Algebra & Computation: Elliptic Curves

Talk 2: Group Laws, Torsion, Derivations

Jesko Hüttenhain

Spring 2010

We always assume $k = \overline{k}$ to be an algebraically closed field with $\mathrm{char}(k) \notin \{2, 3\}$. Let E be the elliptic curve over k defined by $Y^2 - X^3 - AX - B$.

1 Derivations

We give a quick introduction to modules of differentials. The results are simplified versions of a more general theory which is treated very well and thoroughly in [Eis94]. Your motivation for this section should be that it will be a *very* handy technical asset.

Definition 1.1. If S is a k-algebra, and M an S-module, a k-vectorspace homomorphism $D : S \to M$ is called a **k-linear derivation** if it satisfies the **Leibniz rule**

$$\forall f, g \in S : \; D(fg) = D(f) \cdot g + f \cdot D(g). \tag{1}$$

We denote by $\mathrm{Der}_k(S, M)$ the S-module of all k-linear derivations from S to M with scalar multiplication defined by $(f \cdot D)(g) := f \cdot D(g)$. We also write $\mathrm{Der}_k(S) := \mathrm{Der}_k(S, S)$.

Fact 1.2. *Let $D \in \mathrm{Der}_k(S)$.*

1. $\forall \lambda \in k : \; D(\lambda) = 0.$
2. $\forall f \in S : \; \forall n \in \mathbb{N} : \; D(f^n) = n \cdot f^{n-1} \cdot D(f).$

Proof. For the first statement, note that

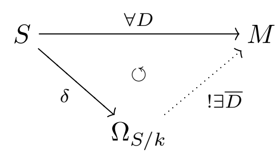
$$D(1) = D(1 \cdot 1) = D(1) + D(1) \quad \Rightarrow \quad D(1) = 0$$

and thus, $D(\lambda) = \lambda \cdot D(1) = 0$. For the second statement, we perform induction on n. In the case $n = 1$, the statement is trivial. Hence,

$$\begin{aligned} D(f^n) &= D(f^{n-1} \cdot f) \\ &= D(f^{n-1}) \cdot f + f^{n-1} \cdot D(f) \\ &= (n-1) \cdot f^{n-2} \cdot D(f) \cdot f + f^{n-1} \cdot D(f) \\ &= n \cdot f^{n-1} \cdot D(f) \end{aligned}$$

verifies our claim. □

Proposition 1.3. *Let S be a k-algebra. Then, there exists an S-module $\Omega_{S/k}$ and a surjective, k-linear derivation $\delta : S \to \Omega_{S/k}$ with the following universal property: For all k-linear derivations $D : S \to M$, there exists a unique homomorphism $\overline{D} : \Omega_{S/k} \to M$ of S-modules such that $D = \overline{D} \circ \delta$.*



The module $\Omega_{S/k}$ is called ***the module of Kähler differentials*** *and δ is called* ***the universal derivation****.*

Proof. We define

$$\Omega_{S/k} := \bigoplus_{f \in S} \delta_f S \Big/ N$$

where δ_f is a formal variable and N is the submodule generated by

1. $\forall f, g \in S : \delta_{fg} - f\delta_g - g\delta_f$
2. $\forall a, b \in k : \forall f, g \in S : \delta_{af+bg} - a\delta_f - b\delta_g$

We then set $\delta(f) := \delta_f$. Since we divided out all relations of the form (2), δ is a k-linear map. By dividing out (1), we forced it to satisfy the Leibniz rule. Thus, δ is actually a derivation. Note that it is also surjective. To check the universal property, let $D : S \to M$ be a derivation.

If $\delta(f) = 0$, then f satisfies one of the relations in (1) or (2), so we also know $D(f) = 0$. This means $\ker(\delta) \subseteq \ker(D)$ and the statement is just the fundamental theorem on homomorphisms. □

Corollary 1.4. *As S-modules, $\mathrm{Der}_k(S, M) \cong \mathrm{Hom}_S(\Omega_{S/k}, M)$.* □

Proposition 1.5. *For $S = k[x_1, \ldots, x_n]$, $\mathrm{Der}_k(S)$ is a free S-module with a basis given by the partial derivatives $\partial_i := \partial/\partial x_i$.*

Proof. Since S is generated as a k-algebra by the x_i, the module of Kaehler differentials $\Omega_{S/k}$ is generated by the $\delta(x_i)$ as an S-module. Thus, there is an epimorphism $\varphi : S^n \twoheadrightarrow \Omega_{S/k}$ defined by sending e_i to $\delta(x_i)$.

Let $d_i : \Omega_{S/k} \to S$ be the S-module homomorphism with $d_i \circ \delta = \partial_i$. Then, the map $d := (d_1, \ldots, d_n) : \Omega_{S/k} \to S^n$ is an inverse for φ since

$$d(\varphi(\alpha_1, \ldots, \alpha_n)) = d(\alpha_1\delta(x_1) + \ldots + \alpha_n\delta(x_n)) = (\alpha_1, \ldots, \alpha_n).$$

Thus, we have

$$\mathrm{Der}_k(S) \cong \mathrm{Hom}_S(\Omega_{S/k}, S) \cong \mathrm{Hom}_S(S^n, S) \cong S^n$$

and under these isomorphisms, $\partial_i \mapsto d_i \mapsto d_i \circ \varphi \mapsto e_i$, verifying our claim. □

Corollary 1.6. *A derivation $D \in \mathrm{Der}_k(k[x_1, \dots, x_n])$ is uniquely defined by the values $D(x_1), \dots, D(x_n)$.* □

