SOLUTIONS TO
THE ARITHMETIC OF ELLIPTIC CURVES
BY J. H. SILVERMAN

JUSTIN SCARFY

ABSTRACT. The main motivation of starting on, undertaking of, and (eventually completing of) this project is mostly due to the author's intense appreciation of the subject: ever since Professor Sujatha Ramdorai's introduction to the subject, the author is attracted by its beauty, and also fascinated by its complexity. The author would not have the technicality or the audacity to even begin this project if he had not been inspired by Professor Sujatha Ramdorai's classes on this topic, and hence the first author is very grateful for her guidance throughout the undergraduate years he spent at the University of British Columbia.

1. ALGEBRAIC VARIETIES

Exercise 1.1. *Let $A, B \in \bar{K}$. Characterize the values of A and B for which each of the following varieties are singular. In particular, as (A, B) ranges over $\mathbb{A}^2$, show that the "singular values" lie on a one-dimensional subset of $\mathbb{A}^2$, so "most" values of (A, B) give a nonsingular variety.*

(a) $V : Y^2Z + AXYZ + BYZ^2 = X^3$.

Solution. We see that any singular points on V satisfy:

$$V^{\text{sing}} : AYZ - 3X^2 = 2YZ + AXZ + BZ^2 = Y^2 + AXY + 2BYZ = 0$$

▲

(b) $V : Y^2Z = X^3 + AXZ^2 + BZ^3$.

Solution. We see that any singular points on V satisfy:

$$V^{\text{sing}} : 3X^2 + AZ^2 = -2YZ = 2AXZ + 3BZ^2 = 0$$

▲

Exercise 1.2. *Find the singular point(s) on each of the following varieties. Sketch $V(\mathbb{R})$.*

(a) $V : Y^2 = X^3$ *in* $\mathbb{A}^2$.

Solution.

$$V^{\text{sing}} : 2Y = 3X^2 = 0,$$

therefore V has one singular point, namely $(0, 0)$.
Sketch of $V(\mathbb{R})$: ▲

(b) $V : 4X^2Y^2 = (X^2 + Y^2)^3$ *in* $\mathbb{A}^2$.

Solution.

$$V^{\text{sing}} : 8XY^2 - 3(X^2+Y^2)^2(2X) = 8X^2Y - 3(X^2+Y^2)^2(2Y) = 0$$
$$8XY^2 - 6X(X^2+Y^2)^2 = 8X^2Y - 6Y(X^2+Y^2)^2 = 0,$$

therefore V has one singular point, namely $(0,0)$.
Sketch of $V(\mathbb{R})$: ▲

(c) $V : Y^2 = X^4 + Y^4$ *in* $\mathbb{A}^2$.

Solution.

$$V^{\text{sing}} : 4X^3 = 4Y^3 - 2Y = 0$$

therefore V has one singular point, namely $(0,0)$.
Sketch of $V(\mathbb{R})$: ▲

(d) $V : X^2 + Y^2 = (Z-1)^2$ *in* $\mathbb{A}^3$.

Solution.

$$V^{\text{sing}} : 2X = 2Y = -2(Z-1) = 0$$

therefore V has one singular point, namely $(0,0,1)$.
Sketch of $V(\mathbb{R})$: ▲

Exercise 1.3. *Let $V \subset \mathbb{A}^n$ be a variety given by a single equation as*

$$f(X_1, X_2, \ldots, X_n) = n.$$

Prove that a point $P \in V$ is nonsingular if and only if

$$\dim_{\bar{K}} M_P/M_P^2 = \dim V.$$

[Hint: Let $f = 0$ be the equation of V and define the tangent plane of V at P by

$$T = \left\{ (y_1, \ldots, y_n) \in \mathbb{A}^n : \sum_{i=1}^{n} \Big(\frac{\partial f}{\partial X_i}(P) \Big) y_i = 0 \right\}.$$

Show that the map

$$M_P/M_P^2 \times T \longrightarrow \bar{K}, \qquad (g, y) \longmapsto \sum_{i=1}^{n} \Big(\frac{\partial g}{\partial X_i}(P) \Big) y_i$$

is a well-defined perfect pairing of $\bar{K}$-vector spaces. Now use the fact that $(X_1, X_2, \ldots, X_n) = P \in V$ is a singular point if and only if

$$\frac{\partial f}{\partial X_1}(P) = \cdots \frac{\partial f}{\partial X_n}(P) = 0.]$$

Proof. First suppose $P \in V$ is nonsingular,
Conversely, if

$$\dim_{\bar{K}} M_P/M_P^2 = \dim V.$$

□

Exercise 1.4. *Let $V/\mathbb{Q}$ be the variety*

$$V : 5X^2 + 6XY + 2Y^2 = 2YZ + Z^2.$$

Prove that $V(\mathbb{Q}) = \emptyset$.

Proof. □

Exercise 1.5. *Let $V/\mathbb{Q}$ be the projective variety*

$$V : Y^2 = X^3 + 17,$$

and let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be distinct points of V. Let L be the line through P_1 and P_2.

(a) Show that $V \cap L = \{P_1, P_2, P_3\}$ and express $P_3 = (x_3, y_3)$ in terms of P_1 and P_2.
(b) Calculate P_3 for $P_1 = (-1, 4)$ and $P_2 = (2, 5)$.
(c) Show that if $P_1, P_2 \in V(\mathbb{Q})$, then $P_3 \in V(\mathbb{Q})$.

Proof. □

Exercise 1.6. *Let V be the variety*

$$V : Y^2 Z = X^3 + Z^3.$$

Show that the map

$$\phi : V \longrightarrow \mathbb{P}^2, \qquad \phi = [X^2, XY, Z^2],$$

is a morphism. (Notice that ϕ does not give a morphism $\mathbb{P}^2 \to \mathbb{P}^2$.)

