MATH 4573: HOMEWORK 9

INSTRUCTOR: TYLER GENAO

Due: April 10, 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 elliptic curve group law theorem in §5.7 our notes (including the definition of nP for $P \in E$ and $n \in \mathbb{Z}$). Everything else must be proven.**

1. Problems to Submit

Exercise 1. Parametrize the rational points on the hyperbola

$$H : x^2 - 2y^2 = 1$$

using the point $(1, 0) \in C(\mathbb{Q})$.

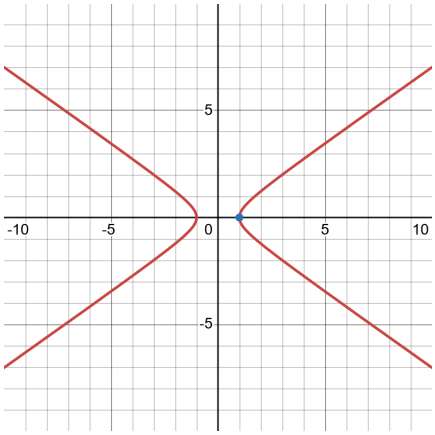

Figure 1. The hyperbola $H : x^2 - 2y^2 = 1$.

Exercise 2. Let $a, b, c \in \mathbb{Q}$ with $ab \neq 0$.

a) Show that if the conic

$$C : ax^2 + by^2 = c$$

is singular, then its only singular point is $(0, 0)$, and $c = 0$.

b) Show that if a and b are squares in $\mathbb{Q}$, then the conic

$$C : ax^2 - by^2 = 0$$

is the union of two rational lines through the origin. Use this to characterize all rational points on C.

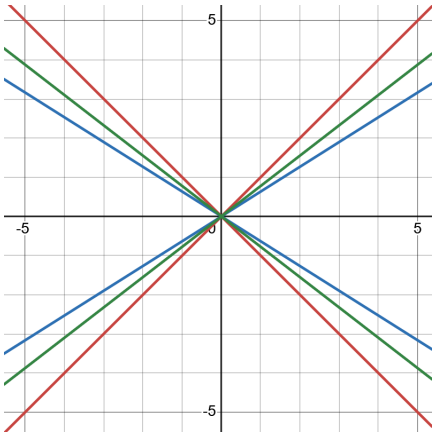

FIGURE 2. The (singular) conics $x^2 - y^2 = 0$, $2x^2 - 5y^2 = 0$ and $3x^2 - 5y^2 = 0$.

Exercise 3.

a) Show that for a polynomial $f(x) \in \mathbb{R}[x]$ and an integer $n \geq 2$, the curve

$$C : y^n = f(x)$$

has a singular point if and only if $f(x)$ has a *repeated root* in $\mathbb{R}$, i.e., there exists $x_0 \in \mathbb{R}$ with $f(x_0) = 0$ and $f'(x_0) = 0$.

b) Given a curve

$$C/\mathbb{R} : y^2 = (x - \alpha)(x - \beta)(x - \gamma)$$

where α, β and γ are real or complex numbers, the **discriminant** of C is

$$\Delta_C := [(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)]^2.$$

Prove that $\Delta_C = 0$ if and only if C is singular.

When such a curve $C : y^n = f(x)$ is nonsingular, it is called a *superelliptic curve*. When $n = 2$ and $\deg(f) \in \{3, 4\}$, this is an elliptic curve (which is more clear when $\deg(f) = 3$).

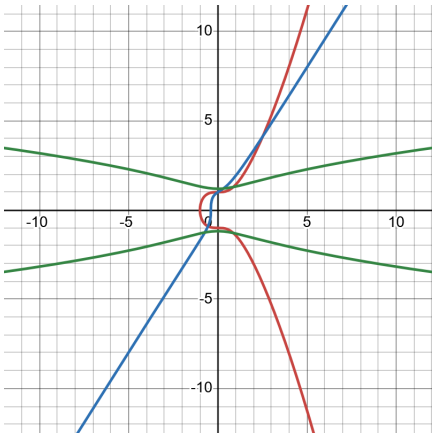

FIGURE 3. The hyperelliptic curves $y^2 = x^3 + 1$, $y^3 = 4x^3 + 2x + 1$ and $y^4 = x^2 + 1$.

Exercise 4. Let $E/\mathbb{Q}$ be an elliptic curve in **general Weierstrass form:**

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

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$.