Fact 1.7. *If S is an integral k-algebra, then $D \in \mathrm{Der}_k(S)$ extends naturally to a derivation $\mathrm{Q}(S) \to \mathrm{Q}(S)$ by $D(1/g) = -1/g^2 \cdot D(g)$. This yields the formula*

$$D(f/g) = D(f \cdot 1/g) = \frac{D(f) \cdot g - f \cdot D(g)}{g^2} \tag{2}$$

*which is also called the **quotient rule**.*

Proof. Let us first check that this is well-defined. Assuming that $f_1/g_1 = f_2/g_2$, i.e. $f_1 g_2 = f_2 g_1$, we calculate

$$\begin{aligned} D(f_1/g_1) &= \frac{D(f_1) \cdot g_1 - f_1 \cdot D(g_1)}{g_1^2} = \frac{D(f_1)}{g_1} - \frac{f_2}{g_2} \cdot \frac{D(g_1)}{g_1} \\ &= \frac{D(f_1) g_2 - f_2 D(g_1)}{g_1 g_2} \\ &= \frac{D(f_1 g_2) - f_1 D(g_2) - D(f_2 g_1) + D(f_2) g_1}{g_1 g_2} \\ &= \frac{D(f_2) g_1 - f_1 D(g_2)}{g_1 g_2} = \dots = D(f_2/g_2). \end{aligned}$$

It is an equally straightforward computation to verify that D remains a k-vectorspace homomorphism satisfying the Leibniz rule (1). Alternatively, the entire statement follows from the fact that Kähler differentials commute with localization in the sense of [Eis94, Proposition 16.9]. □

Proposition 1.8. *There exists a unique derivation $D \in \mathrm{Der}_k(K(E))$ satisfying*

$$D(x) = 2y \quad \text{and} \quad D(y) = 3x^2 + A \tag{3}$$

Proof. By 1.7, we have to find a $D \in \mathrm{Der}_k(k[x,y])$ satisfying (3). By 1.6, there exists a unique $D' \in \mathrm{Der}_k(k[X,Y])$ with $D(X) = 2Y$ and $D(Y) = 3X^2 + A$. We denote by $\pi : K[X,Y] \twoheadrightarrow k[x,y]$ the canonical projection whose kernel is given by the curve equation, i.e. $\ker(\pi) = \big(Y^2 - X^3 - AX - B\big)$. Since

$$\begin{aligned} D'(Y^2 - X^3 - AX - B) &= D'(Y^2) - D'(X^3) - A \cdot D'(X) \\ &= 2Y \cdot D'(Y) - (3X^2 + A) \cdot D'(X) \\ &= D'(X) \cdot D'(Y) - D'(Y) \cdot D'(X) \\ &= 0 \end{aligned}$$

we get a unique homomorphism $D : k[x,y] \to k[x,y]$ satisfying $D \circ \pi = \pi \circ D'$. Since D' is a derivation, so is D and it is unique with (3). □

Definition 1.9. From now on, we will always write D for the derivation satisfying (3) and call it the **derivation on** E.

Lemma 1.10. *If $f \in k[x,y]$ satisfies $D(f) \neq 0$, then $\deg(D(f)) = \deg(f) + 1$. In particular, the inequality $\deg(D(f)) \leq \deg(f) + 1$ always holds.*

Proof. Certainly this holds for $f = x$ and $f = y$ by (3). Consequently, it holds for polynomials in x and since any polynomial has a canonical representation $f(x,y) = u(x) + y \cdot v(x)$, the general case follows. □

Proposition 1.11. *Let $P \in E$ be any point.*

1. *If r is a rational function which is finite at P, then so is $D(r)$.*

2. *If u is a uniformizer at P, then $D(u)$ is finite and nonzero at P.*

Proof. For $P \neq \mathcal{O}$, part (1) follows from the quotient rule (2). On the other hand, $r(\mathcal{O}) \neq \infty$ means $r = f/g$ with $\deg(f) \leq \deg(g)$. By the quotient rule, we want to show that

$$\deg(D(f)g - fD(g)) \leq \deg(g^2).$$

We distinguish two cases:

Case 1 ($\deg(f) = \deg(g)$)**.** In this case, $D(f) \cdot g$ and $f \cdot D(g)$ have the same leading term. Since we can write both polynomials in a unique normal form, this yields

$$\begin{aligned} \deg(D(f)g - fD(g)) &= \deg(D(f)g) - 1 = \deg(D(f)) + \deg(g) - 1 \\ &\overset{(1.10)}{=} \deg(f) + 1 + \deg(g) - 1 = 2\deg(g) = \deg(g^2). \end{aligned}$$

Case 2 ($\deg(f) \neq \deg(g)$)**.** In this case, we can also use 1.10 to conclude

$$\begin{aligned} \deg(D(f)g - fD(g)) &\leq \max\{\deg(D(f)) + \deg(g),\ \deg(f) + \deg(D(g))\} \\ &\leq \deg(f) + \deg(g) + 1 \leq 2\deg(g) = \deg(g^2). \end{aligned}$$

We now proceed to prove (2). Since there are only three kinds of uniformizers, we can check each one of them individually. If $P = \mathcal{O}$ then $u = x/y$ and

$$D(\,x/y\,) = \frac{D(x)y - xD(y)}{y^2} = \frac{2y^2 - 3x^3 - Ax}{y^2} = \frac{-y^2 - Ax + B}{y^2}$$

evaluates to -1 at $\mathcal{O}$. If $P = (\omega, 0)$ is a point of order two then $u = y$ and

$$D(y)(P) = (3x^2 + A)(P) = \partial_X(X^3 + AX + B)(\omega) \in k^{\times}$$

since E is nonsingular. The final case is where P is none of the above and the uniformizer is given by $u = x - x(P) \Rightarrow D(u) = 2y$. Since P is not of order two, $2y(P)$ is finite and nonzero. □

Corollary 1.12. *Let r be a rational function on E. If $\operatorname{ord}_P(r) = d$ is not a multiple of $\operatorname{char}(k)$, then $\operatorname{ord}_P(D(r)) = d - 1$.*

Proof. Let u be a uniformizer at P and $r = u^d r_1$. Then, r_1 is finite and nonzero at P and

$$\begin{aligned} D(r) = D(u^d \cdot r_1) &= d \cdot u^{d-1} \cdot D(u) \cdot r_1 + u^d \cdot D(r_1) \\ &= u^{d-1} \cdot \underbrace{(d \cdot D(u) \cdot r_1 + u \cdot D(r_1))}_{r_2} \end{aligned}$$

By 1.11, $D(u)(P) \in k^\times$ and $r_1(P) \in k^\times$ by assumption. Since $u(P) = 0$ and d is not a multiple of $\mathrm{char}(k)$, r_2 is finite and nonzero at P. Thus, $D(r) = u^{d-1} r_2$ means that $\mathrm{ord}_P(D(r)) = d - 1$. $\square$

Corollary 1.13. *Let r be a rational function on E which has a zero at P and $j < \mathrm{char}(k) \neq 0$ or $j > \mathrm{char}(k) = 0$. Then, $D^j(r)(P) = 0 \Leftrightarrow \mathrm{ord}_P(r) > j$.*

Remark. In particular, the equivalence holds for all $1 \leq j \leq 4$ by our global assumption on $\mathrm{char}(k)$.

