Université de Rennes I 1st Semester 2013-2014

Introduction to elliptic curves

By
Christophe RITZENTHALER

These are notes of a course taught at Rennes in the first semester 2013-2014. They can be found on http://perso.univ-rennes1.fr/christophe.ritzenthaler/. Please send comments and corrections to me at christophe.ritzenthaler@univ-rennes1.fr.

Notation and convention. Then integer q is a power $n > 0$ of a prime p and k is a finite field of cardinal q. The letter K is any (perfect) field of characteristic p, and here p can be 0 as well.

Contents

1 Introduction to elliptic curves

1.1 Some definitions

1.1.1 First definition of an elliptic curve

Definition 1.1.1. A *Weierstrass equation* of an elliptic curve E over a field K is

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

where $a_1, a_2, a_3, a_4, a_6 \in K$ and $\Delta \neq 0$ where Δ is the *discriminant* of E and is defined as follow

$$\begin{cases} \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ b_2 = a_1^2 + 4a_2, \\ b_4 = 2a_4 + a_1a_3, \\ b_6 = a_3^2 + 4a_6, \\ b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{cases}$$

This definition raises many comments.

A non singular algebraic affine curve defined over K

The previous equation defines an algebraic affine curve since it is given by a polynomial in two variables in the affine plane. It is defined over K meaning that the coefficient of the equation are in K.
To any affine curve C given by an equation $C : f(x, y) = 0$, where $f \in K[x, y]$, one can associate the set of its *K-rational points*, *i.e.*

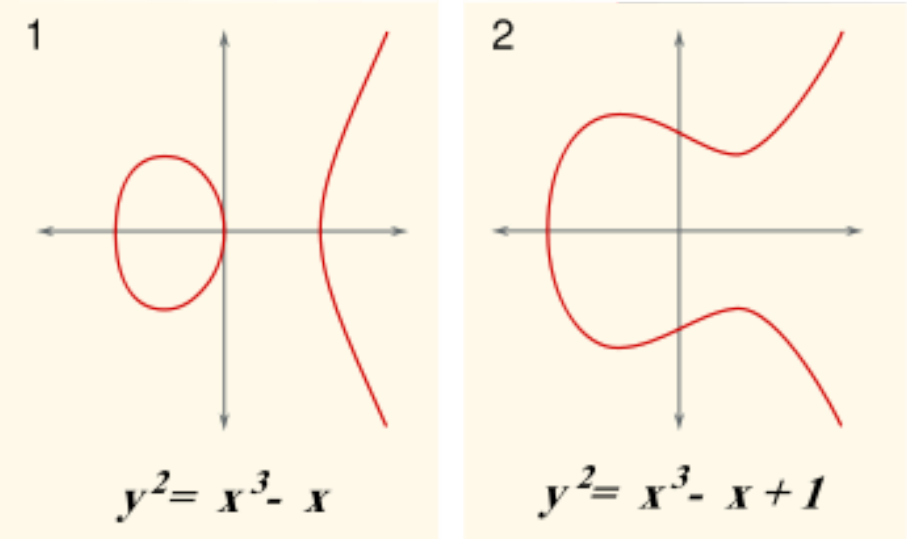
$$C(K) := \{(a, b) \in K^2,\ f(a, b) = 0\}.$$

Note that this set can be empty (for instance $x^2 + y^2 = -1$ over $\mathbb{R}$) so the set of points does not determine the equation of the curve. However if K is algebraically closed and if f is irreducible (check it looking at f as a polynomial of degree 2 in y) then f is uniquely determined by $C(K)$ up to a scalar multiplier. For this reason, it is important

to be able to consider the set of points of a curve C/K not only over K but over all extensions of K. In particular, we simply call a $\bar{K}$-rational point, a point of C.
The condition $\Delta \neq 0$ insures that E has no singular point. Let us check this in the case $a_1 = a_3 = a_2 = 0$ and $\operatorname{char} K \neq 2, 3$. A point $P = (a, b) \in E(\bar{k})$ is singular if and only if $\partial f/\partial x(a, b) = \partial f/\partial y(a, b) = 0$ where $f = y^2 - (x^3 + a_4 x + a_6)$. Hence we get

$$\begin{cases} 2b & = 0, \\ -(3a^2 + a_4) & = 0, \\ b^2 - (a^3 + a_4 a + a_6) & = 0. \end{cases}$$

It then means that $b = 0$ and a is a solution of $x^3 + a_4 x + a_6 = 0$ and its derivative, *i.e.* a is a double root. This can happen if and only if the discriminant of this polynomial is zero, *i.e.* if and only if $-(4a_4^3 + 27a_6^2) = 16\Delta = 0$.
Let us draw pictures over $\mathbb{R}$.



