2.3 Exercise Sheet 3

2.3.A Numerical and Exploration

Exercise 2.3.1. For each prime $p \neq 2, 3$, and $b, c = 0, \ldots, p-1$ such that $4b^3 + 27c^2 \not\equiv 0 \pmod{p}$, let $E_{p,b,c}$ be the elliptic curve $y^2 = x^3 + bx + c$ over $\mathbb{F}_p$.

(a) Using, say, a simple `for` loop and the `E.abelian_group()` function in Sage, study the abelian group structure on $E_{p,b,c}$ for each $p \leq 19$ and each allowable b, c. Find patterns and make conjectures. For instance, what can you say about the ratio $\#E_{p,b,c}(\mathbb{F}_p)/p$ in general? Can you find (p, b, c) such that $E_{p,b,c}(\mathbb{F}_p)$ is cyclic of order 11? 19? When is this group cyclic? When it is not, does it ever need more than 2 generators?

(b) Modify your `for` loop in (a) to remove all results in which the group $E_{p,b,c}(\mathbb{F}_p)$ is cyclic, so that we can focus on the non-cyclic case. (In Sage, you can test whether a group is cyclic using the `is_cyclic()` function.) Allowing $p \leq 100$ now, find patterns and make conjectures. Does this group ever need more than 2 generators? Can you find a (p, b, c) such that the group $E_{p,b,c}(\mathbb{F}_p)$ is isomorphic to $\mathbb{Z}/3 \oplus \mathbb{Z}/3$? $\mathbb{Z}/m \oplus \mathbb{Z}/m$ for $m = 4, 5, \ldots, 9, 10$? $\mathbb{Z}/33 \oplus \mathbb{Z}/3$? $\mathbb{Z}/18 \oplus \mathbb{Z}/6$? When the group $E_{p,b,c}(\mathbb{F}_p)$ is $\mathbb{Z}/m \oplus \mathbb{Z}/m$, what do you notice about $p \mod m$?

(c) Can you use your calculations in (a) and (b) to give a lower bound on the number N_p of isomorphism classes of elliptic curves over $\mathbb{F}_p$ for each p with say $5 \leq p \leq 100$?

Exercise 2.3.2. Given a prime $p \neq 2, 3$, write Sage code to compute the number N_p of isomorphism classes of elliptic curves over $\mathbb{F}_p$ (up to isomorphism over $\mathbb{F}_p$). For $p \leq 200$, compute N_p/p. What patterns do you notice? (Possible hints: You might try something similar to what you did in 2.3.1. In Sage, you can test whether a curve `E1` defined over a field say `GF(p)` is isomorphic to another curve `E2` defined over the same field by using the boolean function `E1.is_isomorphic(E2)`.)

Exercise 2.3.3.

(a) Classify all elliptic curves over $\mathbb{F}_2$ (up to isomorphism over $\mathbb{F}_2$); in particular, compute N_2. (Hint: Note that each of the quantities $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_2$ could give rise to a curve, which means a priori that there are $2^5 = 32$ possibilities, but it is easy to eliminate a lot of these possibilities by inspection. For instance, it is clear from the formula for Δ in characteristic two (1.9.13) that not both a_1 and a_3 can be zero. You may use Sage to speed up calculations if that is helpful.)

(b) For each (isomorphism class of a) curve E as in (a),
  (i) identify the group $E(\mathbb{F}_2)$,
  (ii) find out if the curve E is supersingular,
  (iii) figure out the automorphism groups $\mathrm{Aut}_{\mathbb{F}_2}(E)$ and $\mathrm{Aut}_{\overline{\mathbb{F}}_2}(E)$, and
  (iv) calculate the j-invariant $j(E)$.

(c) $(*)$ For each pair of curves that are not isomorphic over $\mathbb{F}_2$ but have the same j-invariant, figure out the smallest field extension $L/\mathbb{F}_2$ over which those two curves *are* isomorphic. (Hint: This L is one of $\mathbb{F}_4, \mathbb{F}_{16}, \mathbb{F}_{256}$.)