Proof. The statement would follow immediately from 1.12 unless $\mathrm{ord}_P(r)$ is a multiple of $p := \mathrm{char}(k)$. In this case, we claim that both statements are true. Since the order of r at P must be greater than zero, this would mean that $p \neq 0$ and $\mathrm{ord}_P(r) \geq p > j$ by assumption. We write $\mathrm{ord}_P(r) = np$ and pick a uniformizer u at P to write $r = u^{np} s$ with some s that is finite and nonzero at P. Then,

$$D(r) = D(u^{np})s + u^{np} D(s) = p \cdot n u^{np-1} s + u^{np} D(s) = u^{np} D(s)$$

and by 1.8, $D(s)$ is finite and nonzero at P. Thus, $\mathrm{ord}_P(D(r)) = \mathrm{ord}_P(r)$, so $D^j(r)(P) = 0$ holds for all j. $\square$

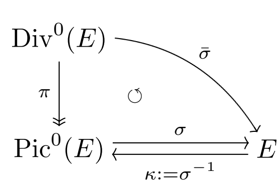
2 The Group Law

In this section, we define a group structure on the points of E and show that it can be given a very profund geometric intuition.

Recall. $\Delta \in \mathrm{Div}^0(E) \Rightarrow \exists!\, P_\Delta \in E$ with $\Delta \sim \langle P_\Delta \rangle - \langle \mathcal{O} \rangle$. The map

$$\begin{aligned} \bar{\sigma} : \mathrm{Div}^0(E) &\longrightarrow E \\ \Delta &\longmapsto P_\Delta \end{aligned}$$

induces a bijection $\sigma : \mathrm{Pic}^0(E) \xrightarrow{\sim} E$,



since $\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\!\sim$. We set $\kappa := \sigma^{-1}$.

Definition 2.1. We define a group law on E by

$$\begin{array}{rcl} E \times E & \longrightarrow & E \\ (P, Q) & \longmapsto & P + Q := \sigma(\kappa(P) + \kappa(Q)) \end{array}$$

In other words, $E = (E, +)$ has the group structure induced by σ. For $Q \in E$, we define the **translation by** Q to be the map $T_Q : E \to E$ defined by $P \mapsto P+Q$. The translation by $-Q$ is an inverse for it.

Fact 2.2. *The neutral element of E is $\sigma(0) = \mathcal{O}$.*

Proof. Follows from $\sigma(0) = \sigma(\pi(0)) = \bar{\sigma}(0) = \mathcal{O}$. □

Lemma 2.3. *Whenever $l(x, y) = \alpha x + \beta y + \gamma$ is a line on E with divisor*

$$\operatorname{div}(l) = \langle P_1 \rangle + \ldots + \langle P_n \rangle - n \langle \mathcal{O} \rangle ,$$

then $P_1 + \ldots + P_n = \mathcal{O}$ in E.

Proof. From the equality $\sigma(\pi(\langle P \rangle - \langle \mathcal{O} \rangle)) = \bar{\sigma}(\langle P \rangle - \langle \mathcal{O} \rangle) = P$, we conclude that $\kappa(P) = \sigma^{-1}(P) = \pi(\langle P \rangle - \langle \mathcal{O} \rangle)$. Thus,

$$\begin{array}{rcl} \kappa(P_1) + \ldots + \kappa(P_n) & = & \pi(\langle P_1 \rangle - \langle \mathcal{O} \rangle) + \ldots + \pi(\langle P_n \rangle - \langle \mathcal{O} \rangle) \\ & = & \pi(\langle P_1 \rangle + \ldots + \langle P_n \rangle - n \langle \mathcal{O} \rangle) \\ & = & \pi(\operatorname{div}(l)) = 0 \end{array}$$

implies that $P_1 + \ldots + P_n = \sigma(0) = \mathcal{O}$ by 2.2. □

Proposition 2.4. *The inverse of $P \in E$ is $-P := (x(P), -y(P))$.*

Proof. Consider the line $l(x, y) := x - x(P)$. It has exactly two zeros on E at P and $-P$. It also has a pole on E at $\mathcal{O}$. We note that

$$u_{\mathcal{O}}^2 \cdot l = (x/y)^2 \cdot (x - x(P)) = \frac{x^2(x - x(P))}{y^2} = \frac{x^3 - x(P) \cdot x^2}{x^3 + Ax + B}$$

evaluates to 1 at $\mathcal{O}$. Hence, $\operatorname{ord}_{\mathcal{O}}(l) = -2$. Thus,

$$\operatorname{div}(l) = \langle P \rangle + \langle -P \rangle - 2 \langle \mathcal{O} \rangle$$

and the claim follows from 2.3. □

Proposition 2.5. *Let $P_1, P_2 \in E \setminus \{\mathcal{O}\}$ such that $P_1 \neq -P_2$ and set $P_3 := P_1 + P_2$. Let $x_i := x(P_i)$ as well as $y_i := y(P_i)$ for $i = 1, 2, 3$. With*

$$\lambda := \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & ; \quad x_1 \neq x_2 \\[2ex] \dfrac{3x_1^2 + A}{2y_1} & ; \quad x_1 = x_2 \end{cases}$$

we then claim that

$$x_3 = \lambda^2 - x_1 - x_2 \quad \text{and} \quad y_3 = \lambda(x_1 - x_3) - y_1. \tag{4}$$

Proof. We define

$$\gamma := \begin{cases} \dfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1} & ; \quad x_1 \neq x_2 \\ \\ y_1 - \lambda x_1 & ; \quad x_1 = x_2 \end{cases}$$

and claim that the line

$$l(x, y) := y - \lambda x - \gamma.$$

has a zero on E at P_1 and P_2. In the case $x_1 \neq x_2$, we check this by calculating

$$(x_2 - x_1) \cdot l(P_1) = y_1(x_2 - x_1) + (y_1 - y_2)x_1 - (y_1 x_2 - y_2 x_1) = 0$$
$$(x_2 - x_1) \cdot l(P_2) = y_2(x_2 - x_1) + (y_1 - y_2)x_2 - (y_1 x_2 - y_2 x_1) = 0$$

Since $x_1 = x_2$ implies $y_1 = y_2$ by our assumption $P_1 \neq -P_2$, the second case is trivial. Intuitively speaking, l is the line through P_1 and P_2. For $P_1 = P_2$, it is the tangent to E at that point.