Proof. □

Exercise 1.7. *Let V be the variety*

$$V : Y^2 Z = X^3,$$

and let ϕ be the map

$$\phi : \mathbb{P}^1 \longrightarrow V, \qquad \phi = [S^2 T, S^3, T^3].$$

(a) Show that ϕ is a morphism.
(b) Find a rational map $\phi : V \to \mathbb{P}^1$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity map whenever they are defined.
(c) Is ϕ an isomorphism?

Proof. □

Exercise 1.8. *Let $\mathbb{F}_q$ be a finite field with q elements and let $V \subset \mathbb{P}^n$ be a variety defined over $\mathbb{F}_q$.*

(a) Prove that the q^{th}-power map

$$\phi = [X_0^q, \ldots, X_n^1]$$

is a morphism $\phi : V \to V$. It is called the Frobenius morphism.
(b) Prove that ϕ is one-to-one and onto.
(c) Prove that ϕ is not an isomorphism.
(d) Prove that $V(\mathbb{F}_q) = \{P \in V : \phi(P) = P\}$.

Proof. □

Exercise 1.9. *If $m > n$, prove that there are no nonconstant morphisms $\mathbb{P}^m \to \mathbb{P}^n$. (Hint: Use the dimension theorem [111, I.7.2]).*

Proof. □

Exercise 1.10. *For each prime $p \geq 3$, let $V_p \subset \mathbb{P}^2$ be the variety given by the equation*

$$V_p : X^2 + Y^2 = Z^2.$$

(a) Prove that V_p is isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$ if and only if $p \equiv 1 \mod 4$.

(b) Prove that for $p \equiv 3 \mod 4$, no two of the V_p's are isomorphic over $\mathbb{Q}$.

Proof. □

Exercise 1.11.

(a) Let $f \in K[X_0, \dots, X_n]$ be a homogeneous polynomial, and let

$$V = \{P \in \mathbb{P}^n : f(P) = 0\}$$

be the hypersurface defined by f. Prove that if a point $P \in V$ is singular, then

$$\frac{\partial f}{\partial X_0}(P) = \cdots = \frac{\partial f}{\partial X_n}(P) = 0$$

Thus for hypersurfaces in projective space, we can check for smoothness using homogeneous coordinates.

(b) Let $n \geq 1$, and let $W \subset \mathbb{P}^n$ be a smooth algebraic set, each of whose component varieties has dimension $n - 1$. Prove that W is a variety. (Hint. First use Krull's Hauptidealsatz, to show that W is the zero of a single homogeneous polynomial.)

Proof. □

Exercise 1.12.

(a) Let V/K be an affine variety. Prove that

$$K[V] = \{f \in \bar{K}[V] : f^\sigma = f \text{ for all } \sigma \in G_{\bar{K}/K}\}.$$

(Hint: One inclusion is clear. For the other, choose some polynomial $F \in \bar{K}[X]$ with $F \equiv f \mod I(V)$. Show that the map $G_{\bar{K}/K} \to I(V)$ defined by $\sigma \mapsto F^\sigma - F$ is a 1-cocycle. Now use (B.2.5a) to conclude that there exists a $G \in I(V)$ such that $F + G \in K[X]$.)

(b) Prove that

$$\mathbb{P}^n(K) = \{P \in \mathbb{P}^n(\bar{K} : P^\sigma = P \text{ for all } \sigma \in G_{\bar{K}/K}\}.$$

(Hint: Write $P = [x_0, \dots, x_n]$. If $P = P^\sigma$, then there is a $\lambda_\sigma \in \bar{K}^*$ such that $x_i^\sigma = \lambda_\sigma x_i$ for all $0 \leq i \leq n$. Show that the map $\sigma \mapsto \lambda_\sigma$ gives a 1-cocycle from $G_{\bar{K}/K}$ to $\bar{K}^*$. Now use Hilbert's Theorem to find an $\alpha \in \bar{K}^*$ such that $[\alpha x_0, \dots, \alpha x_n] \in \mathbb{P}^n(K)$.)

(c) Let $\phi : V_1 \to V_2$ be a rational map of projective varieties. Prove that ϕ is defined over K if and only if $\phi^\sigma = \phi$ for every $\sigma \in G_{\bar{K}/K}$. (Hint: Use (a) and (b).)

Proof. □

2. Algebraic Curves

Exercise 2.1. *Let R be a Noetherian local domain that is not a field, let $\mathfrak{M}$ be its maximal ideal, and let $k = R/\mathfrak{M}$ be its residue field. Prove that the following are equivalent:*

(i) *R is a discrete valuation ring.*
(ii) *$\mathfrak{M}$ is principal.*
(iii) $\dim_k \mathfrak{M}/\mathfrak{M}^2 = 1$.

(Note that this lemma was used in (II.1.1) to show that on a smooth curve, the local rings $\bar{K}[C]_P$ are discrete valuation rings.)

Proof. □

Exercise 2.2. *Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves, let $f \in \overline{K}(C_2)^*$, and let $P \in C_1$. Prove that*

$$\operatorname{ord}_P(\phi^* f) = e_\phi(P)\operatorname{ord}_{\phi(P)}(f).$$

Proof. □

Exercise 2.3. *Verify directly that each of the following results from the text is true for the particular case of the curve $C = \mathbb{P}^1$.*

(a) *Prove the two parts of (II.2.6):*
(i)

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi \quad \textit{for all } Q \in \mathbb{P}^1.$$

(ii)

$$\#\phi^{-1}(Q) = \deg_s(\phi) \qquad \textit{for all but finitely many } Q \in \mathbb{P}^1.$$

(b) *Prove the Riemann-Roch theorem (II.5.4) for $\mathbb{P}^1$.*
(c) *Prove Hurwitz's theorem (II.5.9) for a nonconstant separable map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$.*

Proof. □

Exercise 2.4. *Let C be a smooth curve and let $D \in \operatorname{Div}(C)$. Without using the Riemann-Roch theorem, prove the following statements.*

(a) *$\mathcal{L}(D)$ is a $\bar{K}$-vector space.*
(b) *If $\deg D \geq 0$, then*

$$\ell(D) \leq \deg D + 1.$$

Proof. □

Exercise 2.5. *Let C be a smooth curve. Prove that the following are equivalent (over $\bar{K}$):*

(i) *C is isomorphic to $\mathbb{P}^1$.*
(ii) *C has genus 0.*
(iii) *There exists distinct points $P, Q \in C$ satisfying $(P) \sim (Q)$.*

Proof. □

Exercise 2.6. *Let C be a smooth curve of genus one, and fix a base point $P_0 \in C$.*

(a) Prove that for all $P, Q \in C$ there exists a unique $R \in C$ such that

$$(P) + (Q) \sim (R) + (P_0).$$

Denote this point R by $\sigma(P, Q)$.