(d) $(*)$ Repeat the same for $\mathbb{F}_3, \mathbb{F}_4, \mathbb{F}_5$, and $\mathbb{F}_7$. (Hint: Again, you may use Sage. This problem is not as difficult as it may look, since over $\mathbb{F}_3$ you can put elliptic curves in the short Weierstrass form $y^2 = x^3 + ax^2 + bx + c$, and over $\mathbb{F}_5$ and $\mathbb{F}_7$ you can put them in the even shorter Weierstrass form $y^2 = x^3 + bx + c$, as above. Recall that $\mathbb{F}_4 \cong \mathbb{F}_2[\omega] \cong \mathbb{F}_2[x]/(x^2 + x + 1)$. The way to work with $\mathbb{F}_4$ in Sage is to use `K.<a> = GF(4)`; this returns a field K isomorphic to $\mathbb{F}_4$ with a generator named a satisfying $a^2 + a + 1 = 0$.)

If you haven't seen the fields $\mathbb{F}_{p^n}$ for $n \geq 2$ (note that $\mathbb{F}_{p^n} \ncong \mathbb{Z}/(p^n)$ as rings!), you can skip those parts of this exercise for now and return to them later when you do.

Exercise 2.3.4.

(a) Find all rational solutions to $x^2 + y^2 = 2$ by projecting from $(-1, -1)$ and using t as the slope of the line, i.e., by mapping t to the other intersection of $y + 1 = t(x + 1)$ with $x^2 + y^2 = 2$.

(b) Using your solution to (a) or otherwise, prove that if p, q, r are positive integers with $p < q < r$ such that p^2, q^2 and r^2 are in arithmetic progression, then there are coprime $m, n \in \mathbb{Z}$ of different parity with $m > n > 0$ such that (p, q, r) is one of

$$\left(\pm(2mn - (m^2 - n^2)), m^2 + n^2, 2mn + m^2 - n^2\right).$$

Figure out exactly when each sign holds. (Hint: Your answer may have something to do with $\sqrt{2} \pm 1$.)

Exercise 2.3.5. (Adapted from [14].) For simplicitly, let's work over $K = \mathbb{Q}$. Let $C \subset \mathbb{P}^2_K$ be the cubic curve with equation

$$XY^2 - X^2Y + 2X^2Z - 2XZ^2 - 3Y^2Z + 3YZ^2 = 0.$$

(a) (∗) Suppose $p, q, r, s \in \mathbb{Z}_{>0}$ are such that p^2, q^2, r^2, s^2 are in arithmetic progression. Suppose that $p \neq s$, so the sequence is not the constant sequence. Show that

$$[p - s : q - s : r - s] \in C(K).$$

Therefore, to get a handle on all four-term sequences of squares in arithmetic progressions, it suffices to get a handle on $C(K)$. (Hint: There are many ways to do this. One is to just plug and check. Another, possibly more illuminating, way might be to express the given condition in terms of two quadratic conditions on p, q, r, s; indeed, what *does* it mean to be in arithmetic progression? Next, let $(X, Y, Z) = (p - s, q - s, r - s)$, and write these quadratic conditions in terms of X, Y, Z, and s. Finally, try to eliminate s from the equations.)[4]

(b) Is C smooth? Find a rational inflection point on C. (Hint: Get Desmos to draw a picture of the affine patch $Z \neq 0$ of C. Then try an intersection with a coordinate axis.)

(c) Using your solution to (b) or otherwise, find the linear change of coordinates that transforms C into the elliptic curve $E \subset \mathbb{P}^2_K$ in short Weierstrass form

$$y^2 = x(x + 1)(x + 4).$$

We met this curve in 1.8.4.

(d) Using the Nagell-Lutz Theorem, find all torsion points in $E(K)$. How many of them are there? Describe the structure of the torsion subgroup $\operatorname{Tors} E(K)$. (Hint: Up to isomorphism, there are three groups of size $\#\operatorname{Tors} E(K)$. Part of your task is to figure out which of these is the isomorphism type of $\operatorname{Tors} E(K)$. What distinguishes these three types?)

(e) Later in the course, we will prove that $\operatorname{rank} E = 0$. Assuming this result, prove the theorem stated by Fermat in 1640 and first proven by Euler in 1780 which states that there are no nonconstant four-term sequence of squares in arithmetic progression in the integers.

(f) How much of the above discussion carries over when we replace K by a number field or a finite field? For which characteristics does the above discussion still apply, and for which does it not? When it does apply, what do we learn about four squares in arithmetic progressions over these fields?

2.3.B PODASIPs

Prove or disprove and salvage if possible the following statements.

Exercise 2.3.6. Let K be a field.

(a) Let $C \subset \mathbb{A}^2_K$ be an affine curve. If C is integral, then so its projective closure $\overline{C} \subset \mathbb{P}^2_K$.

