TD Elliptic Curves 2 and 3

Damien Robert

29 September 2023

1 Resultants

Exercice 1.1. Compare the method `resultant` with directly computing the determinant of the Sylvester matrix. Test with polynomials over different fields.

Exercice 1.2. Let K be a field such that the two polynomials $P(x) = x^3 - 1$ and $Q(x) = x^2 + 3x + 1$ have a common root. What is the characteristic of K?

Exercice 1.3. Let α_1, α_2 and α_3 be the three complex roots of $A(x) = x^3 + 5x + 7$. Compute $B(x) = (x - \alpha_1^2)(x - \alpha_2^2)(x - \alpha_3^2)$.

Exercice 1.4. Let $C \subset \mathbb{R}^2$ be the curve parametrised by the equations:

$$x(t) = \frac{4t(1-t^2)^2}{(1+t^2)^3}$$
$$y(t) = \frac{8t^2(1-t^2)^2}{(1+t^2)^3}.$$

Give an implicit equation for the curve C.

Exercice 1.5. Compute the discriminant of the polynomial $f(x) = x^3 + ax + b$. Compare with the discriminant of the elliptic curve $E : y^2 = x^3 + ax + b$.

Exercice 1.6. Compute the points of intersection of the curves $x^2 + 2y^3 - 3 = 0$ and $x^2 + xy + y^3 - 3 = 0$.

2 Weierstrass models

An elliptic curve E over a field K is defined by a (long) Weierstrass equation

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

where the coefficients a_1, a_2, a_3, a_4, a_6 are elements in K such that the **discriminant** of the curve E is not null. Computer representation:

$$E = [a_1, a_2, a_3, a_4, a_6].$$

When the characteristic of K is different from 2 and 3, every elliptic curve K has as (short) Weierstrass equation:

$$y^2 = x^3 + ax + b$$

The discriminant of this curve is $\Delta = -16(4a^3 + 27b^2)$, and its j-invariant is $j = 1728\frac{4a^3}{4a^3+27b^2}$.

Note that two distinct equations can define the same elliptic curve (up to isomorphism), and that the discriminant depends on the equation, not on the curve itself, while the j-invariant only depend on the (isomorphism class of the) curve.

Exercice 2.1.

1. Look at the help of the function `EllipticCurve`.
2. Check with Sage the formulae above for an elliptic curve given by a short Weierstrass equation.
3. Compute with Sage the discriminant and the j-invariant for a curve given by a long Weierstrass equation.

Exercice 2.2. Let E be the elliptic curve over $\mathbb{Q}$ defined by the equation with integer coefficients:

$$y^2 + y = x^3 - x^2 - 10x - 20$$

1. What is the discriminant of E? Of its invariant j?
2. Using a change of variable, find an equation of E of the form

   $$y^2 = x^3 + px + q$$

   where p and q are in $\mathbb{Q}$. Hint: once you have found a change of variable, you can either substitute the new variables on the polynomials with Sage or you use `E.change_weierstrass_model()`.
3. Recover the result using `E.short_weierstrass_model()`.
4. Let $E2$ = `E.change_weierstrass_model([1/3,0,0,0])`. Compare the discriminant and the invariant j of $E2$ with those of E.
5. Let $E3$ be the elliptic curve given by the short Weierstrass equation $y^2 = x^3 - 13392 * x - 1080432$. Is $E3$ isomorphic to E?

Exercice 2.3.

1. Write a function `ellisoncurve` that checks if a point is on an elliptic curve.
2. Test this function with the curve $E : y^2 = x^3 + 17$ and the points $P_1 = (-2, 3)$ et $P_2 = (-1, 4)$.
3. Write a function `elladd` that computes the sum of two points in an elliptic curve (you may assume that E is given by a short Weierstrass model).

4. Compute $P_1 + P_1$, $P_1 - P_1$ et $P_1 + 0_E$.
5. Compute some multiples $n_1P_1 + n_2P_2$.

Exercice 2.4.
Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + x^2 + x - 2$.

1. Let $P = (1, 1)$. Check that P is a point on E.
2. Compute $[n]P$ for several values of n.
3. Write a function `ellmul`(E, P, n) based on the method of binary exponentiation to compute $[n]P$ where n is an integer and $P \in E(K)$ is a point of E. (Warning: here E is not given by a short Weierstrass model so you need to convert to a short Weierstrass model to use `elladd` or instead you could use Sage's native addition directly.)
4. Compare the speed of this function with the native Sage implementation.

Exercice 2.5.
1. Let $E : y^2 = x^3 + 256$. Check that $P = (0, 16)$ is on the curve. Check that it is a torsion point and compute its order using the function from the preceding exercice.
2. Same question with $E : y^2 = x^3 + x/4$ et $P = (1/2, 1/2)$.
3. Same question with $E : y^2 = x^3 - 43x + 166$ et $P = (3, 8)$.
4. Compare with the method from Exercice 4.1.

3 Edwards models

An Edwards model is a curve given by the equation:

$$x^2 + y^2 = c^2(1 + dx^2y^2)$$

where $cd(1 - dc^4) \neq 0$. There are only two parameters: computer representation $E = [c, d]$.

