2.2 Exercise Sheet 2

Make sure to finish all the exercises from Sheet 1 that you did not get to in the first week (e.g., 2.1.9) too!

2.2.A Numerical and Exploration

Exercise 2.2.1. For any $n \in \mathbb{Z}_{\geq 0}$ and prime p, how many points does $\mathbb{P}^n(\mathbb{F}_p)$ have? Draw a picture of $\mathbb{P}^1(\mathbb{F}_3)$. Draw a picture of $\mathbb{P}^1(\mathbb{F}_p)$ for any $p \geq 2$. Draw a picture of $\mathbb{P}^2(\mathbb{F}_2)$, including all lines on it, and capturing all the incidence relations between points and lines. (Does this picture remind you of something magical?)

Exercise 2.2.2. When does a (projective linear) change of coordinates fix the line at infinity ($Z = 0$) as a set? When does it fix it pointwise? When does it fix the line $Z = 0$ as a set, and fix the point $[0 : 1 : 0]$ on it?

Exercise 2.2.3. Let $K = \mathbb{R}$, let $b, c \in \mathbb{R}$ with $\Delta = -16(4b^3 + 27c^2) \neq 0$, and let E be the elliptic curve with Weierstrass equation $y^2 = x^3 + bx + c$.

(a) When does $E(\mathbb{R})$ consist of one connected component? When does it consist of two connected components?[2] (Hint: What does this have to do with Exercise 2.1.1?)
(b) Consider the curve with $(b, c) = (-21, -20)$. How many connected components does $E(\mathbb{R})$ have? Take the point $P := (-3, 4) \in E(\mathbb{R})$. Get Sage to compute (and maybe even plot!) the points nP for $n = 0, 1, \ldots, 10$. Which component does each of these points lie on? Observe patterns, and make and prove conjectures.
(c) Repeat the same procedure as in (b) for more elliptic curves over $\mathbb{R}$ with two components.

Exercise 2.2.4. Let K be a field with $\operatorname{ch} K \neq 3$, and let $\alpha \in K$, and let

$$E_\alpha = \mathbb{V}(X^3 + Y^3 - \alpha Z^3) \subset \mathbb{P}^2_K.$$

(a) Show that if $\alpha \neq 0$, then E_α is smooth. (What happens when $\operatorname{ch} K = 3$?)

    Hence suppose that $\alpha \neq 0$.

(b) Given a point $P_0 = (x_0, y_0) \in E_\alpha(K)$, find a formula for the point $P_1 = (x_1, y_1)$ obtained by the same "chord and tangent process" as in the Bachet example (1.1.6): draw the tangent line, and then take the third point of intersection with E_α. This procedure gives a way to produce an infinite sequence of points $P_n \in E_\alpha(K)$ as before. (Hint: Your final formula should be quite elegant.)
(c) A point $P_0 \in E_\alpha(K)$ is said to be *exceptional* if the set $\{P_0, P_1, \ldots\}$ is finite; in other words, when the "chord and tangent process" only gets you finitely many points. Find at least one exceptional point on E_α for any α. When $K = \mathbb{Q}$ and $\alpha = 1, 2$, find some more exceptional points.
(d) $(*)$ Suppose now that $K = \mathbb{Q}$ and that $\alpha \geq 1$ is a cube-free integer. Use your answer to (b) to show that the only exceptional points on E_α are the ones you found in (c).
(e) Using the discussion from 1.2.B or otherwise, compute the j-invariant $j(E_\alpha)$ as a function of α.
(f) Finally, suppose now that $K = \mathbb{F}_p$ for primes $p \neq 3$. Using Sage, compute $\#E_1(\mathbb{F}_p)$ for all primes p with $5 \leq p \leq 1000$. What patterns do you observe? Make and prove conjectures. (Hint: Consider the cases $p \equiv 1, 2 \pmod 3$ separately.)

2.2.B PODASIPs

Prove or disprove and salvage if possible the following statements.

Exercise 2.2.5. For any $b \in \mathbb{Z}$, the polynomial $x^3 + bx + 1 \in \mathbb{Q}[x]$ is irreducible, i.e., does not factor into two polynomials of smaller degree. The same is true for $x^3 + bx - 1$. (Hint: What does this have to do with this course? A result we talked about very early on may help.)

Exercise 2.2.6. Let K be a field, $F \in K[X, Y, Z]$ a homogeneous polynomial, $D = \mathbb{V}(F) \subset \mathbb{P}^2_K$. Let L/K be a field extension and $P = (x_0, y_0) = [x_0 : y_0 : 1] \in D(L)$.

[2] What's a connected component?

(a) Let $f(x,y) := F(x,y,1) \in K[x,y]$ denote the dehomogenization of F with respect to Z, and $C = D^\circ = \mathbb{V}(f) \subset \mathbb{A}^2_K$ the corresponding affine curve. Then $(x_0, y_0) \in C(L)$ is a smooth point of the affine curve C iff $[x_0 : y_0 : 1] \in D(L)$ is a smooth point of the projective curve D. Further, the projective tangent line $\mathbb{T}_P(D)$ is the projective closure of the affine tangent line $\mathrm{T}_P(C)$, i.e., $\mathbb{T}_P(D) = \overline{\mathrm{T}_P(C)}$.