(b) Let $D \subset \mathbb{P}^2_K$ be a projective curve. If D is integral, then so is each affine patch $D^\circ \subset \mathbb{A}^2_K$.

The same statements are true with "integral" replaced by "geometrically integral".

Exercise 2.3.7. Let K be a field.

(a) Let $C \subset \mathbb{A}^2_K$ be an integral affine curve with defining equation $f \in K[x, y]$. The element $f \in K[x, y]$ is prime.

We define the *function field* of C to be $K(C) := \operatorname{Frac} K[x, y]/(f)$. (Make sure you see why this is independent of the choice of f!)

(b) If $C \subset \mathbb{A}^2_K$ is an integral curve with projective closure $\overline{C}$, then $K(C) \cong K(\overline{C})$.

(c) If $D \subset \mathbb{P}^2_K$ is an integral curve with affine patch say $D^\circ \subset \mathbb{A}^2_K$, then $K(D) \cong K(D^\circ)$.

[4] For the cognoscenti: The curve $\mathbb{V}(p^2 + r^2 - 2q^2, q^2 + s^2 - 2r^2) \subset \mathbb{P}^3_K$ is a smooth projective geometrically integral curve of genus one, and hence an elliptic curve when equipped with the rational point $[1 : -1 : -1 : 1]$. We are trying to find a Weierstrass equation for it, which can be done by projecting from the point $[1 : 1 : 1 : 1]$ to embed the curve as a cubic $C \subset \mathbb{P}^2_K$, and then applying a linear change of coordinates.

Exercise 2.3.8. Let K be a field.

(a) Let $C_1, C_2 \subset \mathbb{A}^2_K$ be affine curves, say $C_i = \mathbb{V}(f_i)$ for nonzero $f_1, f_2 \in K[x,y]$. Let $C = \mathbb{V}(f_1 \cdot f_2)$, so that for all fields L/K we have $C(L) = C_1(L) \cup C_2(L)$. (Note that C is not the "union" of C_1 and C_2 in the naive sense; for instance we could have $f_1 = f_2 = x$, in which case C would be $C = \mathbb{V}(x^2)$.) If L/K is a field extension, and $P \in C_1(L) \cap C_2(L)$, then $P \in C(L)$ is a singular point. (This might help explain why curves like $\mathbb{V}(x^2)$ are everywhere singular.) A similar result is true for projective curves.

(b) If $C \subset \mathbb{A}^2_K$ is a smooth affine curve, then C is (geometrically) integral. The same is true for projective curves. (Hint: You may use the full strength of Bézout's Theorem (1.6.9), which we have admittedly not proven.)

Exercise 2.3.9. Let K be a field, $C \subset \mathbb{P}^2_K$ a smooth cubic curve, and $\mathscr{O}_1, \mathscr{O}_2 \in C(K)$. For $i = 1, 2$, let $\oplus_i$ denote the operation $P \oplus_i Q := \mathscr{O}_i * (P * Q)$ for $P, Q \in C(K)$, so that $(C(K), \oplus_i)$ is an abelian group by 1.7.7. The map

$$(C(K), \oplus_1) \to (C(K), \oplus_2), \quad P \mapsto \mathscr{O}_1 * (\mathscr{O}_2 * P)$$

is a group isomorphism. In particular, the group law on $C(K)$ does not depend on the choice of $\mathscr{O}$, up to isomorphism.

Exercise 2.3.10. (**)

(a) Let $b \in \mathbb{Z}$ be fourth-power-free, and let $E_b/\mathbb{Q}$ be the elliptic curve with Weierstrass equation

$$y^2 = x^3 + bx.$$

Then $\operatorname{Tors} E_b(\mathbb{Q})$ is either $\mathbb{Z}/2$ or $\mathbb{Z}/4$. When does each case hold?

(b) Let $c \in \mathbb{Z}$ be sixth-power-free, and let $E_c/\mathbb{Q}$ be the elliptic curve with Weierstrass equation

$$y^2 = x^3 + c.$$

Then $\operatorname{Tors} E_c(\mathbb{Q})$ is either $\mathbb{Z}/2$ or $\mathbb{Z}/3$. When does each case hold? Compare your result to your answer to 2.2.4(e).

(Hint: First, try lots of examples, using Sage. Then, if needed, refer to [1, §12] for a detailed hint.)