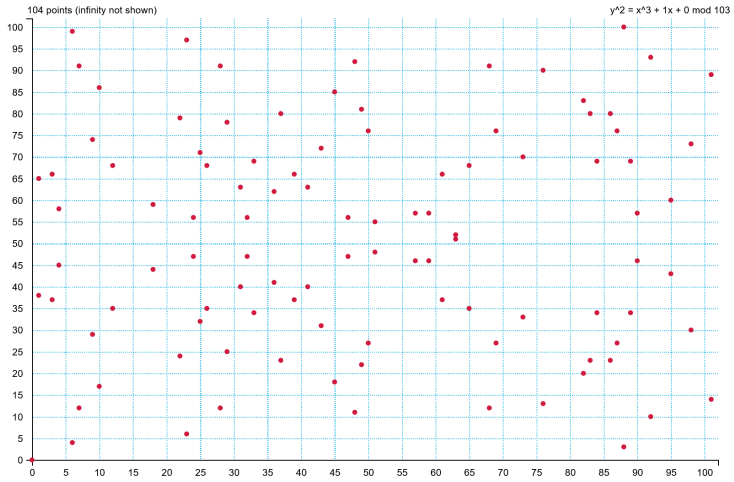

FIGURE 4. The elliptic curve $E : y^2 = x^3 + x$ modulo 103.

Exercise 6. Who did you consult for this assignment? What resources did you use?

2. Other Recommended Problems

Bonus Exercise 7. This exercise deals with the ":)-theorem."

In the following, let us define the **radical** function: for $\in \mathbb{Z}^+$, we set

$$\text{rad}\left(\right) := \prod_{\text{prime} \mid } .$$

Then the :)-theorem is as follows.

Theorem (:)-theorem)**.** *For each* $\ > 0$*, there are finitely many* $\in \mathbb{Z}^+$ *with* $\gcd\left(\ ,\ ,\ \right) = 1$ *and* $+\ =\ $*, such that*

$$\ > \operatorname{rad}\left(\ \cdot\ \cdot\ \right)^{1+\ }.$$

Prove the :)-theorem. (*Hint:* good luck!)