2.4 Exercise Sheet 4

2.4.A Numerical and Exploration

Exercise 2.4.1. Here we list some pairs (E, P), where $E/\mathbb{Q}$ is an elliptic curve and $P \in E(\mathbb{Q})$. Using Sage, find the order of P in $E(\mathbb{Q})$.

(a) $E : y^2 = x^3 - 4x + 4$ and $P = (2, 2)$.
(b) $E : y^2 = x^3 - x + 1$ and $P = (1, 1)$.
(c) $E : y^2 = x^3 - 219x + 1654$ and $P = (11, 24)$.
(d) $E : y^2 + xy = x^3 - x + 137$ and $P = (2, 11)$.
(e) $E : y^2 = x^3 - 189x + 1269$ and $P = (3, 27)$. Also do $P = (21, 81)$ on the same curve.

Find other interesting examples on the LMFDB.

Exercise 2.4.2. (Adapted from [2, Exercise 2.12]) Using the Nagell-Lutz Theorem or otherwise, for each elliptic curve $E/\mathbb{Q}$ below, find all rational points of finite order on E and determine the structure of $\operatorname{Tors} E(\mathbb{Q})$:

(a) $y^2 = x^3 - 2$
(b) $y^2 + xy + y = x^3$.
(c) $y^2 = x^3 + 1$
(d) $y^2 = x^3 - 43x + 166$
(e) $y^2 + xy = x^3 - 45x + 81$

(Hint: You may have to complete the square to bring the given curve into shortest Weierstrass form to apply Nagell-Lutz. At least try to do some of these computations by hand (i.e., without using Sage) to convince yourself that they can be done in a reasonable amount of time!)

Exercise 2.4.3. Let p be a prime and let $E/\mathbb{Q}$ be the elliptic curve with equation $y^2 = x^3 + p^2$. What is $\operatorname{Tors} E(\mathbb{Q})$? Experiment in Sage, make conjectures, and then prove your conjectures.

Exercise 2.4.4.

(a) Fix a prime p. For each integer $m \in \mathbb{Z}_{\geq 0}$, let $S_m(p) := \sum_{x=0}^{p-1} x^m$. What can you say about the function $m \mapsto S_m(p) \pmod p$? Observe patterns, and make and prove conjectures. What does the value of 0^0 need to be in order to obtain a very clean and uniform result?
(b) (Only for those who know about finite fields other than $\mathbb{F}_p$ for primes p.) Fix a finite field $\mathbb{F}_q$. Repeat the same as in (a) for the function $m \mapsto \sum_{x \in \mathbb{F}_q} x^m$.

Exercise 2.4.5 (Fisher)**.** Let p be an odd prime, and let E be an elliptic curve over $\mathbb{F}_p$.

(a) Show that there exists and elliptic curve E' over $\mathbb{F}_p$ such that $\#E(\mathbb{F}_p) + \#E'(\mathbb{F}_p) = 2(p+1)$. (Hint: Modulo the right definitions of these objects, you could probably have solved this problem before you knew anything about elliptic curves.)
(b) Given the curves E and E' as in (a), what do you notice about the sizes of $E(\mathbb{F}_p) \times E'(\mathbb{F}_p)$ and of $E(\mathbb{F}_{p^2})$ and $E'(\mathbb{F}_{p^2})$? Observe patterns and make conjectures.
(c) (**) Prove your conjectures from (b). (Hint: It might be helpful to consider the "conjugation" map $\mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$ given by $a \mapsto a^2$. If you don't know much about the fields $\mathbb{F}_{p^2}$ in general, try to attempt this problem for small special cases such as $p = 3$ where $\mathbb{F}_9 \cong \mathbb{F}_3[i] := \mathbb{F}_3[x]/(x^2 + 1)$ or $p = 5$ where $\mathbb{F}_{25} \cong \mathbb{F}_5[\omega] := \mathbb{F}_5[x]/(x^2 + x + 1)$.)

