TD Elliptic Curves 4, 5 and 6

Damien Robert

October–November 2023

1 Rational functions

Exercice 1.1.

- Show that if $y_P \neq 0$, a uniformiser at P is $x - x_P$;
- Show that if $y_P = 0$, a uniformiser at P is y;
- Show that a uniformiser at 0_E is x/y. Deduce that $v_{0_E}(g) = -\deg(g)$ where $\deg(x) = 2$ and $\deg(y) = 3$.

Exercice 1.2. Let E be the elliptic curve $y^2 = x^3 - x$ over $\mathbb{Q}$.

- Compute the order and the value of the rational function x/y at $P = (0, 0)$.
- Compute the order and the value of the rational function $\frac{y+x-1}{x-1}$ at $P = (1, 0)$.
- Compute the order and the value of the rational function $\frac{x^3}{2y^2}$ at 0_E.
- Compute the order and the value of the rational function $\frac{x^2+y}{xy}$ at 0_E.

Exercice 1.3. Let E be the elliptic curve $y^2 = x^3 + 6$ over $\mathbb{F}_{11}$.

- Compute the order and the value of the rational function $-2x - y + 4$ at $P = (-2, 8)$.
- Compute the order and the value of the rational function $x + 3y$ at $P = (-2, 8)$.

Exercice 1.4. Let E be an elliptic curve and P a point of E which is not a Weierstrass point. Let $r(x, y) = \frac{y-y_P}{x-x_P}$. Compute the order and the value of r at P.

Let $P = (x_P, 0)$ a Weierstrass point of E. Compute the order and the value of $x - x_P$ at P.

Exercice 1.5. Let E be the elliptic curve $y^2 = x^3 - 7x + 6$ over $\mathbb{Q}$.

- Compute the order and the value of the rational function $x^2 + y - 1$ at $P = (1, 0)$.
- Compute the order and the value of the rational function $x^2 + y^2 - 1$ at $P = (1, 0)$.
- Compute the order and the value of the rational function $x^3 - (x^2 - 1)y - 1$ at $P = (1, 0)$.

2 Divisors

Exercice 2.1. For P, Q two points on an elliptic curve E, write a function `line(P,Q)` that computes the equation of the line going through P and Q (or if $P = Q$ the equation of the tangent to E at P).

Exercice 2.2. Let E be the elliptic curve $y^2 = x^3 + x + 3$ over $\mathbb{F}_{11}$, $P = (1, 4)$, $Q = (3, 0)$, $R = (0, 6)$, $S = (1, 7)$. Compute the equation and the associated divisor of

- the line going through S and $-S$;
- the tangent at R;
- the line going through P and Q;
- the tangent at P;
- the tangent at Q.

Exercice 2.3.

- Write a function which takes for input two points $P_1, P_2 \in E$ and outputs μ_{P_1,P_2} where μ_{P_1,P_2} is a function with divisor $[P_1] + [P_2] - [P_1 + P_2] - [0_E]$.
- Write a function which takes for input $\ell \in \mathbb{N}$ and a point $P \in E$ and outputs $f_{\ell,P}$ where $f_{\ell,P}$ is a function with divisor $\ell[P] - [\ell P] - (\ell - 1)[0_E]$. (You can try the naive method and compare it with the double and add method).

Exercice 2.4. Let E be the elliptic curve $y^2 = x^3 + x + 1$ over $\mathbb{F}_7$ and $P = (0, 1)$. Check that $D = 5[P] - 5[0_E]$ is principal and compute a function $f_{5,P}$ whose associated divisor is D.

Compute a function $f_{5n,P}$ whose divisor is nD for several n. What can you say about the degree of this function?

Exercice 2.5.
We now compute the same functions as in Exercice 2.3 except we only evaluate them on a point Q.

- Write a function which takes for input three points $P_1, P_2, Q \in E$ and outputs $\mu_{P_1,P_2}(Q)$.
- Write a function which takes for input $\ell \in \mathbb{N}$ and two points $P, Q \in E$ and outputs $f_{\ell,P}(Q)$. (You can try the naive method and compare it with the double and add method).

3 Pairings

Exercice 3.1. The Weil pairing is a $\mathbb{Z}$-bilinear application, alternate and non degenerate:

$$e_m : E(\overline{\mathbb{F}_p})[m] \times E(\overline{\mathbb{F}_p})[m] \longrightarrow \mu_m(\overline{\mathbb{F}_p})$$

where $\mu_m(\overline{\mathbb{F}_p})$ is the multiplicative group of m-th roots of unity in $\overline{\mathbb{F}_p}$.