(b) Prove that the map $\sigma : C \times C \to C$ from (a) makes C into an abelian group with identity element P_0.

(c) Define a map

$$\kappa : C \longrightarrow \operatorname{Pic}^0(C), \qquad P \mapsto \textit{divisor class of } (P) - (P_0).$$

Prove that κ is a bijection of sets, and hence that κ can be used to make C into a group via the rule

$$P + Q = \kappa^{-1}\left(\kappa(P) + \kappa(Q)\right).$$

(d) Prove that the group operations on C defined in (b) and (c) are the same.

Proof. □

Exercise 2.7. *Let $F(X, Y, Z) \in K[X, Y, Z]$ be a homogeneous polynomial of degree $d \geq 1$, and assume that the curve C in $\mathbb{P}^2$ given by the equation $F = 0$ is nonsingular. Prove that*

$$\operatorname{genus}(C) = \frac{(d-1)(d-2)}{2}.$$

(Hint. Define a map $C \to \mathbb{P}^1$ and use (II.5.9).)

Proof. □

Exercise 2.8. *Let $\phi : C_1 \to C_2$ be a nonconstant separable map of smooth curves.*

(a) Prove that $\operatorname{genus}(C_1) \geq \operatorname{genus}(C_2)$.

(b) Prove that if C_1 and C_2 have the same genus g, then one of the following is true:

(i) $g = 0$.

(ii) $g = 1$ and ϕ is unramified.

(iii) $g \geq 2$ and ϕ is an isomorphism.

Proof. □

Exercise 2.9. *Let a, b, c, d be squarefree integers with $a > b > c > 0$, and let C be the curve in $\mathbb{P}^2$ given by the equation*

$$C : aX^3 + bY^3 + cZ^3 + dXYZ = 0.$$

Let $P = [x, y, z] \in C$ and let L be the tangent line to C at P.

(a) Show that $C \cap L = \{P, P'\}$ and calculate $P' = [x', y', z']$ in terms of a, b, c, d, x, y, z.

(b) Show that if $P \in C(\mathbb{Q})$, then $P' \in C(\mathbb{Q})$.

(c) Let $P \in C(\mathbb{Q})$. Choose homogeneous coordinates for P and P' that are integers satisfying $\gcd(x, y, z) = 1$ and $\gcd(x', y', z') = 1$. Prove that

$$|x'y'z'| > |xyz|.$$

(Note the strict inequality.)

(d) Conclude that either $C(\mathbb{Q}) = \emptyset$ or else $C(\mathbb{Q})$ is an infinite set.

(e) $**$ Characterize, in terms of a, b, c, d, whether $C(\mathbb{Q})$ contains any points.

Proof. □

Exercise 2.10. *Let C be a smooth curve. The* <u>*support*</u> *of a divisor $D = \sum n_P(P) \in \operatorname{Div}(C)$ is the set of points $P \in C$ for which $n_p \neq 0$. Let $f \in \bar{K}(C)^*$ be a function such that $\div(f)$ and D have disjoint supports. Then it makes sense to define*

$$f(D) = \prod_{P \in C} f(P)^{n_P}.$$

Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves. Prove that the following two equalities are valid in the sense that if both sides are well-defined, then they are equal.

(a) $f(\phi^* D) = (\phi_* f)(D)$ for all $f \in \bar{K}(C_1)^*$ and all $D \in \operatorname{Div}(C_2)$.
(b) $f(\phi_* D) = (\phi^* f)(D)$ for all $f \in \bar{K}(C_2)^*$ and all $D \in \operatorname{Div}(C_1)$.

Proof. □

Exercise 2.11. *Let C be a smooth curve and let $f, g \in \bar{K}(C)^*$ to be functions such that $\div(f)$ and $\div(g)$ have disjoint support. (See Exercise 2.10.) Prove* <u>*Weil's reciprocity law*</u>

$$f\left(\operatorname{div}(g)\right) = g\left(\operatorname{div}(f)\right)$$

using the following two steps:

(a) Verify Weil's reciprocity law directly for $C = \mathbb{P}^1$.
(b) Now prove it for arbitrary C by using the map $g : C \to \mathbb{P}^1$ to reduce to (a).

Proof. □

Exercise 2.12. *Use the extension of Hilbert's Theorem 90 (B.3.2), which says that*

$$H^1\left(G_{\bar{K}/K}, \operatorname{GL}_n(\bar{K})\right) = 0,$$

to give another proof of (II.5.8.1).

Proof. □

Exercise 2.13. *Let C/K be a curve.*

(a) Prove that the following sequence is exact:

$$1 \longrightarrow K^* \longrightarrow K(C)^* \longrightarrow \operatorname{Div}_K^0(C) \longrightarrow \operatorname{Pic}_K^0(C).$$

(b) Suppose that C has genus one and that $C(K) \neq \emptyset$. Prove that the map

$$\operatorname{Div}_K^0(C) \longrightarrow \operatorname{Pic}_K^0(C)$$

is surjective.

Proof. □

Exercise 2.14. *For this exercise we assume that* $\operatorname{char} K \neq 2$. *Let $f(x) \in K[x]$ be a polynomial of degree $d \geq 1$ with nonzero discriminant, let C_0/K be the affine curve given by the equation*

$$C_0 : y^2 = f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_{d-1} x + a_d,$$

and let g be the unique integer satisfying $d - 3 \leq 2g \leq d - 1$.

