2.6 Exercise Sheet 6

2.6.1 Numerical and Exploration

Exercise 2.6.1 (Brianchon's Theorem). Let $C \subset \mathbb{P}^2_k$ be a smooth conic, and $(L_1, \dots, L_6)$ an ordered six-tuple of pairwise distinct lines tangent to it. For $i = 1, \dots, 6$, let $P_i := L_i \cap L_{i+1}$, where $L_7 := L_1$, and for $1 \leq i < j \leq 6$, let M_{ij} denote the line joining P_i and P_j.

(a) Show that the lines M_{14}, M_{25} and M_{36} are concurrent. See Figure 2.3.
(b) How many such distinct configurations can you produce from an unordered set of 6 distinct lines $L_1, \dots, L_6$?
(c) Explore what happens when some of the lines $L_1, \dots, L_6$ "collide"–what theorems can you obtain then?

(Hint: Theorem 1.13.5 and Exercise 2.5.10.)

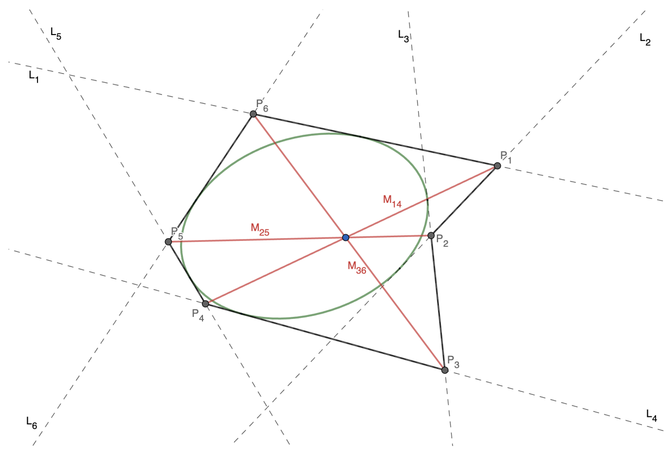

Figure 2.3: Brianchon's Theorem. Picture made with Geogebra.

Exercise 2.6.2. Suppose that k is an algebraically closed field of characteristic other than 2. Show that there are, up to projective changes of coordinates, exactly 8 types of pencils of conics in $\mathbb{P}^2_k$, as described in Example 1.15.7. Explore what happens when k is not algebraically closed or has characteristic 2.

Exercise 2.6.3. Solve, by hand, the quartic equation

$$x^4 - 4x^3 - 22x^2 + 116x - 119 = 0$$

over an arbitrary field k. In other words, given a arbitrary field k, determine how many roots this equation has in k and what are their multiplicities are. (Hint: Example 1.15.11.)

Exercise 2.6.4. Suppose that k is a field of characteristic other than 2 or 3.

(a) For each $\alpha \in k$, let $F_\alpha := X^3 + Y^3 + \alpha Z^3 \in k[X, Y, Z]$, and let $E_\alpha := C_{F_\alpha}$ be the corresponding cubic curve. Show that when $\alpha \neq 0$, the curve E_α is smooth, and so becomes an elliptic curve when equipped with the base point $O = [1 : -1 : 0]$.
(b) Find a projective change of coordinates that brings E_α into Weierstrass normal form, and use this to find $j(E_\alpha) = 0$.
(c) Next, suppose that $k = \mathbb{Q}$. Determine $E_\alpha(\mathbb{Q})$, i.e. the $\mathbb{Q}$-rational points of E_α for $\alpha \in \{\pm 1, \pm 2\}$. Show that if α is an integer other than $\pm 1, \pm 2$, then $E_\alpha(\mathbb{Q})$ is infinite. Conclude that for each integer α other than $\pm 1, \pm 2$, there are infinitely many coprime triples (X, Y, Z) of integers such that $X^3 + Y^3 + \alpha Z^3 = 0$.

(d) Using a computer, determine $\#E_1(\mathbb{F}_p)$, i.e. the number of points on E_1 over the finite field $k = \mathbb{F}_p$ with p elements, for all primes $p \in [5, 1000]$. What patterns do you observe? Make conjectures, and prove them. (Hint: Consider the cases $p \equiv 1, 2 \pmod 3$ separately.)