(b) Suppose that $\varphi : \mathbb{P}^2_K \to \mathbb{P}^2_K$ is a projective linear change of coordinates. Then P is a smooth point of D iff $\varphi(P)$ is a smooth point of $\varphi(D)$, in which case we have $\varphi(\mathbb{T}_P D) = \mathbb{T}_{\varphi(P)}\varphi(D)$. (What is $\varphi(D)$?)

Exercise 2.2.7.

(a) Let K be a field and $D \subset \mathbb{P}^2_K$ a curve. Suppose that $P \in D(K)$ is a singular point. Then for any line L passing through P, we have that $m_P(D, L) \geq 2$, i.e., L intersects D in multiplicity at least 2 at P.

(b) (**) (This might require a little Galois theory, so if you haven't seen that, you can skip this part.) Suppose $D \subset \mathbb{P}^2_K$ is an integral cubic curve. Suppose that L/K is a field extension, and that $P \in D(L)$ is a singular point. Then in fact $P \in D(K)$. (Hint: See 1.5.5 which might suggest you look only at perfect K. Next, consider the cubic $\mathbb{V}(X^3+XY^2+Y^3+X^2Z+XYZ+Y^2Z+Z^3) \subset \mathbb{P}^2_{\mathbb{F}_2}$ or the cubic $\mathbb{V}(X^3-3XY^2-Y^3-3X^2Z-3XYZ-3Y^2Z+3Z^3) \subset \mathbb{P}^2_{\mathbb{Q}}$. Finally, for a very strong salvage, consider the case of *geometrically* integral D (e.g., a D in Weierstrass form) over a perfect field K. Here "geometrically integral" means that D remains integral over an algebraic closure $\overline{K}$ of K. If it makes things easier for you, you may suppose that L/K is finite.)

Exercise 2.2.8. (Adapted from [2, Exercise 2.13].) Let K be a field of characteristic other than 2, let $t \in K$, and consider the cubic $E_t \subset \mathbb{P}^2_K$ defined as the projective closure of the affine curve

$$y^2 = x^3 - (2t-1)x^2 + t^2 x.$$

(a) The curve E_t is nonsingular iff $t \notin \{0, 1/4\}$, in which case E_t is an elliptic curve over K in Weierstrass form. What is $j(E_t)$ as a function of t?

(b) In the situation in (a), the point $(t,t) \in E(K)$ has order 4.

(c) If $E \subset \mathbb{P}^2_K$ is any elliptic curve over a field K of characteristic other than 2 such that there is a point $P \in E(K)$ of order 4, then there is a projective linear change of coordinates $\varphi : \mathbb{P}^2_K \to \mathbb{P}^2_K$ and a $t \in K \smallsetminus \{0, 1/4\}$ such that $\varphi(E) = E_t$ and $\varphi(P) = (t,t)$.

(d) For a given (E,P) as in (c), the t found in (c) is unique. (Possible salvage: How many values of t work?)

Exercise 2.2.9. Let $R := \mathbb{Z}[a,b,c]$ be the polynomial ring in the variables a,b,c. Take the polynomial $f = f(x) = x^3 + ax^2 + bx + c \in R[x]$, and let $f'(x) = 3x^2 + ax + b$ and $f''(x) = 6x + a$ be the first and second formal derivatives of f with respect to x. The equation $y^2 = f(x)$ defines an elliptic curve E in Weierstrass form over $K = \mathbb{Q}(a,b,c)$, or over any field K of characteristic other than 2 when given specific $a,b,c \in K$ such that $\Delta \neq 0$ in K, which happens iff f and f' have no common roots over an algebraic closure.

(a) Let $f_3(x) := 2f(x)f''(x) - f'(x)^2$. Compute $f_3(x)$ explicitly as an element of $R[x]$. What is the degree of $f_3(x)$? What is its leading coefficient?

(b) PODASIP: For any field K and $P = (x,y) \in E(K) \smallsetminus \{\mathscr{O}\}$, the point P has order 3 (i.e., $3P = \mathscr{O}$, i.e., $P \in E[3](K)$) iff $f_3(x) = 0$. (Possible hints: $3P = \mathscr{O}$ is equivalent to $2P = -P$. Alternatively, think about inflection points. Can you check that

$$\frac{\mathrm{d}^2 y}{\mathrm{d}x^2} = \frac{f_3(x)}{4yf(x)}?$$

What does the second derivative have to do with inflection points?)

(c) PODASIP: For any field K, given $a,b,c \in K$ with $\Delta \neq 0$, the polynomial $f_3(x) \in K[x]$ never has repeated roots. (Hint: What is $f_3'(x)$? How many roots can this share with $f_3(x)$?)