(a) *Let C be the closure of the image of C_0 via the map*

$$[1, x, x^2, \ldots, x^{g-1}, y] : C_0 \longrightarrow \mathbb{P}^{g+2}.$$

Prove that C is smooth and that $C \cap \{X_0 \neq 0\}$ is isomorphic to C_0. The curve C is called a <u>hyperelliptic curve</u>.

(b) *Let*

$$f^*(v) = v^{2g+2} f(1/v) = \begin{cases} a_0 + a_1 v + \cdots + a_{d-1} v^{d-1} + a_d v^d & \text{if } d \text{ is even} \\ a_0 v + a_1 v^2 + \cdots + a_{d-1} v^d + a_d v^{d+1} & \text{if } d \text{ is odd} \end{cases}$$

Show that C consists of two affine pieces

$$C_0 : y^2 = f(x) \quad \text{and} \quad C_1 : w^2 = f^*(v),$$

"glued together" via the maps

$$\begin{aligned} C_0 \to C_1, C_1 & \quad \to C_0, \\ (x, y) \mapsto (1/x, y/x^{g+1}), (v, w) & \quad \mapsto (1/v, w/v^{g+1}). \end{aligned}$$

(c) *Calculate the divisor of the differential dx/y on C and use the result to show that C has genus g. Check your answer by applying Hurwitz's formula (II.5.9) to the map $[1, x] : C \to \mathbb{P}^1$. (Note that Exercise 2.7 does not apply, since $C \not\subset \mathbb{P}^2$.)*

(d) *Find a basis for the holomorphic differentials on C. (Hint. Consider the set of differential forms $\{x^i dx/y : i = 0, 1, 2, \ldots\}$. How many elements in this set are holomorphic?)*

Proof. □

Exercise 2.15. *Let C/K be a smooth curve defined over a field of characteristic $p > 0$, and let $t \in K(C)$. Prove that the following are equivalent:*

(i) *$K(C)$ is a finite separable extension of $K(t)$.*

(ii) *For all but finitely many points $P \in C$, the function $t - t(P)$ is a uniformizer at P.*

(iii) *$t \notin K(C)^p$.*

Proof. □

Exercise 2.16. *Let C/K be a curve that is defined over K and $P \in C(K)$. Prove that $K(C)$ contains uniformizers for C at P, i.e., prove that there are uniformizers that are defined over K.*

Proof. □

3. The Geometry of Elliptic Curves

Exercise 3.1. *Show that the polynomials*

$$x^4 - b_4x^2 - 2b_6x - b_8 \qquad \textit{and} \qquad 4x^3 + b_2 + 2b_4x + b_6$$

appearing in the duplication formula (III.2.3d) are relatively prime if and only if the discriminant of the associated Weierstrass equation is nonzero.

Proof. □

Exercise 3.2.

- *(a) Derive a triplication formula, analogous to the duplication formula (III.2.3), i.e., express* $x\left([3]P\right)$ *as a rational function of* $x\left(P\right)$ *and* $a_1, \ldots, a_6$.
- *(b) Use the results from (a) to show that if* $\operatorname{char}(K) \neq 3$*, then* E *has a nontrivial point of order* 3*. Conclude that if* $\gcd(m, 3) = 1$*, then* $[m] \neq [0]$*. (Warning. You'll probably want to use a computer algebra package for this problem.)*

Proof. □

Exercise 3.3. *Assume that* $\operatorname{char}(K) \neq 3$ *and let* $A \in K^*$*. Then Exercise 2.7 tells us that the curve*

$$E : X^3 + Y^3 = AZ^3$$

is a curve of genus one, so together with the point $O = [1, -1, 0]$*, it is an elliptic curve.*

- *(a) Prove that three points on* E *add to* O *if and only if they are collinear.*
- *(b) Let* $P = [X, Y, Z] \in E$*. Prove that the formulas*

$$\begin{aligned} -P &= [Y, X, Z] \\ [2]P &= [-Y(X^3 + AZ^3), X(Y^3 + AZ^3), X^3Z - Y^3Z]. \end{aligned}$$

- *(c) Develop an analogous formula for the sum of two distinct points.*
- *(d) Prove that* E *has* j*-invariant* 0.

Proof. □

Exercise 3.4. *Referring to (III.2.4), express each of the points* $P_2, P_4, P_5, P_6, P_7, P_8$ *in the form* $[m]P_1 + [n]P_3$ *with* $m, n \in \mathbb{Z}$.

Proof. □

Exercise 3.5. *Let* E/K *be given by a singular Weierstrass equation.*

- *(a) Suppose that* E *has a node, and let the tangent lines at the node be*

$$y = \alpha_1 x + \beta_1 \qquad \textit{and} \qquad y = \alpha_2 x + \beta_2.$$

  - *(i) If* $\alpha_1 \in K$*, prove that* $\alpha_2 \in K$ *and*

$$E_{ns}(K) \cong K^*.$$

  - *(ii) If* $\alpha_1 \notin K$*, prove that* $L = K(\alpha_1, \alpha_2)$ *is a quadratic extension of* K*. Note that (a)i tells us that* $E_{ns}(K) \subset E_{ns}(L) \cong L^*$*. Prove that*

$$E_{ns}(K) \cong \left\{ t \in L^* : N_{L/K}(t) = 1 \right\}.$$

(b) Suppose that E has a cusp. Prove that

$$E_{ns}(K) \cong K^+.$$

Proof. □

Exercise 3.6. *Let C be a smooth curve of genus g, let $P_0 \in C$, and let $n \geq 2g+1$ be an integer. Choose a basis $\{f_0, \dots, f_m\}$ for $\mathcal{L}\left(n(P_0)\right)$ and define a map*

$$\phi : [f_0, \dots, f_m] : C \longrightarrow \mathbb{P}^m.$$

(a) Prove that the image $C' = \phi(C)$ is a curve in $\mathbb{P}^m$.
(b) Prove that the map $\phi : C \longrightarrow C'$ has degree one.
(c) $*$ Prove that C' is smooth and that $\phi : C \longrightarrow C'$ is an isomorphism.