Our first goal is to show that

$$\exists R \in E: \ \operatorname{div}(l) = \langle P_1 \rangle + \langle P_2 \rangle + \langle R \rangle - 3 \langle \mathcal{O} \rangle \tag{5}$$

For $P_1 \neq P_2$, the above is obvious since $\deg(l) = 3$. For $P := P_1 = P_2$, we have to show that $\operatorname{ord}_P(l) \geq 2$. This follows from 1.13 because

$$\begin{aligned} D(l) &= D((y - y_1) - \lambda(x - x_1)) \\ &= 3x^2 + A - 2\lambda y \\ &= (3x^2 + A) - (3x_1^2 + A) \cdot (y/y_1) \end{aligned}$$

implying $D(l)(P) = 0$.

From (5), we can now conclude that $P_1 + P_2 = -R$ by virtue of 2.3. Thus, $P_3 = -R$ and this means $R = (x_3, -y_3)$ by 2.4. The x-coordinates of P_1, P_2 and $-P_3$ are the roots of

$$g(X) := X^3 + AX + B - (\lambda X + \gamma)^2$$

which means $g(X) = c(X - x_1)(X - x_2)(X - x_3)$. Comparing coefficients, we immediately conclude $c = 1$ and $x_1 + x_2 + x_3 = \lambda^2$. This verifies the first part of (4). The second part follows because $l(x_3, -y_3) = 0$ implies

$$y_3 = -\lambda x_3 - \gamma = \lambda(x_1 - x_3) - \lambda x_1 - \gamma = \lambda(x_1 - x_3) - y_1$$

□

Fact 2.6. *The linear coefficient λ in 2.5 can always be expressed as*

$$\lambda := \frac{x_2^2 + x_1 x_2 + x_1^2 + A}{y_1 + y_2}$$

Proof. For $x_1 = x_2 \Rightarrow y_1 = y_2$, this is obvious. On the other hand,

$$\begin{aligned} \frac{y_2 - y_1}{x_2 - x_1} &= \frac{y_2 - y_1}{x_2 - x_1} \cdot \frac{y_2 + y_1}{y_2 + y_1} = \frac{y_2^2 - y_1^2}{(x_2 - x_1)(y_2 + y_1)} \\ &= \frac{(x_2^3 - x_1^3) + A(x_2 - x_1)}{(x_2 - x_1)(y_2 + y_1)} = \frac{x_2^2 + x_1 x_2 + x_1^2 + A}{y_1 + y_2} \end{aligned}$$

verifies the formula in the case $x_2 \neq x_1$. □

Definition 2.7. We define a map sum : $\mathrm{Div}(E) \to E$ by

$$\sum_{P \in E} n_P \langle P \rangle \quad \longmapsto \quad \sum_{P \in E} n_P \cdot P$$

which means $\mathrm{sum}|_{\mathrm{Div}^0(E)} = \bar{\sigma}$.

Proposition 2.8. *A divisor* $\Delta \in \mathrm{Div}(E)$ *is principal if and only if* $\deg(\Delta) = 0$ *and* $\mathrm{sum}(\Delta) = \mathcal{O}$*.*

Proof. Both conditions imply $\Delta \in \mathrm{Div}^0(E)$, so $\Delta \sim \langle \mathrm{sum}(\Delta) \rangle - \langle \mathcal{O} \rangle$ and thus, the claim follows because $\mathrm{sum}(\Delta) = \mathcal{O} \Leftrightarrow \Delta \sim 0 \Leftrightarrow \Delta$ is principal. □

3 Point Multiplication

By **point multiplication** we understand the scalar multiplication of E as a $\mathbb{Z}$-module. For finite curves (over finite fields), this multiplication gives rise to the diffie-hellman problem – which has important applications in cryptography.

Recall. We consider the rational maps as points of the curve $E(K(E))$, points with coordinates in the field of rational functions $K(E)$.

Proposition 3.1. *Let* F_1 *and* F_2 *be rational maps on* E*. If* $F_3 = F_1 + F_2$ *as points of* $E(K(E))$*, then* $\forall P \in E : F_3(P) = F_1(P) + F_2(P)$*.*

Proof. We will assume that $F_i \neq \mathcal{O}_M$ for all i since the statement is obviously correct in these cases. Hence, we write $F_i = (f_i, g_i)$. We write

$$\lambda = \frac{f_1^2 + f_1 f_2 + f_2^2 + A}{g_1 + g_2}$$

as in 2.6.

Case 1 $(F_1(P) \neq \mathcal{O},\ F_2(P) \neq \mathcal{O})$**.** If $g_1(P) \neq -g_2(P)$, this case is trivial because the addition formulas coincide. Otherwise, we have $F_1(P) = -F_2(P)$ and also, λ has a pole at P. Consequently, f_3 and g_3 have poles at P yielding $F_3(P) = \mathcal{O} = F_1(P) + F_2(P)$.

