MATH 4573: HOMEWORK 9

INSTRUCTOR: TYLER GENAO

Due: April 19, 2024.

This homework has two sections: the first section has the problems that you'll turn in for credit. The second section contains recommended problems from the textbook, myself or other sources; you are not required to do these, but I recommend that you check them out.

For any problem in this assignment, **you must show all of your work in order to receive full credit.** Please do not use words such as "clear", "obvious" or "trivial" in your solutions.

Your solutions should not use theorems from sections which come after the day the homework was assigned. This HW should use up to what we've covered in class so far (including §5.6 and §5.7, as well as our notes in class).

For this homework assignment, **Each problem is worth** 10 **points.** This homework will be **out of 60 points,** so you only need to do six problems. Extra problems that you do correctly will count as extra credit.

1. Problems to Submit

Exercise 1. This exercise determines when certain plane curves are nonsingular.

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

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

in $\mathbb{R}^2$ 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

$$C : y^2 = (x - \alpha)(x - \beta)(x - \gamma)$$

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

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

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

In particular, when a cubic polynomial $f(x) \in \mathbb{Q}[x]$ has no repeated roots, the cubic curve defined by $y^2 = f(x)$ is nonsingular, and in fact is an elliptic curve.

Exercise 2. 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, the previous exercise might help.)

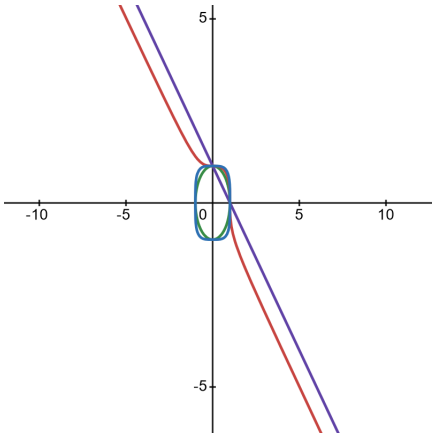

FIGURE 1. The Fermat curves F_1, F_2, F_3 and F_4 in $\mathbb{R}^2$.

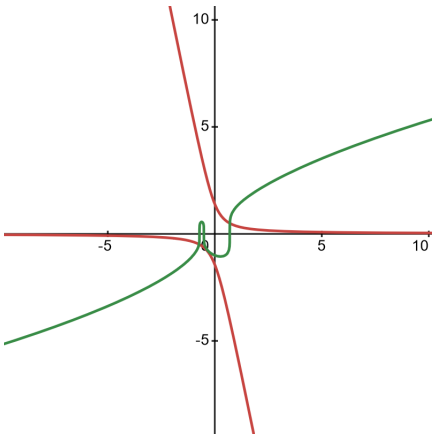

FIGURE 2. The curves C_1 (hyperbola) and C_2 (hyperelliptic) in $\mathbb{R}^2$.

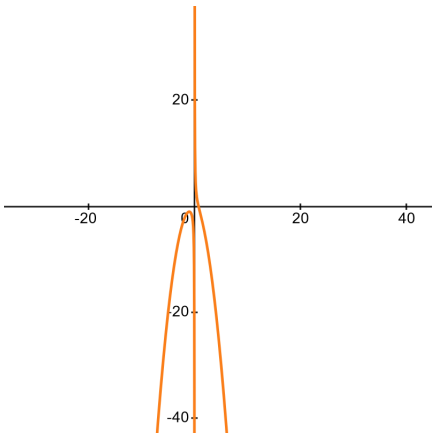

FIGURE 3. The curve C_3, dehomogenized and pictured in $\mathbb{R}^2$.

Exercise 3. Parametrize the rational points on the hyperbola

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

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

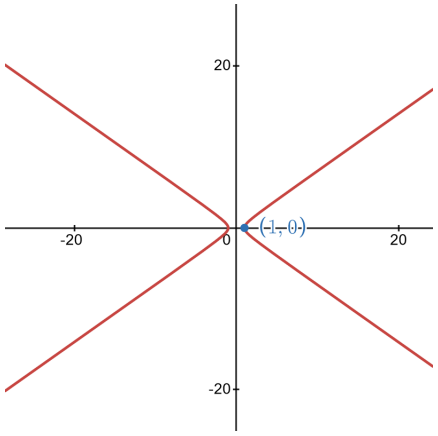

FIGURE 4. The hyperbola $H : x^2 - 2y^2 = 1$.