Proof. □

Exercise 3.7. *This exercise gives an elementary, highly computational, proof that the multiplication-by-m map has degree m^2. Let E be given by the Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and let b_2, b_4, b_6, b_8 be the usual quantities. (If you're content to work with $\operatorname{char}(K) \neq 2, 3$, you may find it easier to use the short Weierstrass form $E : y^2 = x^3 + Ax + B$.)

We define <u>division polynomials</u> $\psi_m \in \mathbb{Z}[a_1, \dots, a_6, x, y]$ using initial values

$$\begin{aligned}
&\psi_1 = 1, \\
&\psi_2 = 2y + a_1x + a_3, \\
&\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, \\
&\psi_4 = \psi_2 \cdot \left(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)\right),
\end{aligned}$$

and then inductively by the formulas

$$\begin{aligned}
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 && \text{for } m \geq 2, \\
\psi_2\psi_{2m} &= \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^2 && \text{for } m \geq 3.
\end{aligned}$$

Verify that ψ_{2m} is a polynomial for all $m \geq 1$, and then define further polynomials ϕ_m and ω_m by

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1}, \\
4y\omega_m &= \psi_{m-1}^2\psi_{m+2} + \psi_{m-2}\psi_{m+1}^2.
\end{aligned}$$

(a) Prove that if m is odd, then ψ_m, ϕ_m, and $y^{-1}\omega_m$ are polynomials in

$$\mathbb{Z}[a_1, \dots, a_6, x, (2y + a_1x + a_3)^2].$$

and similarly for $(2y)^{-1}\psi_m, \phi_m$, and ω_m if m is even. So replacing $(2y + a_1x + a_3)^2$ by $4x^3 + b_2x^2 + 2b_4x + b_6$, we may treat each of these quantities as a polynomial in $\mathbb{Z}[a_1, \dots, a_6, x]$.

(b) As polynomials in x, show that

$$\begin{aligned}
\phi_m(x) &= x^{m^2} + \text{(lower order terms)}, \\
\psi_m(x)^2 &= m^2x^{m^2-1} + \text{(lower order terms)}.
\end{aligned}$$

(c) *If $\Delta \neq 0$, prove that $\phi_m(x)$ and $\psi_m(x)^2$ are relatively prime polynomials in $K[x]$.*

(d) *Continuing with the assumption that $\Delta \neq 0$, so E is an elliptic curve, prove that for any point $P = (x_0, y_0) \in E$ we have*

$$[m]P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3} \right).$$

(e) *Prove that the map $[m] : E \to E$ has degree m^2.*

(f) *Prove that the function $\psi_n \in K(E)$ has divisor*

$$\operatorname{div}(\psi_n) = \sum_{T \in E[n]} (T) - n^2(O).$$

Thus ψ_n vanishes at precisely the nontrivial n-torsion points and has a corresponding pole at O.

(g) *Prove that*

$$\psi_{n+m}\psi_{n-m}\psi_r^2 = \psi_{n+r}\psi_{n-r}\psi_m^2 - \psi_{m+r}\psi_{m-r}\psi_n^2 \qquad \text{for all } n > m > r.$$

Proof. □

Exercise 3.8.

(a) *Let $E/\mathbb{C}$ be an elliptic curve. We will prove later (VI.5.1.1) that there is a lattice $L \subset \mathbb{C}$ of complex analytic isomorphism of groups $\mathbb{C}/L \cong E(\mathbb{C})$. (N.B. This isomorphism is given by convergent power series, not by rational functions.) Assuming this fact, prove that*

$$\deg[m] = m^2 \qquad \text{and} \qquad E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

(b) *Let K be a field with $\operatorname{char}(K) = 0$ and let E/K be an elliptic curve. Use (a) to prove that $\deg[m] = m^2$. (Hint. If K can be embedded into $\mathbb{C}$, then the result follows immediately from (a). Reduce to this case.)*

Proof. □

Exercise 3.9. *Let E/K be an elliptic curve over a field K with $\operatorname{char}(K) \neq 2, 3$, and fix a homogeneous Weierstrass equation for E,*

$$F(X_0, X_1, X_2) = X_1^2 X_2 - X_0^3 - AX_0X_2^2 - BX_2^3 = 0,$$

i.e., $x = X_0/X_2$ and $y = X_1/X_2$ are affine Weierstraa coordinates. Let $P \in E$.

(a) *Prove that $[3]P = O$ if and only if the tangent line to E at P intersects E only at P.*

(b) *Prove that $[3]P = O$ if and only if the Hessian matrix*

$$\left(\frac{\partial^2 F}{\partial X_i X_j}(P) \right)_{0 \leq i, j \leq 2}$$

has determinant 0.

(c) *Prove that $E[3]$ consists of nine points.*

Proof. □

Exercise 3.10. *Let E/K be an elliptic curve with Weierstrass coordinate function x and y.*

(a) *Show that the map*

$$\phi : E \longrightarrow \mathbb{P}^2, \qquad f = [1, x, y, x^2],$$

maps E isomorphically onto the intersection of two quadric surfaces in $\mathbb{P}^3$. (A quadric surface in $\mathbb{P}^3$ is the zero set of a homogeneous polynomial of degree two.) In particular, if $H \subset \mathbb{P}^3$ is a hyperplane, then $H \cap \phi(E)$ consists of exactly four points, counted with appropriate multiplicities.

(b) *Show that $\phi(O) = [0, 0, 0, 1]$, and that the hyperplane $\{T_0 = 0\}$ intersects $\phi(E)$ at the single point $\phi(O)$ with multiplicity* 4.