The curve E is an elliptic curve, whose addition law is given by

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)} \right).$$

Note that the addition formula also directly give the duplication formula, contrary to the case of the Weierstrass model. However the Edward curve is not smooth at infinity, so to be rigorous we would need to remove singularities. But away from the singularities the addition law is well defined and more efficient than the Weierstrass model.

Check that

1. The neutral point is the affine point $(0, c)$.
2. The opposite of a point (x, y) is $(-x, y)$.

Exercice 3.1.

1. Write a function `Edwards`(c,d) which print the equation of the Edwards curve with parameters c,d.
2. Write a function `Edwardsisoncurve`(E,P) which test if a point P is on the Edwards cruve E.
3. Given two points P and Q in E, write a function `Edwardsadd`(E,P,Q) which compute $P+Q$.
4. On a generic model $E=[c,d]$, compute the order of the points $(0,-c)$, $(c,0)$ et $(-c,0)$.
5. Bonus: rewrite these functions using a SAGE class for Edwards curves and one for Edwards points.

Exercice 3.2. We will study how to go from an Edwards model to a Weierstrass model. We use that (generically), an equation of the type $x^2+y^2=1+dx^2y^2$ is birationally equivalent to the Weierstrass curve

$$\frac{1}{1-d}v^2=u^3+2\frac{1+d}{1-d}u^2+u.$$

We use the rational change of variables $(u,v)\mapsto(x,y)$ where

$$x=2u/v \qquad \text{and} \qquad y=(u-1)/(u+1)$$

1. Consider the Weierstrass curve $E_1 : v^2=u^3+3u^2+u$. Show that it is birationally equivalent to the Edwards curve $E_2 : x^2+y^2=1+5x^2y^2$.
2. Write a function converting points in E_1 to points in E_2.
3. Write a function converting points in E_2 to points in E_1.
4. Compare over several finite field (in large and small characteristics) the speed of the addition law on E_1 and on E_2.

4 Group of points of an elliptic curve

Exercice 4.1. The goal of this exercice is to have methods to compute the order of a point on an elliptic curve.

1. Write a method which give the order of a point, provided a a multiple of its order is known.
2. Apply this method to the elliptic curve defined over $\mathbb{F}_{173}$ by

   $$y^2=x^3+146x+33$$

   and the points $P=(168,133)$, $Q=(147,74)$. What multiple of their order do you know?

3. Deduce that $Q = n.P$ for some n and find n.
4. Find all rational points of n-torsion for $2 \leq n \leq 5$.

Exercice 4.2. Let $E : y^2 = x^3 + x$.

1. For which p is $E/\mathbb{F}_p$ an elliptic curve?
2. Compute the cardinal of $E(\mathbb{F}_p)$ and of $E(\mathbb{F}_{p^2})$ for $p = 3, p = 5, p = 7, p = 11$ or more generally all primes $p \leq 100$ (provided that $E/\mathbb{F}_p$ is an elliptic curve).
3. Same questions for $E : y^2 = x^3 + 1$.
4. When $E : y^2 = x^3 + x$ (resp. $E : y^2 = x^3 + 1$), find an interesting pattern on the cardinals of $E(\mathbb{F}_p)$ and $E(\mathbb{F}_{p^2})$ when $p \equiv 3 \pmod 4$ (resp. $p \equiv 2 \pmod 3$).
5. Explain how to compute the characteristic polynomial of π^n given the characteristic polynomial of π. (Hint: use a resultant.) Deduce a method to compute the cardinal of $E(\mathbb{F}_{p^n})$ given only the cardinal of $E(\mathbb{F}_p)$.

Exercice 4.3.

1. For which primes p does the equation $y^2 + y = x^3 - x^2 - 10x - 20$ define an elliptic curve $\mathbb{F}_p$? If p is such a prime, we denote E_p the corresponding curve over $\mathbb{F}_p$.
2. Compute $E_p(\mathbb{F}_p)$ for all primes less than 100. Is this group always cyclic?
3. Compute the group $E(\mathbb{Q})_{\text{tors}}$, and give the list of all its elements.
4. Is the reduction modulo p application

$$E(\mathbb{Q})_{\text{tors}} \longrightarrow E_p(\mathbb{F}_p)$$

injective, surjective? Give some examples. (Be careful that your reduction map is well defined.)

In general, when E is an elliptic curve given by a Weierstrass equation with integral coefficients a_i, the Nagell-Lutz theorem states that, if $P = (x, y)$ is a point of torsion defined over $\mathbb{Q}$, then x and y are integral, except when P is a point of 2-torsion, in which case $P = (c/4, d/8)$ with c and d integers. If furthermore E is given by a short Weierstrass equation, then $x, y \in \mathbb{Z}$ (even if P is of order 2), and either $y = 0$, or $y^2 \mid \Delta_E$.

In particular, the reduction

$$E(\mathbb{Q})_{\text{tors}} \longrightarrow E_p(\mathbb{F}_p)$$

is injective for all prime p not dividing $2\Delta_E$.

Another consequence is that if P does not have integral coordinates and is not of the form $(c/4, d/8)$, then P is of infinite order. In fact, if there exist $n > 0$ such that $[n]P$ is not of this form, then P is of infinite order.

Exemple: the point $P = (1, 1)$ on the curve $E : y^2 = x^3 + x^2 + x - 2$ is of infinite order.