(d) How many roots can it have in K when (i) $\operatorname{ch} K = 3$, (ii) when $K = \mathbb{R}$, (iii), when K is algebraically closed of characteristic other than 3? What implications does this have for the group $E[3](K)$ for various K as above? Specifically, for $K = \mathbb{R}$:

(e) Suppose $K = \mathbb{R}$, and $a,b,c \in \mathbb{R}$ are such that $\Delta \neq 0$. Then $f_3(x) \in \mathbb{R}[x]$ has exactly two real roots, say $\alpha < \beta$. We have $f(\alpha) < 0$ and $f(\beta) > 0$. In particular, $E[3](\mathbb{R})$ is cyclic of order 3.

Here's a real challenge.

Exercise 2.2.10 (Division Polynomials)**.** (**) (Adapted from [5, Exercise 2.6.10].) Let's generalize 2.2.9. For simplicity, we'll do it assuming $a = 0$. Let $R := \mathbb{Z}[b, c]$ be the polynomial ring in two variables b, c. Take the polynomial $f = f(x) = x^3 + bx + c \in R[x]$, and let $f'(x) = 3x^2 + b$ and $f''(x) = 6x$ be the first and second formal derivatives of f with respect to x.

(a) Define the sequence $(f_n)_{n \geq 0}$ of polynomials in $R[x]$ recursively by $f_0 = 0, f_1 = f_2 = 1$,

$$\begin{aligned} f_3 &:= 2f \cdot f'' - (f')^2, \\ f_4 &:= -16f^2 + 4f \cdot f' \cdot f'' - 2(f')^3, \\ f_{2n+1} &:= f_{n+2} \cdot f_n^3 - 16f^2 \cdot f_{n-1} \cdot f_{n+1}^3 \quad \text{for } n \geq 2 \text{ odd}, \\ f_{2n+1} &:= 16f^2 \cdot f_{n+2} \cdot f_n^3 - f_{n-1} \cdot f_{n+1}^3 \quad \text{for } n \geq 2 \text{ even, and} \\ f_{2n} &:= f_n(f_{n+2} \cdot f_{n-1}^2 - f_{n-2} \cdot f_{n+1}^2) \quad \text{for } n \geq 3. \end{aligned}$$

For $n \geq 1$, we have

$$f_n = \begin{cases} nx^{(n^2-1)/2} + \cdots, & \text{for } n \text{ odd, and} \\ (n/2)x^{(n^2-4)/2} + \cdots, & \text{for } n \text{ even,} \end{cases}$$

where $\cdots$ denotes terms of lower degree. Get Sage to write down the polynomials f_n for $n \leq 5$ explicitly.

(b) The equation $y^2 = f(x)$ defines an elliptic curve E in Weierstrass form (over $K = \mathbb{Q}(b, c)$ or over any field K of characteristic other than 2 when given specific $b, c \in K$ such that $4b^3+27c^2 \neq 0 \in K$). In this case,

$$\gcd(f_n, f \cdot f_{n+1} \cdot f_{n-1}) = (1)$$

when n is odd and

$$\gcd(f \cdot f_n, f_{n+1} \cdot f_{n-1}) = (1)$$

when $n \geq 2$ is even.

(c) If $P = (x, y) \in E(K)$, then the coordinates of $nP \in E(K)$ are given as

$$nP = \left(x - \frac{4 \cdot f \cdot f_{n+1} \cdot f_{n-1}}{f_n^2}, y \cdot \frac{f_{2n}}{f_n^4} \right)$$

when n is odd and

$$nP = \left(x - \frac{f_{n+1} \cdot f_{n-1}}{4f \cdot f_n^2}, y \cdot \frac{f_{2n}}{16f^2 \cdot f_n^4} \right)$$

when n is even. (Hint: WOP, of course.)

(d) Now fix an $n \geq 1$, and suppose that K is a field with $\operatorname{ch} K \nmid 2n$.

(1) For $P = (x, y) \in E(K)$, we have $nP = \mathscr{O}$ iff the x-coordinate $x(P)$ of P satisfies $f_n(x) = 0$ when n is odd or satisfies $f(x) \cdot f_n(x) = 0$ when n is even.

(2) When n is odd, the polynomial f_n is separable (i.e., has nonzero discriminant, i.e., has distinct roots over an algebraic closure of K), and when n is even, the polynomial $f \cdot f_n$ is separable.

(3) There are exactly n^2 points of order dividing n in $E(K)$, and, in fact, we have

$$E[n](K) \cong \mathbb{Z}/n \oplus \mathbb{Z}/n.$$

(Hint: If G is an abelian group of order n^2 for some $n \geq 1$ such that for each divisor $d \mid n$ we have $\#G[d] = d^2$, where $G[d] \subset G$ is the subgroup of all points of order dividing d, then $G \cong \mathbb{Z}/n \oplus \mathbb{Z}/n$.)[3]

[3] This result is also true if we only assume $\operatorname{ch} K \nmid n$, but the proof is harder. We might do it in class if time permits.