(c) *Let $P, Q, R, S \in E$. Prove that $P + Q + R + S = O$ if and only if the four points $\phi(P), \phi(Q), \phi(R), \phi(S)$ are coplanar, i.e., if and only if there is a plane $H \subset \mathbb{P}^3$ such that the intersection $E \cap H$, counted with appropriate multiplicities, consists of the points $\phi(P), \phi(Q), \phi(R), \phi(S)$.*

(d) *Let $P \in E$. Prove that $[4]P = O$ if and only if there exists a hyperplane $H \subset \mathbb{P}^3$ satisfying $H \cap \phi(E) = \{P\}$. If* $\operatorname{char}(K) \neq 2$, *prove that there are exactly* 16 *such hyperplanes, and hence that* $\#E[4] = 16$.

(e) *Continuing with the assumption that* $\operatorname{char}(K) \neq 2$, *prove that there is a $\bar{K}$-linear change of coordinates such that $\phi(E)$ is given by equations of the form*

$$T_0^2 + T_2^2 = T_0T_3 \qquad \textit{and} \qquad T_1^2 + \alpha T_2^2 = T_2T_3.$$

For what value(s) of α do these equations define a nonsingular curve?

(f) *Using the model in (e) and the addition law described in (c), find formulas for $-P$, for $P_1 + P_2$, and for $[2]P$, analogous to the formula given in (III.2.3).*

(g) *What is the j-invariant of the elliptic curve described in (e)?*

Proof. □

Exercise 3.11. *Generalize Exercise 3.10 as follows. Let E/K be an elliptic curve and choose a basis $f_1, \ldots, f_m$ for $\mathcal{L}(m(O))$. For $m \geq 3$, it follows from Exercise 3.6 that the map*

$$\phi : E \longrightarrow \mathbb{P}^{m-1}, \qquad \phi = [f_1, \ldots, f_m],$$

is an isomorphism of E onto its image.

(a) *Show that $\phi(E)$ is a curve of degree m, i.e., prove that the intersection of $\phi(E)$ and a hyperplane consists of m points, counted with approbated multiplicities. (Hint: Find a hyperplane that intersects $\phi(E)$ at the single point $\phi(O)$ and show that it intersects with multiplicity m.)*

(b) *Let $P_1, \ldots, P_m \in E$. Prove that $P_1 + \cdots + P_m = O$ if and only if the points $\phi(P_1), \phi(P_2), \ldots, \phi(P_m)$ lie on a hyperplane. (Note that if some of the P_i;s coincide, then the hyperplane is required to intersect $\phi(E)$ with correspondingly higher multiplicities at such points.)*

(c) $*$ *Let $P \in E$. Prove that $[m]P = O$ if and only if there is a hyperplane $H \subset \mathbb{P}^{m-1}$ satisfying $H \cap \phi(E) = \{P\}$. If* $\operatorname{char}(K) = 0$ *or* $\operatorname{char}(K) > m$, *prove that there are exactly m^2 such points. Use this to deduce that* $\deg[m] = m^2$.

Proof. □

Exercise 3.12. *Let $m \geq 2$ be an integer, prime to* $\operatorname{char}(K)$ *if* $\operatorname{char}(K) > 0$. *Prove that the natural map*

$$\operatorname{Aut}(E) \longrightarrow \operatorname{Aut}(E[m])$$

is injective except for $m = 2$, where the kernel is $[\pm 1]$. (You should be able to prove this directly, without using (III.10.1).)

Proof. □

Exercise 3.13. *Generalize (III.4.12) as follows. Let $C/\bar{K}$ be a smooth curve, and let Φ be a finite group isomorphisms from C to itself. (For example, if E is an elliptic curve, then Φ might contain some translations by torsion points and $[\pm 1]$.) We observe that an element $\alpha \in \Phi$ acts on $\bar{K}(C)$ via the map*

$$\alpha^* : \bar{K}(C) \longrightarrow \bar{K}(C), \qquad \alpha^*(f) = f \circ \alpha.$$

- *(a) Prove that there exist a unique smooth curve $C'/\bar{K}$ and a finite separable morphism $\phi : C \to \mathbb{C}'$ such that $\phi^*\bar{K}(C') = \bar{K}(C)^\Phi$ denotes the subfield of $\bar{K}(C)$ fixed by every element of Φ.*
- *(b) Let $P \in C$. Prove that*

$$e_\Phi(P) = \#\{\alpha \in \Phi : \alpha P = P\}.$$

- *(c) Prove that ϕ is unramified if and only if every nontrivial element of Φ has no fixed points.*
- *(d) Express the genus of C' in terms of the genus of C, the number of elements in Φ, and the number of fixed points of elements of Φ.*
- *(e) $*$ Suppose that C is defined over K and that Φ is $G_{\bar{K}/K}$-invariant. The latter condition means that for all $\alpha \in \Phi$ and all $\sigma \in G_{\bar{K}/K}$ we have $\alpha^\sigma \in \Phi$. Prove that it is possible to find C' and ϕ as in (a) such that C' and ϕ are defined over K. Prove further that C is unique up to isomorphism over K.*

Proof. □

Exercise 3.14. *Prove directly the natural map*

$$\operatorname{Hom}(E_1, E_2) \longrightarrow \operatorname{Hom}\left(T_\ell(E_1), T_\ell(E_2)\right)$$

is injective. (Hint: If $\phi : E_1 \to E_2$ satisfies $\phi_\ell = 0$, then $E_1[\ell^n] \subset \ker\phi$ for all $n \geq 1$.) Note that this result is not as strong as (III.7.4).