An abstract curve

We have not defined what an elliptic curve is! We only gave an equation of this object. One has to understand that an elliptic curve is an abstract object that can have many avatars (models), a model given by a Weierstrass equation being one. Here are other examples

1. Quartic equations: $y^2 = f(x)$ with f a degree 4 polynomial without multiple root;
2. Hessian model: $x^3 + y^3 + z^3 = dxyz$;
3. Intersection of quadrics in $\mathbb{P}^3$: $x^2 + z^2 = ayt$ and $y^2 + t^2 = axz$;

4. Edwards model: $x^2 + y^2 = 1 + dx^2y^2$.

To keep it simple, we will however often confuse the definition of an elliptic curve and of its (Weierstrass equation) but one has to keep in mind that in general **abstract curve $\neq$ a model of a curve $\neq$ an equation of the curve**.

1.1.2 Second definition

An affine version of a curve is often incomplete, for instance in terms of Bézout theorem. It is then better to consider a projective version.

Definition 1.1.2. A *(projective) Weierstrass equation* of an elliptic curve E over a field K is

$$\tilde{E} : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

where $a_1, a_2, a_3, a_4, a_6 \in K$ and $\Delta \neq 0$.

This is not surprising. More generally considering an affine curve $C : f(x, y) = 0$, one obtains its projective version by defining the curve $\tilde{C} : \tilde{f}(x, y, z) = 0$ where $\tilde{f}$ is the homogeneous polynomial associated to f, *i.e.* such that $\tilde{f}(x, y, 1) = f(x, y)$.
What does it means for the points of $\tilde{E}$? Recall that the K-rational points of the projective plane $\mathbb{P}^2$ are the projective points given by the equivalence classes of triples $(x, y, z) \in K^3 \setminus (0, 0, 0)$ under the multiplicative action of K^*. Since the projective equation of $\tilde{E}$ is homogenous, it makes sense to speak about equivalence classes $(x : y : z)$ which satisfy the equation of the curve and this defines the set $\tilde{E}(K)$. Among these points, we can distinguish

- The affine points of $\tilde{E}$, *i.e.* the ones with $z \neq 0$. We can hence find a representative with $z = 1$ and so with this normalization the affine points of $\tilde{E}$ are the points of E.

- The points at infinity of $\tilde{E}$, *i.e.* the ones with $z = 0$. Letting $z = 0$ in the equation, we get $x^3 = 0$ so there is a unique point at infinity which is denoted $O = (0 : 1 : 0)$.

By a change of coordinate, one can prove that the point O is non singular : around O, we have the affine equation $z + a_1xz + a_3z^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$ and the derivatives with respect to x and z at the point O are 0 and 1. Hence the model $\tilde{E}$ is a non-singular projective curve. Since E and $\tilde{E}$ are so closely related, we often forget the adjective projective or the $\tilde{}$ in our speech.

1.1.3 Third definition

Just for sake of completeness, let us give the abstract definition of an elliptic curve.

Definition 1.1.3. An elliptic curve over a field K is a projective non-singular curve of genus 1 with a K-rational point O.

The genus is a 'topological invariant' which is a non negative integer. Hence if two curves have different genus they cannot be transformed into each other in a contineous way without introducing singulairities. This hence defines a stratification of the set of curves with growing 'complexity' according to the genus. Note that the genus 0 algebraic curves are the one which admit a parametrization, for instance the conics, *i.e.* plane curves given by a projective equation of degree 2. One can prove that an elliptic curve does not admit a parametrization. Since it can be given by a degree 3 equation, this is somehow the simplest example after the conics. Note that if Δ would be zero we can see that we can get a parametrization.

Remark 1.1.4. To go even further and make the link with our initial definition, we'd have to use Riemann-Roch theorem to see that we can obtain an embedding of our abstract curve as a plane curve using the Riemann-Roch space associated to the divisor $3O$ (see [Sil92, Prop.III.3.1]).

Remark 1.1.5. At least, over $\mathbb{C}$, one can see that the genus of an elliptic curve is 1. First, one has to understand that an elliptic curve can be given as $\mathbb{C}$ modulo a lattice Λ through the so-called Weierstrass functions (see DH **??**). But $\mathbb{C}$ modulo a lattice is a complex torus and it is well known that the genus counts the number of holes in a compact Riemann surface.