Exercise 2.4.6. Let K be a field and $E \subset \mathbb{P}^2_K$ be an elliptic curve. In §1.12.E, we studied what the group $E[3](\overline{K})$ can look like, where $\overline{K}$ denotes an algebraic closure of K. Perform an analysis similar to the one in §1.12.C to figure out what happens when K is not necessarily algebraically closed. For instance:

(a) Give an example of a field K and an elliptic curve E/K such that $(\#E[3](\overline{K}), \#E[3](K))$ is (i) $(9, 1)$ (ii) $(9, 3)$, (iii) $(9, 9)$, (iv) $(3, 1)$, (v) $(3, 3)$, and (vi) $(1, 1)$.
(b) (**) As done in §1.12.C for two-torsion, classify exactly when each of the possibilities in (a) occurs.
(c) (*) Show that for any field K, there is an extension L/K of degree $[L : K] \leq 8$ such that there is a $P \in E[3](L) \smallsetminus \{\mathcal{O}\}$. Show that if $\operatorname{ch} K = 3$ and E is not supersingular, this can bound can be improved to $[L : K] \leq 3$. Give examples to show that both of these bounds are sharp. (Hint: Look at the proof of 1.12.22 carefully, and use that $8 = 4 \cdot 2$.)

2.4.B PODASIPs

Prove or disprove and salvage if possible the following statements.

Exercise 2.4.7. Let K be a field, and for $\lambda \in K \smallsetminus \{0,1\}$, let

$$j(\lambda) := 2^8 \frac{(\lambda(1-\lambda)+1)^3}{\lambda^2(1-\lambda)^2}.$$

(a) For $\lambda, \lambda' \in K \smallsetminus \{0,1\}$, we have that $j(\lambda) = j(\lambda')$ iff $\lambda' \in S(\lambda)$, where

$$S(\lambda) := \left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, 1-\frac{1}{\lambda}, 1-\frac{1}{1-\lambda}\right\}.$$

(b) For any $\lambda \in K \smallsetminus \{0,1\}$, the set $S(\lambda)$ of (a) has cardinality exactly six.

Exercise 2.4.8. Let K be a field.

(a) For any elliptic curve E over K, there is a(n) (admissible) change of coordinates which brings E into the form $E_\lambda : y^2 = x(x-1)(x-\lambda)$ for some $\lambda \in K \smallsetminus \{0,1\}$. The j-invariant of E_λ is precisely the $j(\lambda)$ of 2.4.7, i.e., $j(E_\lambda) = j(\lambda)$.

(b) For $\lambda, \lambda' \in K \smallsetminus \{0,1\}$, there is an admissible change of coordinates taking E_λ to $E_{\lambda'}$ iff $\lambda' \in S(\lambda)$ iff $j(\lambda) = j(\lambda')$. In particular, the j-invariant classifies elliptic curves up to admissible changes of coordinates (and hence by 1.10.6 up to isomorphism). (Hint: The "change in the x-coordinate alone" would have to send the unordered triple $\{0,1,\lambda\}$ to $\{0,1,\lambda'\}$.)

Exercise 2.4.9. Let K be a field (of any characteristic!). Given any $j \in K$, there is a unique elliptic curve E over K (up to admissible changes of coordinates over K) such that $j(E) = j$.

Exercise 2.4.10. Let K be a field. Given finitely many points $P_i \in \mathbb{P}^2(K)$, there is a line $L \subset \mathbb{P}^2_K$ that doesn't pass through any of the P_i. In particular, up to a linear change of coordinates, we can assume that each P_i lies in $\mathbb{P}^2_K \smallsetminus \mathbb{V}(Z) \cong \mathbb{A}^2_K$.

Exercise 2.4.11. Let K be a field and $E \subset \mathbb{P}^2_K$ an elliptic curve in Weierstrass form.

(a) If $P, Q \in E(K)$ are inflection points, then so is $P * Q$.

(b) If $S \subset E(K)$ is the set of inflection points, then no four points in S are collinear, but any line passing through two points in S passes through a third point in S.

Exercise 2.4.12.

(a) (∗) Suppose $S \subset \mathbb{A}^2(\mathbb{R})$ is a finite set of points with the property that a line passing through any two of them passes through a third. Then S is contained in a line. (Hint: This is just plane geometry; it has nothing to do with elliptic curves.)

(b) If $E \subset \mathbb{P}^2_{\mathbb{R}}$ is an elliptic curve, then exactly three of its nine complex inflection points are real, i.e., even though $\#E[3](\mathbb{C}) = 9$, the subgroup $E[3](\mathbb{R}) \subset E[3](\mathbb{C})$ has size $\#E[3](\mathbb{R}) = 3$. In particular, $E[3](\mathbb{R}) \cong_{\mathsf{Ab}} \mathbb{Z}/3$. (See also 2.2.9.)