Exercise 2.6.5. (Adapted from [12, Exercise 1.18].) Consider the elliptic curve E defined in Weierstrass normal form by

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

over $k = \mathbb{Q}$. Note that E contains the rational points

$$Q_1 = (-2, 3), Q_2 = (-1, 4), Q_3 = (2, 5), Q_4 = (4, 9), \text{ and } Q_5 = (8, 23).$$

(a) Show that Q_2, Q_4 and Q_5 can be expressed as $mQ_1 + nQ_2$ for appropriate choices of $m, n \in \mathbb{Z}$.
(b) Compute the points $Q_6 = -Q_1 + 2Q_3$ and $Q_7 = 3Q_1 - Q_3$.
(c) Notice that the points $Q_1, \ldots, Q_7$ and there inverses all have integer coordinates. There is exactly one more rational point Q_8 on this curve that has integer coordinates and $y > 0$. Find it.

If you are up for a real challenge, here are a few more things to think about in this example:

(d) Show the claim made in (c) about the set of all integral points on E.
(e) Show that $E(\mathbb{Q}) \cong \mathbb{Z}^2$, i.e. there are no nontrivial rational torsion points on E and $E(\mathbb{Q})$ has rank 2. Can some two of the above points $Q_1, \ldots, Q_8$ be taken to be two generators for $E(\mathbb{Q})$, and if so, which ones?

Exercise 2.6.6. (Adapted from [12, Exercise 2.13].) Let k be a field of characteristic other than 2, let $t \in k$, and consider the projective closure $E_t \subset \mathbb{P}^2_k$ of the locus defined by

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

(a) Prove that E_t is nonsingular iff $t \notin \{0, 1/4\}$, in which case (E_t, O) is an elliptic curve over k with $O = [0 : 1 : 0]$. What is $j(E_t)$?
(b) Show that, in the situation in (a), the point $(t, t) \in E(k)$ has order 4.
(c) Show that if $E \subset \mathbb{P}^2_k$ is any elliptic curve over a field k of characteristic other than 2 or 3 such that there is a point $P \in E(k)$ of order 4, then there is a projective change of coordinates $\Phi : \mathbb{P}^2_k \to \mathbb{P}^2_k$ such that $\Phi(E) = E_t$ and $\Phi(P) = [t : t : 1]$ for some $t \notin \{0, 1/4\}$.
(d) For a given pair (E, P) as in (c), how many values of t work?

2.6.2 PODASIPs

Prove or disprove and salvage if possible the following statements.

Exercise 2.6.7. If k is a field, and $S \subset \mathbb{P}^2_k$ a finite subset, then there is a line $L \subset \mathbb{P}^2_k$ such that $S \cap L = \emptyset$, i.e. in projective space, a line can be chosen that avoids any finite set of points. Can we produce two such lines L_1, L_2? Can we produce n such lines for any $n \geq 1$? Can we produce infinitely many?

Exercise 2.6.8. Every connected component of a real elliptic curve is a subgroup of it under the elliptic curve addition law. A real elliptic curve is isomorphic as a group (in fact, as a Lie group[10]) to the circle group $S^1 := \{z \in \mathbb{C} : |z| = 1\}$.

Exercise 2.6.9. Let $E \subset \mathbb{P}^2_k$ be a smooth cubic curve, and let $O, O' \in E$ be two points. There is a projective change of coordinates $\Phi : \mathbb{P}^2_k \to \mathbb{P}^2_k$ such that $\Phi(E) = E$ and $\Phi(O) = \Phi(O')$; in

[10] What's that?

particular, as abelian groups, $(E, O) \cong (E, O')$. (Hint: For a very strong salvage, consider the map $\alpha : E \to E$ defined as follows. Let $L_{O,O'}$ intersect E in the third point T, and consider the map $\alpha : E \to E$ which sends a $P \in E$ to the third intersection point of the line $L_{P,T}$ with E.)

Finally, here are a couple more really challenging exercises to keep you occupied all (the rest of) summer.

Exercise 2.6.10 (Division Polynomials). Let $R := \mathbb{Z}[p, q]$ be the polynomial ring in two variables p, q. Take the polynomial $f := x^3 + px + q \in R[x]$, and let $f' = 3x^2 + p$ and $f'' = 6x$ 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.

(b) The equation $y^2 = f$ defines an elliptic curve E in Weierstrass normal form (over $k = \mathbb{Q}(p, q)$ or over any field k of characteristic other than 2 when given specific $p, q \in k$ such that $4p^3 + 27q^2 \neq 0 \in k$). 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 $P = (x, y) \in E$, then the coordinates of $nP \in E$ 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.

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

(1) For $P = (x, y) \in E$, we have $nP = O$ 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, and when n is even, the polynomial $f \cdot f_n$ is separable (Exercise 2.2.10).