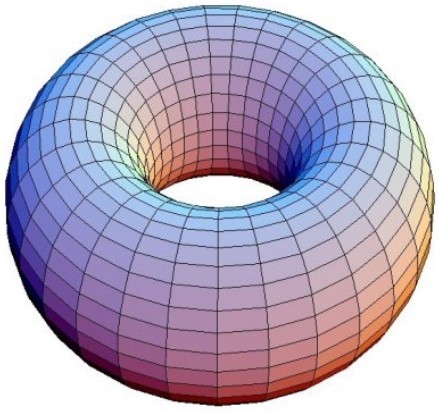


Figure 1.1: A complex torus

1.1.4 Isomorphisms

Between two algebraic varieties, there is a natural notion of morphisms which are 'maps described by polynomials'. We will choose an *ad hoc* definition for isomorphisms between Weierstrass models.

Definition 1.1.6. Two elliptic curves E_1 and E_2 defined over K and given by Weier-

strass equations

$$\begin{aligned} E_1 &: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \\ E_2 &: y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6, \end{aligned}$$

are said to be *isomorphic over* K if there exist $u, r, s, t \in K$ with $u \neq 0$ such that the change of variables

$$(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t)$$

transform the equation of E_1 into the equation of E_2 (up to a non-zero scalar multiplier of course).
If $E_2 = E_1$, such a transformation is called an *automorphism* of E_1.

If the characteristic of K is different from 2, one can simplify a Weierstrass model by completing the square on the left, *i.e.* replacing y by $y - a_1/2x - a_3/2$ we get $y^2 = x^3 + b_2/4x^2 + b_4/2x + b_6/4$ where the b_i are defined in Sec.1.1.1.
Moreover if the characteristic of K is different from 3, one can eliminate the coefficient in front of x^2, getting a *simplified Weierstrass model* of the form $y^2 = x^3 + ax + b$. As the properties we are interested in do not depend on a model up to isomorphism (over K) we will often consider this model when the characteristic is not 2 or 3.

Is there a simple way to see if two Weierstrass models are isomorphic over an algebraically closed field K ? Such a classical problem is part of the general theory of invariants and in this case the answer is simple. Let us start with two simplified Weierstrass models: $y^2 = x^3 + ax + b$ and $y^2 = x^3 + a'x + b'$. It is easy to see that the only possible transformation is $a = u^4a'$ and $b = u^6b'$ for some $u \in K^*$. There exists such an u if and only if $a'^3/b'^2 = a^3/b^2$. However this has no sense if b or b' is zero. There is one quantity which we know is never 0: the discriminant Δ. Here we have $\Delta = -16(4a^3 + 27b^2)$ and $\Delta' = -16(4a'^3 + 27b'^2)$. Hence we can get the same result using the well defined *j-invariant*

$$j := -1728(4a^3)/\Delta.$$

Proposition 1.1.7. *Two simplified Weierstrass models are $\bar{K}$-isomorphic if and only if they have the same j-invariant. Moreover given $j_0 \in K$, there exists a Weierstrass model over K with j-invariant equal to j_0.*

Proof. The direct implication is trivial. Conversely assume that two simplified Weierstrass models have the same j-invariants, then from

$$(4a^3)/(4a^3 + 27b^2) = (4a')^3/(4a'^3 + 27b'^2),$$

we get

$$a^3b'^2 = a'^3b^2.$$

- if $a = 0$ then $b \neq 0$ (since $\Delta \neq 0$) and we can take $u = (b/b')^{1/6}$.

- if $b = 0$ then $a \neq 0$ and we can take $u = (a/a')^{1/4}$.
- if $ab \neq 0$ then we can take $u = (a/a')^{1/4} = (b/b')^{1/6}$.

Finally if $j_0 \neq 0$ or 1728 we can compute that the j-invariant of

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

is j_0. To complete the list one can use $y^2 + y = x^3$ with j-invariant 0 and $y^2 = x^3 + x$ with j-invariant 1728. □

This can be extended to all Weierstrass models (and then to characteristic 2 and 3) by defining $c_4 = b_2^2 - 24b_4$ and $j = c_4^3/\Delta$.

1.2 The group law

1.2.1 Definition

The main reason to care about elliptic curves is that they carry an interesting structure, namely their points form a group under a certain addition law that we will describe now. Let $P, Q \in E$ be two points and L be the line connecting P and Q (tangent to E if $P = Q$) and R be the third point of intersection of L with E by Bézout. Let L' be the line connecting R and O. Then $P + Q$ is the residual point of intersection of L' and E.