Fix points $P := (x_1, y_1)$ and $Q := (x_2, y_2)$ in $E(\mathbb{Q})$. Let L denote the line through P and Q, with slope $m \in \mathbb{Q} \cup \{\infty\}$. We set $O := [0 : 1 : 0] \in E(\mathbb{Q})$.

a) Prove that L is a vertical line if and only if P, Q and O are collinear, iff $x_1 = x_2$ (and thus $y_1 = -a_1x_1 - a_3 - y_2$). (*Hint:* for the second iff, you may need to complete a square.)

b) Show that if P, Q and O are not collinear, then

$$P * Q := (x_3, y_3) = (x_3, m(x_3 - x_1) + y_1)$$

with $x_3 = m^2 + a_1m - a_2 - x_1 - x_2$.

c) Continuing part b), show that

$$P \oplus Q := (x_4, y_4) = (x_3, -a_1x_3 - a_3 - y_3).$$

d) In contrast to parts b) and c), prove that if P, Q and O are collinear, then

$$Q = -P.$$

e) Prove that for a point $P = (x, y) \in E(\mathbb{Q})$, one has

$$-P = (x, -a_1x - a_3 - y).$$

f) Argue why these formulas should still hold if we replace $\mathbb{Q}$ with an arbitrary field F. (One point)

Exercise 5. Let $E/\mathbb{Q}$ be an elliptic curve in **short Weierstrass form:**

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

where $A, B \in \mathbb{Q}$.

a) Briefly explain how short Weierstrass form is a special case of general Weierstrass form.

b) Show that for two points $P := (x_1, y_1)$ and $Q := (x_2, y_2)$ in $E(\mathbb{Q})$ which are not collinear to $O := [0 : 1 : 0]$, one has the formula

$$P \oplus Q := (x_3, y_3) = (m^2 - x_1 - x_2, -m(x_3 - x_1) - y_1).$$

c) Show that for any point $P := (x, y) \in E(\mathbb{Q})$, one has

$$-P = (x, -y).$$

(*Hint for all parts:* use Exercise 4.)

Exercise 6. Consider the elliptic curve

$$E : y^2 = x^3 + 17$$

(we studied it in §5.6). Given points $P_1 := (-2, 3)$, $P_2 := (-1, 4)$ and $P_3 := (2, 5)$ in $E(\mathbb{Q})$, prove the following.

a) $-2P_1 = (8, 23)$.

b) $P_2 \oplus P_3 = \left(-\frac{8}{9}, -\frac{109}{27}\right)$ (which is $\approx (-0.88889, -4.03704)$).

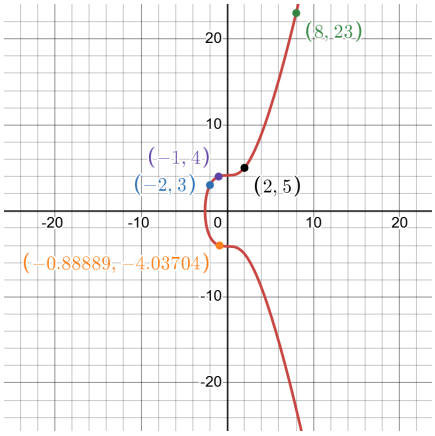

FIGURE 4. The elliptic curve $E : y^2 = x^3 + 17$.

Exercise 7. 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 introduces some basic elliptic curve functions in `Sage`, as well as the *LMFDB database.* A comprehensive manual on elliptic curve functions in `Sage` can be found here.

a) Using the elliptic curve $E : y^2 = x^3 + 17$ from Exercise 6, for the points $P_1 := (-2, 3)$, $P_2 := (-1, 4)$ and $P_3 := (2, 5)$ in $E(\mathbb{Q})$, write `Sage` code to compute the following.

i) $-2P_1$.

ii) $P_2 \oplus P_3$.

iii) nP_1, for $0 \leq n \leq 30$. What do you observe from the output?
(*Hint:* useful functions include `EllipticCurve([a1,a2,a3,a4,a6]),` as well as `E(a,b)` to realize a point (a, b) as a point on an elliptic curve E.)

A great site for elliptic curve data is the **LMFDB.** At this moment in time, it contains over 3.8 million elliptic curves over $\mathbb{Q}$, with dozens of numerical invariants listed for each of these curves. On each elliptic curve page, the 'Show commands' option in the top right corner lets you view these invariants as `Sage` code functions!