Case 2 $(F_1(P) = \mathcal{O},\ F_2(P) \neq \mathcal{O})$**.** We write $f_1 = u^{-d} r$ and $g_1 = u^{-e} s$ where u is a uniformizer and both r and s are finite and nonzero at P. Since

$$\begin{aligned} u^{-2e} s^2 = g_1^2 = f_1^3 + A f_1 + B &= u^{-3d} r^3 + A u^{-d} r + B \\ &= u^{-2e}(u^{2e-3d} r^3 + A u^{2e-d} r + u^{2e} B), \end{aligned}$$

we conclude $2e = 3d$ so $2d > e > d$. Also, $f_1 \neq f_2$ because they differ in P, we can use

$$\lambda = \frac{g_2 - g_1}{f_2 - f_1}$$

for the calculation

$$\begin{aligned} f_3 &= \left(\frac{g_2 - g1}{f_2 - f_1}\right)^2 - (f_2 + f_1) \\ &= \frac{(g_2^2 - 2g_1g_2 + g_1^2) - (f_2 + f_1)(f_2 - f_1)^2}{(f_2 - f_1)^2} \\ &= \frac{g_2^2 - 2g_1g_2 + g_1^2 - f_1^3 + f_1f_2^2 - f_2^3 + f_1^2f_2}{f_1^2 + f_2^2 - 2f_1f_2} \\ &= \frac{g_2^2 - 2g_1g_2 + Af_1 + B + f_1f_2^2 - f_2^3 + f_1^2f_2}{f_1^2 + f_2^2 - 2f_1f_2} \\ &= \frac{f_1^2f_2 - 2g_1g_2}{f_1^2 + f_2^2 - 2f_1f_2} + \underbrace{\frac{g_2^2 + Af_1 + B + f_1f_2^2 - f_2^3}{f_1^2 + f_2^2 - 2f_1f_2}}_{\text{vanishes at } P}. \end{aligned}$$

By multiplying numerator and denominator by $2d$ and evaluating at P, we get that

$$f_3(P) = \frac{r^2f_2 - 2su^{2d-e}g_2}{r^2 + f_2^2u^{2d} - 2ru^df_2}(P) = f_2(P).$$

We therefore know that $F_3(P) \neq \mathcal{O}$. Since $F_3 - F_2 = F_1$, the first case gives us

$$F_3(P) - F_2(P) = F_3(P) + (-F_2)(P) = F_1(P) = \mathcal{O},$$

so we are done.

Case 3 ($F_1(P) = \mathcal{O}$, $F_2(P) = \mathcal{O}$)**.** We know that $F_1 + (F_2 - F_3) = \mathcal{O}_M$. Assume that $F_3(P) = Q \neq \mathcal{O}$. Then, by the previous case,

$$(F_2 - F_3)(P) = F_2(P) - F_3(P) = -Q$$

and consequently,

$$\mathcal{O} = \mathcal{O}_M(P) = (F_1 + (F_2 - F_3))(P) = F_1(P) + (F_2 - F_3)(P) = -Q$$

which is a direct contradiction to $\mathcal{O} \neq Q$. □

Definition 3.2. For every $n \in \mathbb{Z}$, we define the **n-fold point multiplication** to be the map

$$\begin{aligned} [n] : E &\longrightarrow E \\ P &\longmapsto n \cdot P \end{aligned}$$

Also set $g_n := x \circ [n]$ and $h_n := y \circ [n]$, i.e. $n \cdot P = (g_n(P), h_n(P))$. We also define the **$n$-torsion points of** E to be the set

$$E[n] := \{ P \in E \mid n \cdot P = \mathcal{O} \}.$$

It is clearly a subgroup of E.

Theorem 3.3. *For all $n \in \mathbb{Z}$, the n-fold point multiplication is a rational map. For $n \neq 0$, its kernel $E[n]$ is a finite set.*

Remark. In other words, g_n and h_n are rational functions for all $n \in \mathbb{Z}$.

Proof. If the statement holds for $n \geq 0$, then it holds for $-n$ as well by 2.4. Furthermore, the statement is trivial for $n = 0, 1$. We use this as the base for an induction on $n > 0$. By $n \cdot P = (n-1) \cdot P + P$ and 3.1, we can conclude that $[n] = [n-1] + [1]$ is a rational map. To see that $E[n]$ is finite, we only have to verify that $[n] \neq \mathcal{O}_M$.

We note that $E[2] = \{ \mathcal{O}, \Omega_1, \Omega_2, \Omega_3 \}$ is clearly finite. If n is an odd prime, this implies $n \cdot \Omega_1 = \Omega_1 \neq \mathcal{O}$ and therefore, $[n] \neq \mathcal{O}_M$. Thus, we can assume n to have a nontrivial divisor m. More precisely, we assume $n = j \cdot m$ such that by induction hypothesis, $E[j]$ and $E[m]$ are finite. Note that

$$E[n] = \bigcup_{R \in E[j]} \{ P \in E \mid m \cdot P = R \} = \bigcup_{R \in E[j]} [m]^{-1}(R)$$

so it suffices to prove that $[m]^{-1}(R)$ is finite for all R. We may assume that the set is not empty and pick $Q_R \in [m]^{-1}(R)$. The translation T_{Q_R} then induces a bijection $E[m] \cong [m]^{-1}(R)$. □

Corollary 3.4. *We observe $n \neq 1 \Rightarrow g_n - x \not\equiv 0$.*

Proof. If $g_n - x$ was identically zero, then $n \cdot P = \pm P$ would hold for all P. We can write this as $(n \pm 1) \cdot P = \mathcal{O}$ for all P. Thus, either $E[n-1]$ or $E[n+1]$ would have to be infinite – contradicting 3.3. □

4 Counting Torsion Points

We have seen that $E[n]$ is always a finite set – the main result of this section will be the fact that it contains exactly n^2 points as long as n is not a multiple of $\mathrm{char}(k)$. This result will later be used to determine the total number of points on a finite curve. This number has to satisfy certain conditions in order to make the curve suitable for cryptographic purposes – it is our final goal to devise an algorithm for counting all points on a finite curve.