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

$$E[n] \cong \mathbb{Z}/n \times \mathbb{Z}/n.$$

(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 $G \cong \mathbb{Z}/n \times \mathbb{Z}/n$.)

(e) Now suppose that $p, q \in \mathbb{R}$. How many real roots can $f_3(x) \in \mathbb{R}[x]$ have? Use this to give another solution to Exercise 2.5.5(e).

Exercise 2.6.11 (Elliptic Divisibility Sequences). (Adapted from [9, Exercises 3.34-3.36].) Let k be a field. A (nondegenerate) elliptic divisibility sequence (EDS) over k is a sequence $a = (a_n)_{n \geq 1}$ defined by four initial parameters a_1, a_2, a_3, a_4 with $a_1 a_2 a_3 \neq 0$ subject to the recursive relations

$$\begin{aligned} a_{2n+1} &= \frac{1}{a_1^3}\left(a_{n+2}a_n^3 - a_{n-1}a_{n+1}^3\right), \text{ and} \\ a_{2n} &= \frac{1}{a_1^2 a_2} a_n (a_{n+2}a_{n-1}^2 - a_{n-2}a_{n+1}^2) \end{aligned}$$

for all $n \geq 2$.

(a) The sequence a defined by $a_n = n$ is an EDS. The sequence a defined by $a_n = F_n$, where F_n is the n^{th} Fibonacci number, is an EDS. More generally, given $a_1, a_2, x, y \in k$, the sequence a defined by the linear recursive relation

$$a_n = x a_{n-1} + y a_{n-2}$$

for $n \geq 2$ is an EDS.

(b) If $(a_n)_{n \geq 1}$ is an EDS, then for each $m \geq 1$ such that $a_m \neq 0$, so is the sequence $(a_{mn}/a_m)_{n \geq 1}$. An EDS such that $a_1 = 1$ is said to be normalized; given any sequence a we define its normalization $\tilde{a}$ to be given by $\tilde{a}_n = a_n/a_1$ for $n \geq 1$. Given a normalized EDS $(a_n)_{n \geq 1}$, we define its discriminant to be

$$\Delta := a_4 a_2^{15} - a_3^3 a_2^{12} + 3a_4^2 a_2^1 0 - 20 a_4 a_3^3 a_2^7 + 3a_4^3 a_2^5 + 16 a_3^6 a_2^4 + 8 a_4^2 a_3^2 a_2^2 + a_4^4.$$

We say that a EDS is singular if the discriminant of its normalization is zero; else it is said to be nonsingular. Which of the sequences from (a) are nonsingular?

(c) Let $E : y^2 = x^3 + px + q$ be an elliptic curve over k, and let $P = (x_0, y_0) \in E(k)$. The sequence $a = (a_n)_{n \geq 1}$ defined by

$$a_n = \begin{cases} f_n(x_0) & n \text{ odd, and} \\ 2y_0 \cdot f_n(x_0), & n \text{ even,} \end{cases}$$

is an EDS, where the polynomials f_n are as in Exercise 2.6.10. What is the discriminant of (the normalization of) this sequence a_n? Is this sequence singular?

(d) The sequence $a = (a_n)_{n \geq 1}$ is an EDS iff for each $m > n > r > 0$, we have

$$a_{m+n} a_{m-n} a_r^2 = a_{m+r} a_{m-r} a_n^2 - a_{n+r} a_{n-r} a_m^2.$$

(e) Now suppose that $k = \operatorname{Frac} R$ for some integral domain R, and let $a = (a_n)$ be an EDS over k such that $a_1, a_2, a_3, a_4 \in R$ and such that $a_1 \mid a_i$ for $i = 2, 3, 4$ and $a_2 \mid a_4$. Then a is a divisibility sequence in the sense that each $a_n \in R$ and if $m, n \geq 1$ are integers, then

$$m \mid n \Rightarrow a_n \mid a_m.$$

If, further, R is a PID and $\gcd(a_3, a_4) = 1$, then for all $m, n \geq 1$ we have

$$a_{\gcd(m,n)} = \gcd(a_m, a_n),$$

up to units. In particular, these properties hold for the Fibonacci sequence F_n.

(f) Finally suppose that $k = \mathbb{Q}$. Suppose that a is a nonsingular, non-periodic EDS. Then there is a real number $h > 0$ such that

$$\lim_{n \to \infty} \frac{\log |a_n|}{n^2} = h.$$