Parts b) - d) continue to focus on our elliptic curve $E : y^2 = x^3 + 17$ from part a).

b) Navigate the LMFDB and write down the *LMFDB label* of E.
c) Based on its LMFDB page, how many integral points does E have?
d) Based on its LMFDB page, what is the group structure of $E(\mathbb{Q})$, as an abstract abelian group?

The final part of this exercise focuses on patterns in elliptic curve *torsion groups.* For an elliptic curve $E/\mathbb{Q}$, we have its **torsion subgroup over $\mathbb{Q}$,** defined as

$$E(\mathbb{Q})[\text{tors}] := \{P \in E(\mathbb{Q}) : \exists n \in \mathbb{Z}^+, nP = O\}.$$

Thus $E(\mathbb{Q})[\text{tors}]$ is the subgroup of $E(\mathbb{Q})$ of points with finite order.

e) Write code to compute the *size* of torsion subgroups of all elliptic curves $E/\mathbb{Q} : y^2 = x^3 + Ax + B$ where $0 \leq A, B \leq 50$.
(*Hint:* you might find `E.torsion_subgroup()` useful for describing the structure of $E(\mathbb{Q})[\text{tors}]$. Every torsion subgroup satisfies $E(\mathbb{Q})[\text{tors}] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for some $m, n \in \mathbb{Z}$ with $m \mid n$; the function `E.torsion_subgroup().invariants()` returns () if $m = n = 1$, (n) if $n = 1$ and (m, n) otherwise.)
f) Based on your calculations in e), what observations can you make? (One point)

Exercise 8. Who did you consult for this assignment? What resources did you use?

2. Other Recommended Problems

From [NZM91, §5.6], page 260: $\#2, 5, 7 - 10$.
From [NZM91, §5.7], pages $278 - 279$: $\#5, 6$.

Bonus Exercise 9. Prove that for a polynomial $p(x) \in \mathbb{Q}[x]$ of degree $n \geq 1$, if p has $n - 1$ rational roots, then it has n rational roots. (*Hint:* use the proposition from our notes that states $r \in \mathbb{Q}$ is a root of $p(x)$ if and only if $(x - r) \mid p(x)$.)

Bonus Exercise 10. Show that the following affine curves are nonsingular.

a) $F_n : x^n + y^n = 1$, where $n \geq 1$.
b) $C_1 : 5xy + y^2 = 2$.
c) $C_2 : y^5 = 4x^3 + 2x^2 - 2x - 1$.

Prove that the following projective curve is singular.

d) $C_3 : X^3 + X^2Z + X^2Y = Z^3$, where $C_3(\mathbb{R}) \subseteq \mathbb{P}_2(\mathbb{R})$.

(*Hint:* in some parts, Exercise 3 might help.)

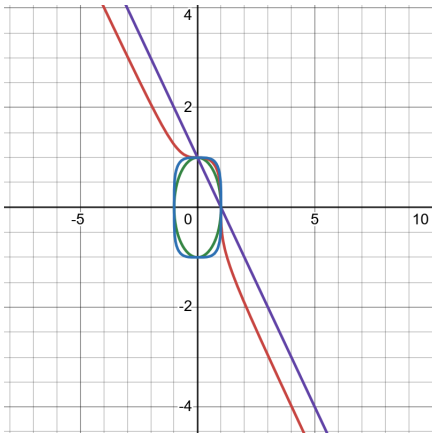

FIGURE 5. The Fermat curves F_1, F_2, F_3 and F_4.

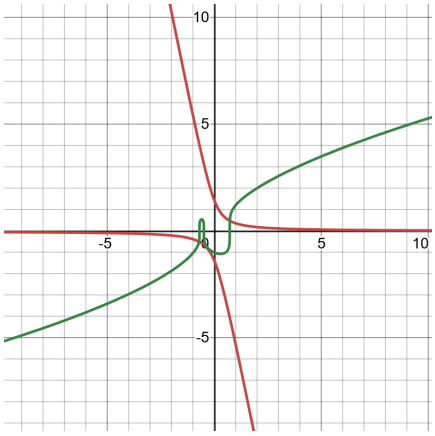

FIGURE 6. The curves C_1 (hyperbola) and C_2 (superelliptic).