Proof. □

Exercise 3.15. *Let E_1/K and E_2/K be elliptic curves, and let $\phi : E_1 \to E_2$ be an isogeny of degree m defined over K, where m is prime to $\operatorname{char}(K)$ if $\operatorname{char}(K) > 0$.*

- *(a) Mimic the construction in (III §8) to construct a pairing*

$$e_\phi : \ker\phi \times \ker\hat{\phi} \longrightarrow \mu_m.$$

- *(b) Prove that e_ϕ is bilinear, nondegenerate, and Galois invariant.*
- *(c) Prove that e_ϕ is compatible in the sense that $\psi : E_2 \to E_3$ is another isogeny, then*

$$e_{\psi\circ\phi}(P, Q) = e_\psi(\phi P, Q) \quad \textit{for all } P \in \ker(\psi \circ \phi) \textit{ and } Q \in \ker(\hat{\psi}).$$

Proof. □

Exercise 3.16. *Alternative Definition of the Weil Pairing. Let E be an elliptic curve. We define a pairing*

$$\tilde{e}_m : E[m] \times E[m] \longrightarrow \mu_m$$

as follows: Let $P, Q \in E[m]$ and choose divisors D_P and D_Q in $\operatorname{Div}^0(E)$ that add to P and Q, respectively, i.e., such that $\sigma(D_P) = P$ and $\sigma(D_Q) = Q$, where σ is as in (III.3.4a). Assume further that D_P and D_Q are chosen with disjoint supports. Since P and Q have order m, there are functions $f_P, f_Q \in \bar{K}(E)$ satisfying

$$\operatorname{div}(f_P) = mD_p \quad \text{and} \quad \operatorname{div}(f_Q) = mD_Q.$$

We define

$$\tilde{e}_m = \frac{f_P(D_Q)}{f_Q(D_P)}.$$

(See Exericse 2.10 for the definition of the value of a function at a divisor.)

(a) Prove that $\tilde{e}_m(P, Q)$ is well-defined, i.e., its value depends only on P and Q, independent of the various choices of D_P, D_Q, f_P, and f_Q. (Hint. Use Weil reciprocity, Exercise 2.11.)
(b) Prove that $\tilde{e}_m(P, Q) \in \mu_m$.
(c) $*$ Prove that $\tilde{e}_m = e_m$, where e_m is the Weil pairing defined in (III §8).

Proof. □

Exercise 3.17. *Let $\mathcal{K}$ be a definite quaternion algebra. Prove that $\mathcal{K}$ is ramified at ∞. (Hint. The ring $M_2(\mathbb{R})$ contains zero divisors.)*

Proof. □

Exercise 3.18. *Let E/K be an elliptic curve and suppose that $\mathcal{K} = \operatorname{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra.*

(a) Prove that if $p \neq \infty$ and $p \neq \operatorname{char}(K)$, then $\mathcal{K}$ spots at p (Hint. Use (III.7.4).)
(b) Deduce that $\operatorname{char}(K) > 0$. (This gives an alternative proof of (III.5.6c).)
(c) Prove that $\mathcal{K}$ is the unique quaternion algebra that is ramified at ∞ and $\operatorname{char}(K)$ and nowhere else.
(d) $*$ Prove that $\operatorname{End}(E)$ is a maximal order in $\mathcal{K}$. (Note that unlike number fields, a quaternion algebra may have more than one maximal order.)

Proof. □

Exercise 3.19. *Let $\mathcal{K}$ be a quaternion algebra.*

(a) Prove that $\mathcal{K} \otimes \bar{\mathbb{Q}} \cong M_2(\bar{\mathbb{Q}})$.
(b) Prove that $\mathcal{K} \otimes \mathcal{K} \cong M_4(\mathbb{Q})$. This shows that $\mathcal{K}$ corresponds to an element of order 2 in the Brauer group $\operatorname{Br}(\mathbb{Q})$. (Hint. First show that $\mathcal{K} \otimes \mathcal{K}$ is simple, i.e., has no two-sided ideals. Then prove that the map

$$\mathcal{K} \otimes \mathcal{K} \longrightarrow \operatorname{End}(\mathcal{K}), \qquad a \otimes b \longmapsto (x \mapsto axb),$$

is an isomorphism.)

Proof. □

Exercise 3.20. *Let $\mathcal{K}$ be an imaginary quadratic field with ring of integers $\mathcal{O}$. Prove that the orders of $\mathcal{K}$ are precisely the rings $\mathbb{Z} + f\mathcal{O}$ for integers $f > 0$. The integer f is called the conductor of the order.*

Proof. □

Exercise 3.21. *Let $C/\bar{K}$ be a curve of genus one. For any point $O \in C$, we can associate to the elliptic curve (C, O) its j-invariant $j(C, O)$. This exercise asks you to prove that the value of $j(C, O)$ is independent of the choice of the base point O. Thus we can assign a j-invariant to any curve C of genus one.*

(a) Let (C, O) and (C', O') be curves of genus one with associated base points, and suppose that there is an isomorphism of curves $\phi : C \to C'$ satisfying $\phi(O) = O'$. Prove that $j(C, O) = j(C', O')$. (Hint. The j-invariant, which is defined in terms of the coefficients of a Weiestrass equation, is independent of the choice of the equation.)
(b) Prove that given any two points $O, O' \in C$, there is an automorphism of C taking O to O'.
(c) Use (a) and (b) to conclude that $j(C, O) = j(C, O')$.

Proof. □

Exercise 3.22. *Let C be a curve of genus one defined over K.*

(a) Prove that $j(C) \in K$.
(b) Prove that C is an elliptic curve over K if and only if $C(K) \neq \emptyset$.
(c) Prove that C is always isomorphic, over $\bar{K}$, to an elliptic curve defined over K.

Proof. □

Exercise 3.23. *Deuring Normal Form. The following normal form for a Weierstrass equation is sometimes useful when dealing with elliptic curves over (algebraically closed) fields of arbitrary characteristic.*

(a)
(b)
(c)
(d)