Exercise 4. Fix an elliptic curve over $\mathbb{Q}$ in (short) Weierstrass form

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

Then the *torsion subgroup of E over $\mathbb{Q}$,* denoted $E(\mathbb{Q})[\text{tors}]$, is the subgroup of $E(\mathbb{Q})$ of points with finite order:

$$E(\mathbb{Q})[\text{tors}] = \{P \in E(\mathbb{Q}) : NP = O \text{ for some } N \in \mathbb{Z}^+\}.$$

(Note that we include $O \in E(\mathbb{Q})[\text{tors}]$.)

This exercise explores the torsion points on E of order two.

a) Show that $P \in E$ has order two if and only if

$$P = (\alpha, 0)$$

where α is a root of $x^3 + Ax + B$.

b) As it turns out, for any elliptic curve $E_{/\mathbb{Q}}$, one has that $E(\mathbb{Q})[\text{tors}]$ is a finite abelian group. With this in mind, prove the following: assume that E is defined by $y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Q}$. If $x^3 + Ax + B$ is a reducible polynomial over $\mathbb{Q}$, then the size of $E(\mathbb{Q})[\text{tors}]$ is even.

Exercise 5. This exercise proves some basic results for elliptic curves in (short) Weierstrass form,

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

a) Show that E has exactly one point at infinity.

b) Show that for any point $P := (a, b) \in E(\mathbb{R})$, one has the additive inverse

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

(*Hint:* the collinearity theorem might help: on an elliptic curve $E_{/\mathbb{Q}} : y^2 = x^3 + Ax + B$, three points $P, Q, R \in E$ are collinear if and only if $P \oplus Q \oplus R = O$.)

Exercise 6. For the elliptic curve

$$E_{/\mathbb{Q}} : y^2 = x^3 + 17,$$

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 $\approx (-0.889, -4.037)$).

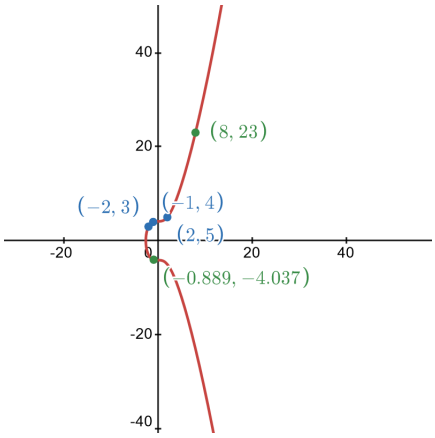

FIGURE 5. The elliptic curve $E : y^2 = x^3 + 17$.

Exercise 7. 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 solution. 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.

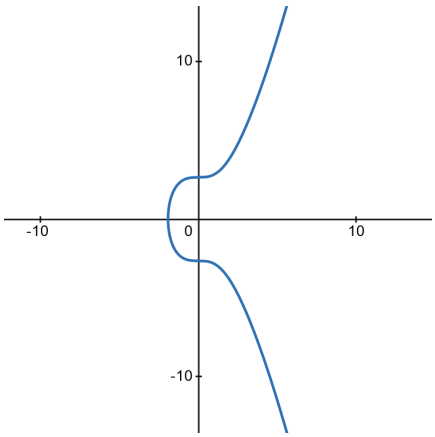

FIGURE 6. The elliptic curve $E : y^2 = x^3 + 7$.

Exercise 8. This exercise explores some arithmetic with elliptic curves not in Weierstrass form.

Consider the cubic curve

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

a) Write down the projective closure E_H of E. Show that $O := [1 : -1 : 0]$ is the only real point at infinity on E. Also show that E has exactly 3 points at infinity over $\mathbb{C}$.

b) Assume that O is a nonsingular inflection point on E_H. Show that E_H is nonsingular. Thus, E_H is a *projective* elliptic curve. (*Hint:* de-homogenize E_H to end up with E again, and check E for singular points.)

c) Assume that $x^3 + y^3 - 1$ is irreducible over $\mathbb{Q}$; thus, E is an elliptic curve over $\mathbb{Q}$. Prove that for any point $P = (a, b) \in E(\mathbb{R})$ with $a \neq b$, the inverse of P is

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

(*Hint:* what *three* points does the line through (a, b) and (b, a) pass through on E?)

d) (Extra credit) Explain why E has no positive rational solutions.

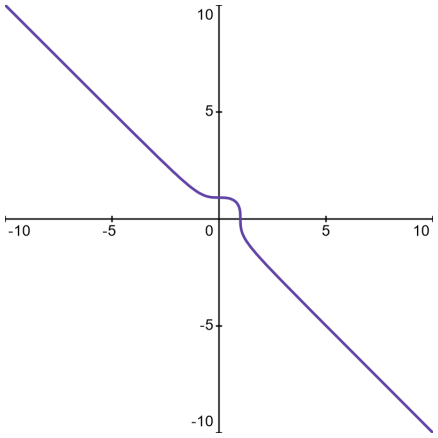

FIGURE 7. The elliptic curve $E : x^3 + y^3 = 1$.