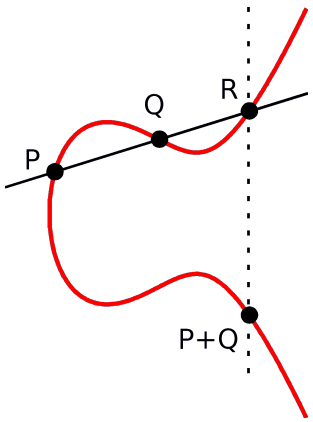


Figure 1.2: Addition on an elliptic curve

Theorem 1.2.1. *Let E/K be an elliptic curve. The previous operation is a commutative group law on $E(K')$ for all extensions K' of K.*

Proof. One has to prove several facts:

- $P + O = P$;
- $P + Q = Q + P$;
- if $P \in E$ then there exists a point Q such that $P + Q = O$;
- if $P, Q \in E(K)$ then $P + Q \in E(K)$;
- for $P, Q, R \in E$ one has $(P + Q) + R = P + (Q + R)$;

Only the last point is not obvious. It can be proved by direct computation with coordinates of the points see TP 4. Another geometric proof is given in [Ful89, p.124]. □

1.2.2 Torsion points

Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over a field K. Since $E(\bar{K})$ is a group we can consider for all $m \in \mathbb{Z}$ the homomorphism $[m] : E(\bar{K}) \to E(\bar{K})$ which associate to a point P the point mP. This map is given by polynomial expressions and is then a morphism of curves. For a general elliptic curve over a field of characteristic 0, these endomorphisms are the only ones and so $\mathrm{End}(E) \simeq \mathbb{Z}$.

Remark 1.2.2. Here we consider only group endomorphisms. Obviously any translation by a point of E is also a morphism.

What is the structure of $E[m] := \ker([m])$? To answer this question, we need the following lemma.

Lemma 1.2.3.

If m is prime to p then the map $[m]$ is separable and $\#\ker([m]) = \deg(m) = m^2$.

Proof. The first fact comes easily from the action of $[m]$ on the regular differential and general results from algebraic geometry [Sil92, Cor.III.5.4]. The first equality can be proved using [Sil92, Prop.II.2.6,Th.III.4.10]. The second equality can be derived using duality [Sil92, Cor.III.6.4], an explicit computation with division polynomials [Was03, Sec.3.2] or an analogy this the complex torus over $\mathbb{C}$. □

Hence $\ker([m])$ when m is prime to p is a commutative group of order m^2 which is killed by multiplication by m: there is only one which is $(\mathbb{Z}/m\mathbb{Z})^2$.
The importance of this $\mathbb{Z}/m\mathbb{Z}$-module (even a vector space when m is prime) is that it makes us able to linearize algebraic properties and to study them with classical tools of linear algebra.

Remark 1.2.4. When $m = p^r$, one has either $\#ker([m]) = 1$ or m.

1.2.3 The Weil pairing

The Weil pairing on the n-torsion points is a major tool in the study of elliptic curves. it has also important applications in cryptography. Let E be an elliptic curve over a perfect field K and let n be an integer not divisible by the characteristic of K. Then $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$. Let $\mu_n = \{x \in \bar{K} | x^n = 1\}$ be the group of nth roots of unity in $\bar{K}$. It is a cyclic group of order n and any generator ζ of μ_n is callaed a *primitive nth root of unity.*

Theorem 1.2.5. *There exists a pairing*

$$e_n : E[n] \times E[n] \to \mu_n$$

called the Weil pairing. *It satisfies the following properties:*

1. *e_n is bilinear in each variable. This means that*

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$

   and

$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2).$$

2. *e_n is alternated: $e_n(T, T) = 1$ for all $T \in E[n]$ and $e_n(T, S) = e_n(S, T)^{-1}$ for all $S, T \in E[n]$.*

3. *e_n is nondegenerate. This means that if $e_n(S, T) = 1$ for all $T \in E[n]$ then $S = O$ and also that if $e_n(S, T) = 1$ for all $S \in E[n]$ then $T = O$.*

4. *$e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$ for all automorphisms $\sigma \in \mathrm{Gal}(\bar{K}/K)$.*

5. *$e_n(u(S), u(T)) = e_n(S, T)^{\deg(u)}$ for all (separable) endomorphisms $u \in \mathrm{End}_{\bar{K}}(E)$.*

We will give proofs for this theorem in the last chapter. Presently we'll derive some consequences.