Proof. □

Exercise 3.24. *Proof.* □

Exercise 3.25. *Proof.* □

Exercise 3.26. *Proof.* □

Exercise 3.27. *Proof.* □

Exercise 3.28. *Proof.* □

Exercise 3.29. *Proof.* □

Exercise 3.30. *Proof.* □

Exercise 3.31. *Proof.* □

Exercise 3.32. *Proof.* □

Exercise 3.33. *Proof.* □

Exercise 3.34. *Proof.* □

Exercise 3.35. *Proof.* □

Exercise 3.36. *Proof.* □

4. The Formal Group of an Elliptic Curve

Exercise 4.1. *Proof.* □

Exercise 4.2. *Proof.* □

Exercise 4.3. *Proof.* □

Exercise 4.4. *Proof.* □

Exercise 4.5. *Proof.* □

Exercise 4.6. *Proof.* □

5. Elliptic Curves over Finite Fields

Exercise 5.1. *Proof.* □

Exercise 5.2. *Proof.* □

Exercise 5.3. *Proof.* □

Exercise 5.4. *Proof.* □

Exercise 5.5. *Proof.* □

Exercise 5.6. *Proof.* □

Exercise 5.7. *Proof.* □

Exercise 5.8. *Proof.* □

Exercise 5.9. *Proof.* □

Exercise 5.10. *Proof.* □

Exercise 5.11. *Proof.* □

Exercise 5.12. *Proof.* □

Exercise 5.13. *Proof.* □

Exercise 5.14. *Proof.* □

Exercise 5.15. *Proof.* □

Exercise 5.16. *Proof.* □

Exercise 5.17. *Proof.* □

Exercise 5.18. *Proof.* □

6. Elliptic Curves over $\mathbb{C}$

Exercise 6.1. *Proof.* □

Exercise 6.2. *Proof.* □

Exercise 6.3. *Proof.* □

Exercise 6.4. *Proof.* □

Exercise 6.5. *Proof.* □

Exercise 6.6. *Proof.* □

Exercise 6.7. *Proof.* □

Exercise 6.8. *Proof.* □

Exercise 6.9. *Proof.* □

Exercise 6.10. *Proof.* □

Exercise 6.11. *Proof.* □

Exercise 6.12. *Proof.* □

Exercise 6.13. *Proof.* □

Exercise 6.14. *Proof.* □

Exercise 6.15. *Proof.* □

Exercise 6.16. *Proof.* □

7. Elliptic Curves over Local Fields

Exercise 7.1. *Proof.* □

Exercise 7.2. *Proof.* □

Exercise 7.3. *Proof.* □

Exercise 7.4. *Proof.* □

Exercise 7.5. *Proof.* □

Exercise 7.6. *Proof.* □

Exercise 7.7. *Proof.* □

Exercise 7.8. *Proof.* □

Exercise 7.9. *Proof.* □

Exercise 7.10. *Proof.* □

Exercise 7.11. *Proof.* □

Exercise 7.12. *Proof.* □

Exercise 7.13. *Proof.* □

Exercise 7.14. *Proof.* □

Exercise 7.15. *Proof.* □

8. Elliptic Curves over Global Fields

Exercise 8.1. *Proof.* □

Exercise 8.2. *Proof.* □

Exercise 8.3. *Proof.* □

Exercise 8.4. *Proof.* □

Exercise 8.5. *Proof.* □

Exercise 8.6. *Proof.* □

Exercise 8.7. *Proof.* □

Exercise 8.8. *Proof.* □

Exercise 8.9. *Proof.* □

Exercise 8.10. *Proof.* □

Exercise 8.11. *Proof.* □

Exercise 8.12. *Proof.* □

Exercise 8.13. *Proof.* □

Exercise 8.14. *Proof.* □

Exercise 8.15. *Proof.* □

Exercise 8.16. *Proof.* □

Exercise 8.17. *Proof.* □

Exercise 8.18. *Proof.* □

Exercise 8.19. *Proof.* □

Exercise 8.20. *Proof.* □

Exercise 8.21. *Proof.* □

Exercise 8.22. *Proof.* □

Exercise 8.23. *Proof.* □

9. Integral Points on Elliptic Curves

Exercise 9.1. *Proof.* □

Exercise 9.2. *Proof.* □

Exercise 9.3. *Proof.* □

Exercise 9.4. *Proof.* □

Exercise 9.5. *Proof.* □

Exercise 9.6. *Proof.* □

Exercise 9.7. *Proof.* □

Exercise 9.8. *Proof.* □

Exercise 9.9. *Proof.* □

Exercise 9.10. *Proof.* □

Exercise 9.11. *Proof.* □

Exercise 9.12. *Proof.* □

Exercise 9.13. *Proof.* □

Exercise 9.14. *Proof.* □

Exercise 9.15. *Proof.* □

Exercise 9.16. *Proof.* □

Exercise 9.17. *Proof.* □

Exercise 9.18. *Proof.* □

10. Computing the Mordell-Weil Group

Exercise 10.1. *Proof.* □

Exercise 10.2. *Proof.* □

Exercise 10.3. *Proof.* □

Exercise 10.4. *Proof.* □

Exercise 10.5. *Proof.* □

Exercise 10.6. *Proof.* □

Exercise 10.7. *Proof.* □

Exercise 10.8. *Proof.* □

Exercise 10.9. *Proof.* □

Exercise 10.10. *Proof.* □

Exercise 10.11. *Proof.* □

Exercise 10.12. *Proof.* □

Exercise 10.13. *Proof.* □

Exercise 10.14. *Proof.* □

Exercise 10.15. *Proof.* □

Exercise 10.16. *Proof.* □

Exercise 10.17. *Proof.* □

Exercise 10.18. *Proof.* □

Exercise 10.19. *Proof.* □

Exercise 10.20. *Proof.* □

Exercise 10.21. *Proof.* □

Exercise 10.22. *Proof.* □

Exercise 10.23. *Proof.* □

Exercise 10.24. *Proof.* □

11. Algorithmic Aspects of Elliptic Curves

Exercise 11.1. *Proof.* □

Exercise 11.2. *Proof.* □

Exercise 11.3. *Proof.* □

Exercise 11.4. *Proof.* □

Exercise 11.5. *Proof.* □

Exercise 11.6. *Proof.* □

Exercise 11.7. *Proof.* □

Exercise 11.8. *Proof.* □

Exercise 11.9. *Proof.* □

Exercise 11.10. *Proof.* □

Exercise 11.11. *Proof.* □

Exercise 11.12. *Proof.* □

Exercise 11.13. *Proof.* □

Exercise 11.14. *Proof.* □

Exercise 11.15. *Proof.* □

Exercise 11.16. *Proof.* □

Exercise 11.17. *Proof.* □

Exercise 11.18. *Proof.* □