Proposition 4.1. *Assume that n is not a multiple of* $\mathrm{char}(k)$. *Then,*

$$(g_n/x)(\mathcal{O}) = n^{-2} \quad \text{and} \quad (h_n/y)(\mathcal{O}) = n^{-3}.$$

Proof. The statement is symbolically correct for $n = 0$ and obviously holds for $n = 1$. We use this as the base for an induction on n. For $n \geq 1$, we consider the point addition $(n+1) \cdot P = n \cdot P + P$. Using 2.6 for (4),

$$\begin{aligned} \frac{g_{n+1}}{x} &= \frac{1}{x} \cdot \left(\left(\frac{g_n^2 + g_n x + x^2 + A}{h_n + y} \right)^2 - g_n - x \right) \\ &= \frac{x^4}{y^2 x} \cdot \left(\frac{(g_n/x)^2 + (g_n/x) + 1 + (A/x^2)}{(h_n/y) + 1} \right)^2 - (g_n/x) - 1. \end{aligned}$$

By induction hypothesis, evaluation at $\mathcal{O}$ yields

$$\begin{aligned}
(g_{n+1}/x)\,(\mathcal{O}) &= \left(\frac{n^{-4}+n^{-2}+1}{n^{-3}+1}\right)^2 - \frac{1}{n^2} - 1 \\
&= \left(\frac{1+n^2+n^4}{n+n^4}\right)^2 - \frac{1+n^2}{n^2} \\
&= \frac{n^8+2n^6+3n^4+2n^2+1}{(n+n^4)^2} - \frac{(1+n^2)(1+n^3)^2}{(n+n^4)^2} \\
&= \frac{n^8+2n^6+3n^4+2n^2+1}{(n+n^4)^2} - \frac{(1+n^2)(1+n^3)^2}{(n+n^4)^2} \\
&= \frac{n^8+2n^6+3n^4+2n^2+1-1-n^2-2n^3-2n^5-n^6-n^8}{(n+n^4)^2} \\
&= \frac{n^6-2n^5+3n^4-2n^3+n^2}{(n+n^4)^2} = \frac{n^4-2n^3+3n^2-2n+1}{(1+n^3)^2} \\
&= \frac{(1-n+n^2)^2}{(1+n^3)^2} = \frac{1}{(1+n)^2}
\end{aligned}$$

For the second coordinate, we use (4) to calculate

$$\begin{aligned}
\frac{h_{n+1}}{y} &= \frac{1}{y}\cdot\left(-y - \frac{g_n^2+g_nx+x^2+A}{h_n+y}\cdot(g_{n+1}-x)\right) \\
&= -1 - \frac{x^3}{y^2}\cdot\frac{(g_n/x)^2+(g_n/x)+1+\left(A/x^2\right)}{(h_n/y)+1}\cdot\left(\frac{g_{n+1}}{x}-1\right)
\end{aligned}$$

and evaluation at $\mathcal{O}$ yields

$$\begin{aligned}
(h_{n+1}/y)\,(\mathcal{O}) &= -1 - \frac{n^{-4}+n^{-2}+1}{n^{-3}+1}\cdot\left(\frac{1}{(n+1)^2}-1\right) \\
&= -1 - \frac{1+n^2+n^4}{n+n^4}\cdot\frac{1-(n+1)^2}{(n+1)^2} \\
&= \frac{1+n^2+n^4}{n+n^4}\cdot\frac{n^2+2n}{(n+1)^2} - 1 \\
&= \frac{n+n^3+n^5+2+2n^2+2n^4}{(1+n^3)(n+1)^2} - 1 \\
&= \frac{n^2-n+1}{(1+n^3)(n+1)^2} = \frac{(n-1)^2+n}{(1+n^3)(n+1)^2} \\
&= \frac{(n^2-1)(n-1)+n^2+n}{(1+n^3)(n+1)^3} = \frac{1}{(n+1)^3}
\end{aligned}$$

which concludes the induction as long as n is not a multiple of $p := \mathrm{char}(k)$. In this case, we have to use the equation $(n+1)\cdot P = (n-1)\cdot P + 2\cdot P$ for the induction step. This is equivalent to the above approach, but with even more mind-numbing calculations. If you are not convinced, check it with a computer algebra program. □

Corollary 4.2. *If n is not a multiple of* $\mathrm{char}(k)$*,*

- g_n *has order* -2 *at* $\mathcal{O}$ *and leading coefficient* n^{-2}.
- h_n *has order* -3 *at* $\mathcal{O}$ *and leading coefficient* n^{-3}.

Proof. Since the rational function

$$(x/y)^2 \cdot g_n = \frac{x^2 \cdot g_n}{x^3 + Ax + B} = \frac{g_n}{x} \cdot \frac{x^2}{x^2 + A + Bx^{-1}}$$

has the same finite and nonzero value at $\mathcal{O}$ as g_n/x, the first claim follows from 4.1. Equivalently, we can write

$$(x/y)^3 \cdot h_n = \frac{(y^2 - Ax - B) \cdot h_n}{y^3} = \frac{h_n}{y} \cdot \frac{y^2 - Ax - B}{y^2}$$

and obtain the result for h_n □

Proposition 4.3. $D(g_n) = 2nh_n$ *and* $D(h_n) = n(3g_n^2 + A)$.

Proof. The statement is clear for $n = 1$ by definition of D (see (3)). The equations

$$\begin{aligned} h_n^2 &= g_n^3 + Ag_n + B && (6) \\ g_{n+1} &= \lambda^2 - (g_n + x) && (7) \\ h_{n+1} &= \lambda \cdot (x - g_{n+1}) - y && (8) \end{aligned}$$

follow from the curve equation and the generic addition formula (4) using

$$\lambda = \frac{g_n^2 + g_n x + x^2 + A}{h_n + y}$$

by 2.6. We note that

$$\begin{aligned} (h_n + y) \cdot D(\lambda) &= D(g_n^2 + g_n x + x^2 + A) - \lambda D(h_n + y) \\ &= 2y(g_n + 2x) + 2nh_n(2g_n + x) - \lambda(3ng_n^2 + 3x^2 + (n+1)A) \end{aligned}$$

In the induction step, it suffices to show that

$$\begin{aligned} 0 &= D(g_{n+1})/2 - (n+1)h_{n+1} \\ &= \lambda \cdot D(\lambda) - nh_n - y - (n+1)\lambda(x - g_{n+1}) + (n+1)y \\ &= \lambda \cdot D(\lambda) - n(h_n - y) + \lambda(n+1)(\lambda^2 - g_n - 2x) \end{aligned}$$

On the right hand side, we reduce occurances of h_n^2 and y^2 using the curve equation. A tedious calculation proves the above equality, we suggest to use a computer algebra system. One proceeds equivalently for h_{n+1}. □