Corollary 1.2.6. *Let $\{T_1, T_2\}$ be a basis of $E[n]$. Then $e_n(T_1, T_2)$ is a primitive nth root of unity.*

Proof. Suppose $e_n(T_1, T_2) = \zeta$ with $\zeta^d = 1$. Then $e_n(T_1, dT_2) = 1$. Let $S \in E[n]$ then $S = aT_1 + bT_2$ therefore

$$e_n(S, dT_2) = e_n(T_1, dT_2)^a e_n(T_2, dT_2) = 1$$

which implies $dT_2 = O$ and so $n|d$. □

If u is an endomorphism, we obtain the action of u on the n-torsion by a matrix $u_n = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with entries in $\mathbb{Z}/n\mathbb{Z}$ describing the action of u on a basis $\{T_1, T_2\}$ of $E[n]$.

Corollary 1.2.7. *We have* $\det(u_n) \equiv \deg(u) \pmod{n}$.

Proof. By Corollary 1.2.6, $\zeta = e_n(T_1, T_2)$ is a primitive nth root of unity. Then using Theorem 2.1.14

$$\begin{aligned} \zeta^{\deg(u)} &= e_n(u(T_1), u(T_2)) = e_n(aT_1 + cT_2, bT_1 + dT_2) \\ &= e_n(T_1, T_2)^{ab} e_n(T_1, T_2)^{ad} e_n(T_2, T_1)^{cb} e_n(T_2, T_2)^{cd} \\ &= \zeta^{ad-bc}. \end{aligned}$$

Hence we get the result. □

2 Elliptic curves over finite fields

2.1 Number of points on elliptic curves over finite fields: theory

2.1.1 An example and an easy result

Example 2.1.1. Let us consider the elliptic curve $E : y^2 = x^3 + 2$ over $\mathbb{F}_7$. One has

$$E(\mathbb{F}_7) = \{O, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}.$$

Hence there is 9 points on this curve.

Could we predict this result ? Or at least give bounds for the number of points of an elliptic curve over a finite field k ? An obvious upper bound since for all $x \in k$, there are at most two y which are solutions is $2q + 1$. Can we do better ?

Example 2.1.2. The elliptic curve $E : y^2 + y = x^3 + x + 1$ has only O as rational point over $\mathbb{F}_2$.

Are there other examples of elliptic curves with no affine rational points ? Infinitely many ?

2.1.2 Hasse-Weil bound: first proof

We have seen that when $p = 0$ then in general the only endomorphisms are the multiplication by $[m]$. However, when $K = k = \mathbb{F}_q = \mathbb{F}_{p^n}$ is a finite field, there exists another important morphism: the Frobenius endomorphism $\phi_q : E \to E$ which maps a point $(x, y) \in E(\bar{k})$ to (x^q, y^q). Let us check that it is an endomorphism of E :

$$(y^q)^2 + a_1 x^q y^q + a_3 y^q = (y^2 + + a_1 xy + a_3 y)^q = (x^3 + a_2 x^2 + a_4 x + a_6)^q = (x^q)^3 + a_2 (x^q)^2 + a_4 x^q + a_6$$

since $x \mapsto x^q$ is k-linear. It also respect the addition since all the formulas have coefficients in k. Finally, for the same reason, it commutes with the action of $[m]$, hence the subring of $\mathrm{End}(E)$ generated by the multiplication maps $[m]$ and ϕ is a commutative ring and the composition of elements of this ring will be denoted multiplicatively.

Lemma 2.1.3. *A point $(x, y) \in E(\bar{k})$ belongs to $E(k)$ if and only if $\phi_q(x, y) = (x, y)$.*

Since $\phi_{q^r} = \phi_q^r$ for all $r \geq 1$, we have the following useful result.

Lemma 2.1.4. $\ker(\phi_q^r - 1) = E(\mathbb{F}_{q^r})$ *for all* $r \geq 1$.

To continue, we need the following facts.

Lemma 2.1.5.

- $\deg(\phi_q) = q$;
- *The map $\phi_q^r - 1$ is separable and so $\#\ker(\phi_q^r - 1) = \deg(\phi_q^r - 1)$;*
- *The degree map $d : \mathrm{End}(E) \to \mathbb{Z}$ is a positive definite quadratic form (i.e. L(a,b)=(d(a+b)-d(a)-d(b))/2 is $\mathbb{Z}$-bilinear).*

Proof. The first and second points can be proved using some algebraic geometry [Sil92, Prop.II.2.11,Cor.III.5.5]. Since $\deg(u) \geq 0$ and that the only morphisms of degree 0 are constant, it is clear that the map is positive definite. To prove that it is bilinear, we will use Corollary 1.2.7. Let $u, v, w \in \mathrm{End}(E)$ and let n be a prime big enough so that all equivalences of the degrees modulo n are equalities in $\mathbb{N}$. It is then enough to use the fact that the 2-dimensional determinant is a quadratic form to conclude. □

Cauchy-Schwarz inequality implies that $|d(a-b) - d(a) - d(b)| \leq 2\sqrt{d(a)d(b)}$. Using this with $a = \phi_q^r$ et $b = 1$, we get

$$\begin{aligned} |d(\phi_q^r - 1) - d(1) - d(\phi_q^r) - d(1)| &\leq 2\sqrt{d(1)d(\phi_q^r)} \\ |\#\ker(E(\mathbb{F}_{q^r})) - 1 - q^r| &\leq 2\sqrt{q^r}. \end{aligned}$$

The last inequality is known as *Hasse-Weil bound*.