The pairings e_m are compatibles between each others: let m' be another integer prime to p, and $P \in E[m]$, $Q \in E[mm']$. Then

$$e_{mm'}(P, Q) = e_m(P, m'Q).$$

1. What does the bilinearity of e_m means?
2. What does alternate means for e_m?
3. What does non degenerate means for e_m?
4. Show that e_m is antisymmetric, which means that

   $$e_m(Q, P) = e_m(P, Q)^{-1}$$

   for all tuple $(P, Q) \in E[m]^2$.
5. To which group is $\mu_m(\overline{\mathbb{F}_p})$ isomorphic to? Show that there exists an integer k such that

   $$\mu_m(\overline{\mathbb{F}_p}) = \mu_m(\mathbb{F}_{p^k}).$$

   What arithmetic condition does k satisfy? What is the smallest k possible?
6. Let P and Q two points de m-torsion. Determine a relation between the order of $e_m(P, Q)$, and the orders of P and Q.
7. Let $P \in E(\overline{\mathbb{F}_p})$ be a (primitive) point of order m. Show that there exists another (primitive) point Q or order m such that $e_m(P, Q)$ is a primitive m-root of unity.
8. Let R be a multiple of P, and Q as in the previous question. We try to determinate the discrete logarithm, meaning an integer ℓ such that $R = \ell P$. Let ℓ_2 be an integer such that $e_{W,m}(R, Q) = e_{W,m}(P, Q)^{\ell_2}$. Show that $R = \ell_2.P$. Deduce a procedure that determines the discrete logarithm over E from the discrete logarithm over a finite field.

Exercice 3.2. Let r be a prime number, the embedding degree is the smallest k such that $\mathbb{F}_{q^k}$ contains the r-th roots of unity.

Let E be an elliptic curve over $\mathbb{F}_q$. Recall that $\#E = q + 1 - t$ where t is the trace of the Frobenius. Let $r \mid \#E$, and k the corresponding embedding degree. Show that k is the order of $t - 1$ modulo r.

- Compute the embedding degree of $y^2 = x^3 - x$ over several prime numbers. (Meaning the embedding degree of the group $E(\mathbb{F}_p)$ over several p, ie take $r = \#E(\mathbb{F}_p)$).

- Compute the embedding degree of $y^2 = x^3 + 1$ over several prime numbers.

Exercice 3.3. Let E be the elliptic curve defined by the long Weierstrass coefficients $[1, 0, 0, -4, -1]$ over $\mathbb{F}_{23}$. E is not given by a short Weierstrass equation, but the Sage function `weil_pairing` still allows to compute the Weil pairing.

- Let $P = (5, 8)$ and $Q = (-2, 1)$ in $E(\mathbb{F}_{23})$. Check that P is of order 4 and Q of order 2. Compute $e_4(P, Q)$ and deduce that Q is not a multiple of P.
- What is the smallest integer k such that $\mathbb{F}_{23^k}$ contains the 4-th roots of unity?
- Check the help of the function `E.division_polynomial` which allows to compute the ψ_n, the n-th division polynomial of E. Compute the polynomial ψ_4 of 4-division of E.
- Looking at the factorisation of ψ_4, check that all points of 4-torsion are defined over $\mathbb{F}_{23^2}$. (Hint: also use the functions `E.is_x_coord` and `E.lift_x`).
- Find a point R of order 4 in $E(\mathbb{F}_{23^2})$ such that $e_4(P, R)$ is a primitive 4-th root of unity.
- Give generators of $E[4](\mathbb{F}_{23})$ using P and R.

Exercice 3.4.

- Recall the formulae to compute the Weil and Tate pairings from the functions $f_{\ell,P}(Q)$ defined in exercice 2.5.
- Write a function that computes the Tate and Weil pairings. Compare to `tate_pairing` and `weil_pairing`.
- Test some examples on the curve $y^2 = x^3 + 5$ over

  $$\mathbb{F}_{1603056903440312827775668828749864951563683810118433749977839298011622224691 3}.$$

  (Check your result with `tate_pairing` and `weil_pairing`.) What is the embedding degree of this curve? Can you use the naive method of Exercice 2.5 to compute these pairings,