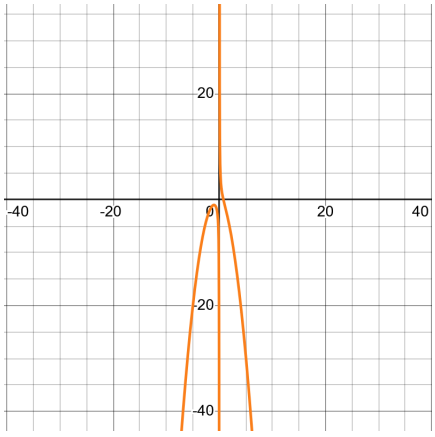

FIGURE 7. The curve C_3, dehomogenized and pictured in $\mathbb{R}^2$.

Bonus Exercise 11. Let $f(x) \in \mathbb{R}[x]$ be a cubic polynomial. Show that $y^2 - f(x) \in \mathbb{R}[x, y]$ is an irreducible polynomial over $\mathbb{C}$. (*Hint:* show that $y^2 - f(x)$ being reducible in $\mathbb{C}[x, y]$ means we can write $y^2 - f(x) = (y - g(x))(y - h(x))$ for some $g, h \in \mathbb{C}[x]$.)

Bonus Exercise 12. Consider the elliptic curve

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

a. Using the picture below, guess the real flex points of E.
b. With proof, determine the real flex points of E.

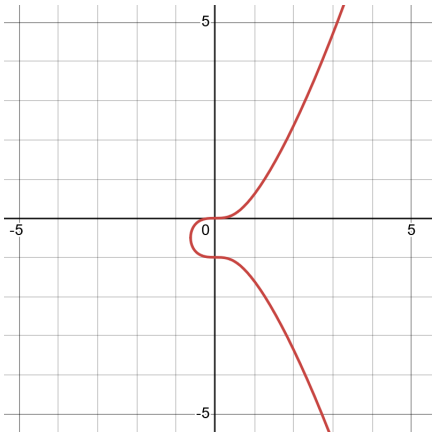

FIGURE 8. The elliptic curve $E : y^2 + y = x^3$.

Bonus Exercise 13. This exercise will explore the concept of the *genus* of a plane curve.

Suppose that $f(x, y) \in \mathbb{Q}[x, y]$ is an irreducible polynomial of degree d such that C_f is *nonsingular*. Then the **genus** of C, written as $g := g(C)$, is equal to $\frac{(d-1)(d-2)}{2}$.

The genus g of a curve $C/\mathbb{Q}$ is intimately connected to the number of rational points on C. When $g = 0$, C has either zero or infinitely many rational points; for example, conics are genus zero curves. When $g = 1$, C is an elliptic curve. And when $g \geq 2$, a celebrated result of G. Faltings implies that C has *finitely* many rational points.

Determine whether the rational curves defined by the following equations have a finite or infinite amount of rational points (or that the information is inconclusive).

a) $C_1 : x^2 + y^2 = r^2$, where $r \neq 0 \in \mathbb{Q}$.
b) $C_2 : y^2 = x(x - 1)(x - 2)$.
c) $C_3 : y^5 = x(x - 1)(x - 3)(x - 5)(x - 7)$.
d) $F_n : x^n + y^n = 1$, where $n \in \mathbb{Z}^+$.

The genus also has a visual interpretation. A nonsingular irreducible curve $C/\mathbb{Q}$ with genus $g \geq 0$, when viewed as a *complex Riemann surface* in *projective space,* appears as a torus with g holes. Thus, an elliptic curve over $\mathbb{C}$ is a "complex donut," for example.

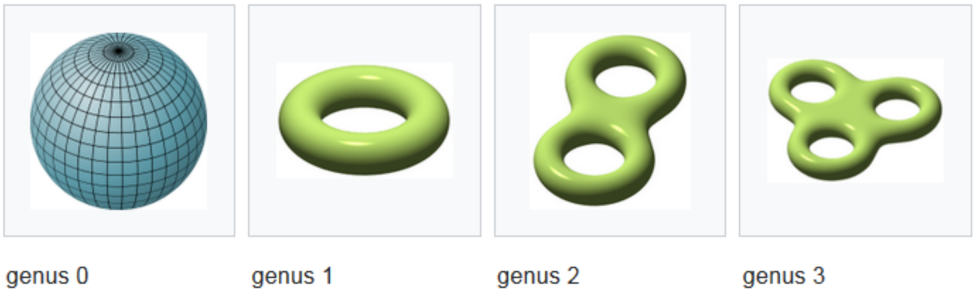

FIGURE 9. Pictures of g-holed tori in complex projective space, cf. Wikipedia.

REFERENCES

[NZM91] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An introduction to the theory of numbers*, 5th Ed., John Wiley & Sons, Inc., New York (1991).