Exercise 9. This exercise investigates the behavior of the number of points of the elliptic curve

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

modulo primes $\ell \in \mathbb{Z}^+$. 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 $\ell \in \mathbb{Z}^+$, we will write $\mathbb{F}_\ell := \mathbb{Z}/\ell\mathbb{Z}$. We will also use $E(\mathbb{F}_\ell)$ to denote the set of points on E modulo ℓ. (*Reminder:* we always include $O := [0 : 1 : 0]$ as a point in $E(\mathbb{F}_\ell)$.)

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

b) Prove that for any prime $\ell \equiv 3 \pmod 4$, one has
$$|E(\mathbb{F}_\ell)| = \ell + 1.$$
(*Hint:* if $y_0^2 \equiv x_0^3 + x_0 \pmod \ell$, then $x_0^3 + x_0$ is a square modulo ℓ. However, -1 is not a quadratic residue modulo ℓ since $\ell \equiv 3 \pmod 4$.)

c) (Extra credit) Create a program that does the following: given a prime $\ell \in \mathbb{Z}^+$ and an elliptic curve $E : y^2 = x^3 + Ax + B$ with $-16(4A^3 + 27B^2) \not\equiv 0 \pmod \ell$, it returns the set of point $E(\mathbb{F}_\ell)$, as well as the size $|E(\mathbb{F}_\ell)|$ (including $[0 : 1 : 0]$). What patterns do you spot for the size of $E(\mathbb{F}_\ell)$, $E : y^2 = x^3 + x$, when $\ell \equiv 1 \pmod 4$? Based off your calculations, make a conjecture on the size.

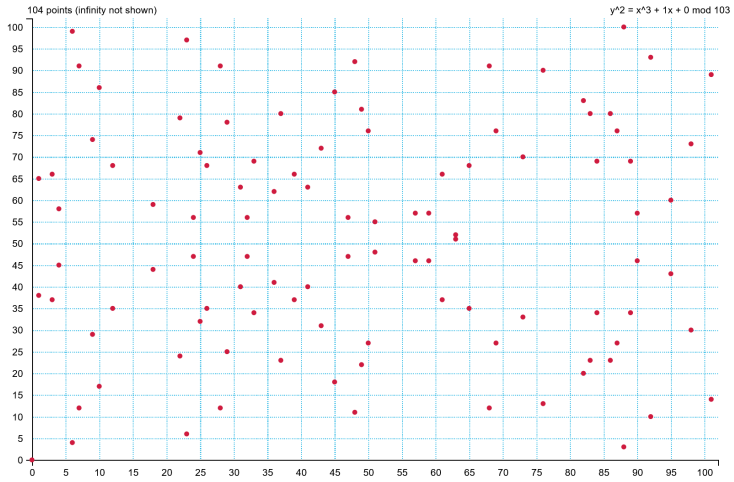

FIGURE 8. The elliptic curve $E : y^2 = x^3 + x$ modulo 103.

Exercise 10. Who did you consult for this assignment? What resources did you use?

2. Other Recommended Problems

From the textbook, page 260: #2, 10.
Pages 279 − 280: #5, 6, 14, 15.

Bonus Exercise 11. This exercise will explore the concept of the *genus* of a plane curve.

Suppose that $f(x, y) \in \mathbb{Z}[x, y]$ 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.

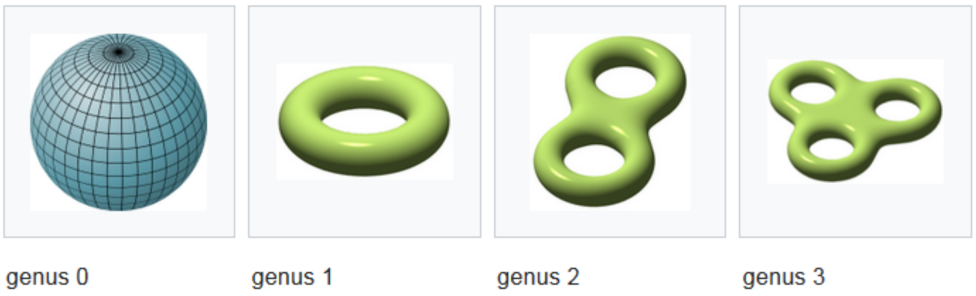

FIGURE 9. Pictures of g-holed tori in complex projective space, cf. Wikipedia.

Bonus Exercise 12. 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*

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

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

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).