2.1.3 Hasse-Weil bound: second proof

Let $q = p^e$, for an odd prime number p and an integer $e \geq 1$. Suppose $E/\mathbb{F}_q$ is an elliptic curve.

Theorem 2.1.6 (Hasse)**.** *If N_q denotes the number of rational points of $E/\mathbb{F}_q$, then*

$$|N_q - q - 1| \leq 2\sqrt{q}.$$

This second proof comes from Manin's article in 1956, explained by Cassels and then completed (for a missing details on the degrees) by Gel'fond and Linnik in 1966. The following part is extracted from the PhD thesis of Afzal Soomro, defended in 2013 who also generalized the proof to the characteristic 2 case.

Let $E/\mathbb{F}_q$ be given by an equation

$$E : \ y^2 = f(x) = x^3 + ax^2 + bx + c.$$

Consider

$$E^{\text{tw}} : \ f(t)y^2 = x^3 + ax^2 + bx + c. \tag{2.1}$$

The curve E^{tw} is a quadratic twist of $E/\mathbb{F}_q(t)$. The two curves E and E^{tw} are isomorphic over $K = \mathbb{F}(t, s)$, where $s^2 = f(t)$. The isomorphism is defined as follows:

$$E^{\text{tw}} \longrightarrow E$$

$$(x, y) \mapsto (x, sy).$$

It is easy to see that the points $Q = (t, 1)$ and $P_0 = (x_0, y_0) = (t^q, f(t)^{(q-1)/2})$ are in $E^{\text{tw}}(\mathbb{F}(t))$. We define

$$P_n = P_0 + nQ, \quad \forall\ n \in \mathbb{Z}.$$

If P_n is not the point at infinity O, set $P_n = (x_n, y_n)$. We write $x_n = f_n/g_n$, where $f_n, g_n \in \mathbb{F}_q[t]$, with $\gcd(f_n, g_n) = 1$. We get a well-defined function

$$d : \mathbb{Z} \to \ \{0, 1, 2, 3, ...\}$$

given by

$$d(n) = d_n = \begin{cases} 0 & \text{if } P_n = O; \\ \deg(f_n) & \text{otherwise.} \end{cases}$$

Since E^{tw} is not in the standard Weierstrass form, there will be modifications in the usual addition and duplication formulae.

(i) If $O \neq P_j = (x_j, y_j) \in E^{\text{tw}}(\mathbb{F}(t))$ and $P_1 \neq \pm P_2$, then

$$x(P_1 + P_2) = f(t)\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a - (x_1 + x_2) \tag{2.2}$$

(ii) If $P = (x, y) \in E^{\text{tw}}(\mathbb{F}(t))$ and $y \neq 0$, then

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}. \tag{2.3}$$

Now we present the properties of d_n.

Lemma 2.1.7. *If $P_n = (x_n, y_n) \neq O$, write $x_n = f_n(t)/g_n(t)$ with $f_n(t), g_n(t) \in \mathbb{F}[t]$. Then $\deg(f_n) > \deg(g_n)$.*

Proof. Suppose $\tau = 1/t$ and view E^{tw} over $\mathbb{F}((\tau))$. We change coordinates as follows:

$$\xi = \tau x \text{ and } \eta = y.$$

In these new coordinates the equation for E^{tw} is

$$(1 + a\tau + b\tau^2 + c\tau^3)\eta^2 = \xi^3 + a\tau\xi^2 + b\tau^2\xi + c\tau^3.$$

We denote by $v(f/g)$ the valuation of f/g seen as an element of $\mathbb{F}((\tau))$. We know that $v(f/g) = v(f) - v(g)$ and if $f \in \mathbb{F}[t]$ then $v(f) = -\deg(f)$. Namely, if $f = a_d t^d + \cdots + a_0$ with $a_d \neq 0$, then

$$\begin{aligned} f &= a_d \tau^{-d} + \cdots + a_0 \\ &= \tau^{-d}(a_d + a_{d-1}\tau + \cdots + a_0 \tau^d). \end{aligned}$$

Since $v(\tau^{-d}) = -d$ and $a_d + a_{d-1}\tau + \cdots + a_0\tau^d \in \mathbb{F}[[\tau]]^*$, we have $v(f) = -d = -\deg(f)$.