Lemma 4.4. *Let $P, Q \in E$ and let u be a uniformizer at P. Then, $u \circ T_Q$ is a uniformizer at $P - Q$.*

Proof. Since $u(T_Q(P - Q)) = u(P) = 0$, we know that

$$m := \operatorname{ord}_{P-Q}(u \circ T_Q) \geq 1.$$

Let v be a uniformizer at $P - Q$ and $u \circ T_Q = v^m s$ with s finite and nonzero at $P - Q$. Let r be any rational function. If $\operatorname{ord}_P(r) = d$, we write $r = u^d t$ with t finite and nonzero at P. Then,

$$r \circ T_Q = (u \circ T_Q)^d \cdot (t \circ T_Q) = v^{md} \cdot \underbrace{s^d \cdot (t \circ T_Q)}_{w}$$

such that $w(P - Q) = s(P - Q)^d \cdot t(P)$ is finite and nonzero. Thus, we obtain the formula $\operatorname{ord}_{P-Q}(r \circ T_Q) = m \cdot \operatorname{ord}_P(r)$. for all rational functions on E. Replacing r by $r \circ T_{-Q}$, we get

$$\operatorname{ord}_P(r \circ T_{-Q}) = \operatorname{ord}_{P-Q}(r)/m \tag{9}$$

Hence, $(v \circ T_{-Q})(P) = v(P - Q) = 0$ means

$$1 \leq \operatorname{ord}_P(v \circ T_{-Q}) = \operatorname{ord}_{P-Q}(v)/m = m^{-1}.$$

Thus, $m = 1$ and $u \circ T_Q$ must be a uniformizer at $P - Q$. □

Corollary 4.5. *For any two points $P, Q \in E$ and any rational function r,*

$$\operatorname{ord}_P(r \circ T_Q) = \operatorname{ord}_{P+Q}(r). \tag{10}$$

Proof. This is just equation (9), since we know $m = 1$. □

Corollary 4.6. $\operatorname{div}(r) = \sum_P n_P \langle P \rangle \Rightarrow \operatorname{div}(r \circ T_Q) = \sum_P n_P \langle P - Q \rangle$. □

Lemma 4.7. *If r_1 and r_2 are rational functions,*

$$\operatorname{ord}_{\mathcal{O}}(r_1 - r_2) \geq \min(\operatorname{ord}_{\mathcal{O}}(r_1), \operatorname{ord}_{\mathcal{O}}(r_2)). \tag{11}$$

Equality holds if and only if both functions have different order at $\mathcal{O}$ or different leading coefficients.

Proof. Let $u = x/y$ and write $r_1 = u^{d_1} s_1$ as well as $r_2 = u^{d_2} s_2$ with s_1 and s_2 finite and nonzero at $\mathcal{O}$. Note that $s_i(\mathcal{O})$ is precisely the leading coefficient of r_i. Without loss of generality, assume that $d_1 \geq d_2$. Then,

$$r_1 - r_2 = u^{d_2} \cdot \underbrace{(u^{d_1 - d_2} s_1 - s_2)}_{s}$$

Now s is finite and nonzero at P if and only if $d_2 > d_1$ or $s_1(\mathcal{O}) = s_2(\mathcal{O})$. □

Notation 4.8. If $M \subseteq E$ is a finite set of points of E, we will write

$$\langle M \rangle := \sum_{P \in M} \langle P \rangle \in \operatorname{Div}(E).$$

Theorem 4.9. *Let $m > n > 0$ such that neither of m, n, $m-n$ and $m+n$ are a multiple of* $\mathrm{char}(k)$. *Then,*

$$\mathrm{div}(g_m - g_n) = \langle E[m+n]\rangle + \langle E[m-n]\rangle - 2\langle E[m]\rangle - 2\langle E[n]\rangle . \tag{12}$$

Proof. We consider the partition

$$E = \underbrace{E[m]\cap E[n]}_{E_1} \cup \underbrace{(E[m]\cup E[n])\setminus (E[m]\cap E[n])}_{E_2} \cup \underbrace{E\setminus (E[m]\cup E[n])}_{E_3}$$

and count multiplicities. We will often require the following observation:

$$\begin{aligned} \forall : P \in E[j]: \quad & [j]\circ T_P = [j] \\ \Longrightarrow \quad & g_j \circ T_p = g_j \\ \Longrightarrow \quad & \mathrm{ord}_P(g_j) = \mathrm{ord}_{\mathcal{O}}(g_j). \end{aligned} \tag{13}$$

This follows since $j\cdot Q = j\cdot(Q+P)$ holds for all $Q\in E$ and the final implication is due to 4.5.

We note that $E_1 \subseteq E[m+n]\cap E[m-n]$. For $P\in E_1$, this means that we have to verify $\mathrm{ord}_P(g_m - g_n) = 1+1-2-2 = -2$. We remark that $(m-n)(m+n) = m^2 - n^2$ is not a multiple of $\mathrm{char}(k)$, so $m^2 \neq n^2$ in k. Thus by 4.2, the leading coefficients of g_m and g_n differ. Since $Q := -P \in E_1$,

$$\begin{aligned} \mathrm{ord}_P(g_m - g_n) &\overset{(10)}{=} \mathrm{ord}_{\mathcal{O}}((g_m - g_n)\circ T_Q) = \mathrm{ord}_{\mathcal{O}}(g_m\circ T_Q - g_n \circ T_Q) \\ &\overset{(13)}{=} \mathrm{ord}_{\mathcal{O}}(g_m - g_n) \overset{(11)}{=} \min(\mathrm{ord}_{\mathcal{O}}(g_m), \mathrm{ord}_{\mathcal{O}}(g_n)) \overset{(4.2)}{=} -2. \end{aligned}$$

We now consider the points $P\in E_2$. Since either $mP = \mathcal{O}$ or $nP = \mathcal{O}$ but not both, $P \notin E[m+n]\cup E[m-n]$. Thus, we have to show $\mathrm{ord}_P(g_m - g_n) = -2$ again. Now, $P\in E[m]$ implies $g_n(P)\neq\infty$. Writing $g_m = u_P^{-d} t$ with $t(P)\in k^\times$, we can see that $g_m - g_n = u_P^{-d}(t - u_P^d g_n)$. Thus,

$$\mathrm{ord}_P(g_m - g_n) = \mathrm{ord}_P(g_m) \overset{(13)}{=} \mathrm{ord}_{\mathcal{O}}(g_m) \overset{(4.2)}{=} -2.$$

Similarly, $P\in E[n]$ implies $g_m(P)\neq\infty$ and we get the desired result in an equivalent way.