Exercise 2.4.13 (Fisher). Let $K = \mathbb{Q}$ and let E be the elliptic curve with Weierstrass equation $y^2 = x^3 + ax^2 + bx$ with $a, b \in \mathbb{Z}$. If $P = (x, y) \in \operatorname{Tors} E(\mathbb{Q}) \smallsetminus \{0\}$, then either $x = 0$ or $x \mid b$ and $x + a + (b/x)$ is a perfect square. (Hint: Review the proof of the Nagell-Lutz Theorem.)

Exercise 2.4.14. Let $E/\mathbb{Q}$ be an elliptic curve given in long Weierstrass form with all coefficients $a_1, \ldots, a_6 \in \mathbb{Z}$.

(a) If $P = (x, y) \in E(\mathbb{Q}) \smallsetminus \{\mathscr{O}\}$, then when expressed as fractions in lowest terms, x and y look like

$$(x, y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$$

for some $m, n, e \in \mathbb{Z}$ with $e \geq 1$ and $\gcd(m, e) = \gcd(n, e) = 1$.

(b) For each prime p and integer $r \in \mathbb{Z}_{\geq 1}$, if we define

$$E_{p,r}(\mathbb{Q}) := \{(x, y) \in E(\mathbb{Q}) \smallsetminus \{\mathscr{O}\} : v_p(x) \leq -2r\} \cup \{\mathscr{O}\},$$

then $E_{p,r}(\mathbb{Q}) \subset E(\mathbb{Q})$ is a subgroup.

In other words, (a) and (b) are saying that the results shown in class are for the short Weierstrass form are also true for the long Weierstrass form, as long as the a_i are integers.

(c) (**) If $P = (x, y) \in \operatorname{Tors} E(\mathbb{Q}) \smallsetminus \{\mathscr{O}\}$, then $x, y \in \mathbb{Z}$. (Hint: Consider $E : y^2 + xy = x^3 + 4x + 1$. For a strong salvage, show that the only thing that can go wrong involves some very small powers of 2. Show also that if $2 \mid a_1$ or if $2P \neq \mathscr{O}$, then $x, y \in \mathbb{Z}$.)

For the next few exercises, we use the following notation: if p is a prime, and $E/\mathbb{F}_p$ an elliptic curve, we let $a_p(E) := p + 1 - \#E(\mathbb{F}_p) \in \mathbb{Z}$. the The integer $a_p(E)$ is called the *trace of Frobenius* associated to the elliptic curve $E/\mathbb{F}_p$. Note that $\#E(\mathbb{F}_p) = p + 1$ iff $a_p(E) = 0$.

Exercise 2.4.15. Let p be a prime other than 2, and let $E : y^2 = f(x)$ be an elliptic curve over $K = \mathbb{F}_p$ in short Weierstrass form.

(a) The integer $a_p(E)$ is congruent mod p to the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$. (Hint: The Legendre symbol and 2.4.4.)

(b) Suppose that $f(x) = x(x-1)(x-\lambda)$ for $\lambda \in \mathbb{F}_p \smallsetminus \{0, 1\}$. The coefficient of x^{p-1} in $f(x)^{(p-1)/2}$ is $h_p(\lambda)$, where $h_p(x) \in \mathbb{F}_p[x]$ is the polynomial defined by

$$h_p(x) := \sum_{i=0}^{(p-1)/2} \binom{(p-1)/2}{i}^2 x^i \in \mathbb{F}_p[x].$$

We have that $h_p(0) \cdot h_p(1) \neq 0$.

Exercise 2.4.16. Fix an integer $b \in \mathbb{Z}$.

(a) For each prime p with $p \nmid 2b$, the equation $y^2 = x^3 + bx$ defines an elliptic curve E_b over $\mathbb{F}_p$. Further,

$$a_p(E_b) \equiv \binom{(p-1)/2}{(p-1)/4} b^{(p-1)/4} \pmod{p}.$$

(b) (**) Further, if $p \geq 5$ and $p \equiv 3 \pmod 4$, then $a_p(E_b) = 0$.

Exercise 2.4.17. Fix an integer $c \in \mathbb{Z}$.

(a) For each prime p, the equation $y^2 = x^3 + c$ defines an elliptic curve E_c over $\mathbb{F}_p$. Further,

$$a_p(E_c) \equiv \binom{(p-1)/2}{(p-1)/3} c^{(p-1)/6} \pmod{p}.$$

(b) (**) Further, if $p \geq 5$ and $p \equiv 2 \pmod 3$, then $a_p(E_c) = 0$.