By reduction modulo τ, we obtain the curve

$$\bar{E}^{tw}/\mathbb{F} : \ \eta^2 = \xi^3.$$

We have a reduction map (see [Sil92, Chapter VII, Prop: 2.1])

$$\begin{array}{rcl} E_0^{\mathrm{tw}}(\mathbb{F}((\tau))) & \xrightarrow{mod\ \tau} & \tilde{E}_{ns}^{tw}(\mathbb{F}) \\ (\xi, \eta) & \mapsto & (\xi \pmod{\tau}, \eta \pmod{\tau}) \text{ if } \min(v(\xi), v(\eta)) = 0 \\ (\xi, \eta) & \mapsto & O \text{ if } v(\xi) \text{ or } v(\eta) < 0 \end{array}$$

where $E_0^{tw}(\mathbb{F}((\tau)))$ is the set of points in $E^{\mathrm{tw}}(\mathbb{F}((\tau)))$ whose reduction modulo τ is in $\bar{E}_{ns}^{tw}(\mathbb{F}) = \{(\xi, \eta) \neq (0,0), \eta^2 = \xi^3\} \cup O$, the set of non-singular points of $\bar{E}^{tw}$. To prove that $E_0^{tw}(\mathbb{F}((\tau)))$ is a group, it is enough to shod that $\bar{E}_{ns}^{tw}(\mathbb{F})$ is also for the law inherited from the classical addition law on E^{tw}. This is classical: the curve $y^2 z = x^3$ without the point $(0,0)$ is isomorphic to $\mathbb{A}^1$ by $(x, y) \mapsto x/y$ with inverse $x \mapsto (x : 1 : x^3)$. The group law $+$ on $\mathbb{A}^1$ induces a group law on the curve. This group law is the classical geometric one: it is enough to see that $x_1 + x_2 + x_3 = 0$ if and only if $P_1 + P_2 + P_3 = O$ (use the coordinates in (x, z)). Therefore $\bar{E}_{ns}^{tw}(\mathbb{F})$ is a group for the geometric group law. Hence, when we take $P_1, P_2 \in E_0^{tw}(\mathbb{F}((\tau)))$ then, by definition, their reduction is on $\bar{E}_{ns}^{tw}(\mathbb{F})$, so also the sum of their reduction. But this means that $P_1 + P_2$ has its reduction on $\bar{E}_{ns}^{tw}(\mathbb{F})$, so it is on $E_0^{tw}(\mathbb{F}((\tau)))$. This last set is also a group.

Let $P = (f/g, y) \in E^{\mathrm{tw}}(\mathbb{F}(t))$, where f and g are polynomials. In new coordinates ξ, η, the point $P = (\tau f/g, y) \in E^{\mathrm{tw}}(\mathbb{F}(t)) \subset E^{\mathrm{tw}}(\mathbb{F}((\tau)))$ (because $\xi = \tau x$. Note that

$$\begin{aligned} P \in E_0^{tw}(\mathbb{F}((\tau))) &\Leftrightarrow v\left(\frac{\tau f}{g}\right) \leq 0 \\ &\Leftrightarrow \deg(f) > \deg(g). \end{aligned}$$

Clearly the points $P = (t^q, f(t)^{(q-1)/2})$ and $Q = (t, 1)$ are in the group $E_0^{tw}(\mathbb{F}((\tau)))$ for all q. Therefore, $P_n = P_0 + nQ \in E_0^{tw}(\mathbb{F}((\tau)))$. This proves the lemma. □

Corollary 2.1.8. *If $P_n \neq O$ then $d_n > 0$, $\forall\ n \in \mathbb{Z}$.*

The following lemma gives the connection between N_q and d_n.