We now consider points $P\in E_3$. Now $g_m - g_n$ can not have a pole at P. It has a zero at P if and only if $mP = \pm nP$ which is the case if and only if $P\in E[m+n]\cup E[m-n]$ since $mP = (m\mp n)P \pm nP$. This means, we only have to count the multiplicities at the points in

$$\begin{aligned} E_3 \cap (E[m-n]\cup E[m+n]) = &\underbrace{E_3\cap (E[m-n]\cap E[m+n])}_{E_4} \\ &\cup \underbrace{E_3\cap (E[m+n]\setminus E[m-n])}_{E_5} \\ &\cup \underbrace{E_3\cap (E[m-n]\setminus E[m+n])}_{E_6} \end{aligned}$$

For points $P \in E_4$, we know $Q := nP = mP = -nP$, so Q is of order two. By 4.3, we can calculate

$$D(g_m - g_n)(P) = (2mh_m - 2nh_n)(P) = 2 \cdot (m-n) \cdot y(Q) = 0$$

which means that the zero at P is of order greater or equal than 2 by 1.13. Let now $\omega := g_n(P) = g_m(P)$. We derive further to see that

$$\begin{aligned} D^2(g_m - g_n)(P) &= D(2mh_m - 2nh_n)(P) \\ &= (2m^2(3g_m^2 + A) - 2n^2(3g_n^2 + A))(P) \\ &= 2 \cdot (m^2 - n^2) \cdot (3\omega^2 + A) \\ &= 2 \cdot (m-n) \cdot (m+n) \cdot \partial_X(X^3 + AX + B)(\omega) \end{aligned}$$

is nonzero since 2, $m-n$ and $m+n$ are not multiples of $\mathrm{char}(k)$ and E is assumed to be nonsingular. Thus, $\mathrm{ord}_P(g_m - g_n) = 2$ is precisely the number we wanted to count.

For $P \in E_5$, we know $nP \neq mP = -nP$ and thus, $h_n(P) = -h_m(P) \neq 0$. Thus, $D(g_m - g_n)(P) = 2(m+n)h_m(P)$ is nonzero and $\mathrm{ord}_P(g_m - g_n) = 1$ by 1.13. The case $P \in E_6$ works equivalently. □

Corollary 4.10. *If n is not a multiple of* $\mathrm{char}(k)$*, then* $\#E[n] = n^2$*.*

Proof. Let $\delta : \mathbb{N} \to \mathbb{N}$ be the function defined by $\delta(n) := \#E[n]$. Let Δ be the set of all functions $d : \mathbb{N} \to \mathbb{N}$ satisfying

$$d(m+n) + d(m-n) - 2d(m) - 2d(n) = 0$$

whenever $m > n > 0$ and neither of m,n,$m+n$ and $m-n$ are multiples of $\mathrm{char}(k)$. Clearly, $\delta \in \Delta$ by (12). Also,

$$\begin{aligned} &(m+n)^2 + (m-n)^2 - 2m^2 - 2n^2 \\ &\quad = m^2 + n^2 + 2mn + m^2 + n^2 - 2mn - 2m^2 - 2n^2 = 0 \end{aligned}$$

verifies that $(-)^2 \in \Delta$. We are now going to show that Δ contains precisely one function d with $d(1) = 1$ and $d(2) = 4$. Since both $(-)^2$ and δ have this property, it will prove the statement. To do so, we first note that for $d_1, d_2 \in \Delta$, also $d := d_1 - d_2 \in \Delta$. We need to show that $d \in \Delta$ with $d(1) = d(2) = 0$ already implies $d \equiv 0$.

Now, let $j > 2$ be no integer multiple of $\mathrm{char}(k) =: p$. We furthermore assume $p \neq 0$ since the opposite can be verified exactly as in

Case 1 ($j-1$ and $j-2$ are prime to p)**.** This case follows by induction from

$$\begin{aligned} d(j) &= d(j) - d((j-1)+1) - d((j-1)-1) + 2d(j-1) + 2d(1) \\ &= 2d(j-1) - d(j-2) = 0. \end{aligned}$$

Case 2 ($j-1$ is a multiple of p)**.** We may assume $j>5$ by our global assumptions on p. In this case, $j-2$ must be prime to p. Also, since $j-1$ is a multiple of $p\neq 3$, $j-4$ is prime to p. Consequently, the induction step follows by

$$\begin{aligned} d(j) &= d(j)-d((j-2)+2)-d((j-2)-2)+2d(j-2)+2d(2) \\ &= 2d(j-2)-d(j-4)=0. \end{aligned}$$

Case 3 ($j-2$ is a multiple of p)**.** We know $j>6$. Also, $j-3$ must be prime to p and $j-6$ can not be a multiple of p because $j-2$ is (and 4 is not prime). The result follows by

$$\begin{aligned} d(j) &= d(j)-d((j-3)+3)-d((j-3)-3)+2d(j-3)+2d(3) \\ &= 2d(j-3)+2d(3)-d(j-6)=0. \end{aligned}$$

This concludes $d\equiv 0$ by induction. □

Corollary 4.11. *For $p:=\mathrm{char}(k)\neq 0$ and $n\notin (p)$, it follows that*

$$E[n] \quad \cong \quad \mathbb{Z}/(n)\times\mathbb{Z}/(n)$$

is a free $\mathbb{Z}/(n)$-module of rank 2.

Proof. This follows from the fundamental theorem of abelian groups – see, for instance, [Bo06, Korollar 2.9.9]. □

References

[CharRob88] Leonard S. Charlap, David P.Robbins, *An Elementary Introduction to Elliptic Curves*, CRD Expository Report 31

[Eis94] David Eisenbud *Commutative Algebra with a View Toward Algebraic Geometry*, Springer 1994

[Bo06] Siegfried Bosch, *Algebra*, Springer 2006