How do 2.4.17 and 2.4.16 relate to 2.1.8? A possible hint for both 2.4.17(a) and 2.4.16(a): experiment in Sage! A possible hint for 2.4.17(b) and 2.4.16(b): combine your solution to (a) with [8, Theorem V.1.1]. Is there an easier way?

Here are a few more exercises, just for fun.

Exercise 2.4.18. Let K be a field. For $h(x) \in K[x]$ and $n \in \mathbb{Z}_{\geq 0}$, let $h^{(n)}(x)$ denote the n^{th} (formal) derivative of h with respect to x, i.e.,

$$h^{(n)}(x) = \frac{\mathrm{d}^n}{\mathrm{d}x^n} h(x) \in K[x].$$

Let $\overline{K}$ be an algebraic closure of K, and suppose there is an $\alpha \in \overline{K}$ such that $h^{(n)}(\alpha) = 0$ for all $n \geq 0$. Then h is the zero polynomial, i.e., $h(x) = 0 \in K[x]$. In other words, if $h(x) \in K[x]$ is not the zero polynomial, then for each $\alpha \in \overline{K}$, there is some $n \in \mathbb{Z}_{\geq 1}$ such that $h^{(n)}(\alpha) \neq 0$. (Hint: For a strong salvage, consider the case in which either $\operatorname{ch} K = 0$ or $\operatorname{ch} K = p > \deg h$. It may help to "translate" so that $\alpha = 0$.)

Exercise 2.4.19. Let K be a field. A *linear differential operator* $\mathscr{D}$ *of degree* $n \in \mathbb{Z}_{\geq 1}$ is an expression of the form

$$\mathscr{D} = c_0(x)\frac{\mathrm{d}^n}{\mathrm{d}x^n} + c_1(x)\frac{\mathrm{d}^{n-1}}{\mathrm{d}x^{n-1}} + \cdots + c_{n-1}(x)\frac{\mathrm{d}}{\mathrm{d}x} + c_n(x),$$

where $c_0(x), c_1(x), \ldots, c_n(x) \in K[x]$ and $c_0(x) \neq 0$.

(a) Given a differential operator $\mathscr{D}$ and a polynomial $h(x) \in K[x]$, describe what it means to "apply $\mathscr{D}$ to h" to get the polynomial $(\mathscr{D}h)(x) \in K[x]$. The resulting map $\mathscr{D} : K[x] \to K[x]$ is K-linear.

(b) Suppose $\mathscr{D}$ as above is a differential operator of order $n \in \mathbb{Z}_{\geq 1}$ and suppose $h(x) \in K[x]$ is a nonzero polynomial killed by $\mathscr{D}$, i.e., such that $(\mathscr{D}h)(x) = 0 \in K[x]$. If $\overline{K}$ is an algebraic closure of K and $\alpha \in \overline{K}$ a root of $h(x)$ of multiplicity at least n, then $c_0(\alpha) = 0$. (Hint: 2.4.18.)

Exercise 2.4.20. Let p be a prime other than 2, and let $h_p(x) \in \mathbb{F}_p[x]$ be the polynomial defined in 2.4.15.

(a) Let $\mathscr{D}$ be the *Picard-Fuchs differential operator*

$$\mathscr{D} := 4x(1-x)\frac{\mathrm{d}^2}{\mathrm{d}x^2} + 4(1-2x)\frac{\mathrm{d}}{\mathrm{d}x} - 1.$$

We have that $(\mathscr{D}h_p)(x) = 0 \in \mathbb{F}_p[x]$.

(b) The polynomial $h_p(x) \in \mathbb{F}_p[x]$ is separable, i.e., has no repeated roots in $\overline{\mathbb{F}}_p$. In particular, there are exactly $(p-1)/2$ elements $\lambda \in \overline{\mathbb{F}}_p \smallsetminus \{0, 1\}$ such that $h_p(\lambda) = 0$.

The following result might explain why this problem is worth considering and potentially motivate you to attempt it: the curve $E : y^2 = x(x-1)(x-\lambda)$ over $\overline{\mathbb{F}}_p$ is supersingular iff $h_p(\lambda) = 0$ ([8, Theorem V.4.1(b)]). This in turn allows us to count the number of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ up to isomorphism.