Lemma 2.1.9.

$$d_{-1} = N_q.$$

Proof. We compute d_{-1}. By the addition formula (2.2)

$$\begin{aligned} x(P_{-1}) &= x(P_0 - Q) \\ &= \frac{f(t)\left[f(t)^{(q-1)/2}+1\right]^2}{(t^q-t)^2} - a - (t^q+t) \\ &= \frac{f(t)^q + 2f(t)^{(q+1)/2} + f(t) - a(t^q-t)^2 - (t^{3q} - t^{2q+1} - t^{q+2} + t^3)}{(t^q-t)^2} \\ &= \frac{t^{2q+1} + \text{ a polynomial of lower degree}}{(t^q-t)^2}. \end{aligned}$$

We can write

$$t^q - t = \prod_{\alpha \in \mathbb{F}} (t - \alpha).$$

Therefore,

$$d_{-1} = 2q + 1 - \#\{\text{Cancellations of degree one factors}\}.$$

Now we count $\#\{\text{Cancellations of degree one factors}\}$. Suppose

$$f(t)\left[f(t)^{(q-1)/2}+1\right]^2 = N(t).$$

We have

$$x(P_{-1}) = \frac{N(t) - a\prod_{\alpha\in\mathbb{F}}(t-\alpha)^2 - (t_q - t)\prod_{\alpha\in\mathbb{F}}(t-\alpha)^2}{\prod_{\alpha\in\mathbb{F}}(t-\alpha)^2},$$

so $t - \alpha$ cancels (from both numerator and denominator) if and only if $N(\alpha) = 0$. For $t = \alpha \in \mathbb{F}$, if $f(\alpha) = 0$, then we have one cancellation. From equality

$$f(\alpha)^{(q-1)/2} = \begin{cases} -1 & \text{if } f(\alpha) \neq 0 \text{ is a non-square} \\ 1 & \text{if } f(\alpha) \neq 0 \text{ is a square,} \end{cases}$$

we see for $f(\alpha) \neq 0$ non-square we have a double cancellation. Also, if $f(\alpha) \neq 0$ is a square, there is no cancellation. Therefore

$$\begin{aligned} d_{-1} &= 1 + 2q - \#\{\alpha \in \mathbb{F} | f(\alpha) = 0\} - 2 \cdot \#\{\alpha \in \mathbb{F} | f(\alpha) \neq 0, \neq \square\} \\ &= 1 + 2 \cdot \{\alpha \in \mathbb{F}\} - \#\{\alpha \in \mathbb{F} | f(\alpha) = 0\} - 2 \cdot \#\{\alpha \in \mathbb{F} | f(\alpha) \neq 0, \neq \square\} \\ &= 1 + 2 \cdot \#\{\alpha \in \mathbb{F} | f(\alpha) \neq 0, = \square\} + \#\{\alpha \in \mathbb{F} | f(\alpha) = 0\} \\ &= N_q. \end{aligned}$$

This proves the lemma. □

Lemma 2.1.10. *The integers d_n satisfy the identity*

$$d_{n-1} + d_{n+1} = 2d_n + 2.$$

Proof. Take P_{n-1}, P_n and P_{n+1}. We consider the following two cases.

Case 1: One of P_{n-1}, P_n and P_{n+1} is O. By definition, $P_n = P_{n-1} + Q = P_{n+1} - Q$, for every $n \in \mathbb{Z}$.

(i) If $P_n = O$, then $P_{n-1} = -(t, 1)$ and $P_{n+1} = (t, 1)$. Therefore, $d_{n-1} = 1$ and $d_{n+1} = 1$. The lemma follows.

(ii) If $P_{n-1} = O$, then $P_n = (t, 1)$ and $P_{n+1} = 2(t, 1)$. By the duplication formula (2.3),

$$x(P_{n+1}) = \frac{t^4 - 2bt^2 - 8ct + b^2 - 4ac}{4t^3 + 4at^2 + 4bt + 4c}. \tag{2.4}$$

We can write this as

$$x(P_{n+1}) = \frac{\frac{df(t)}{dt} - (4a + 2t)f(t)}{4f(t)}.$$

Since $f(t)$ does not have multiple roots, we have (2.4) in lowest form and $d_{n+1} = 4$. This proves the lemma.

(iii) If $P_{n+1} = O$, then the same argument proves the the lemma in this case.

Case 2: None of P_{n-1}, P_n and P_{n+1} is O. Recall that we introduced the notation $P_i = (f_i/g_i, y_i)$ whenever $P_i \neq O$, where $f_i, g_i \in \mathbb{F}[t]$ are coprime, and $y_i \in \mathbb{F}(t)$. By the addition formula (2.2), applied to $P_{n-1} = P_n - Q$, one has

$$\begin{aligned}
\frac{f_{n-1}}{g_{n-1}} &= \frac{-(tg_n + f_n)(tg_n - f_n)^2 - ag_n(tg_n - f_n)^2 + f(t)g_n^3(1 + y_n)^2}{g_n(tg_n - f_n)^2} \\
&= \frac{(tg_n + f_n)(bg_n + tf_n) + 2g_n(af_n + cg_n) + 2f(t)g_n^2 y_n}{(tg_n - f_n)^2} \\
&= \frac{R}{(tg_n - f_n)^2},
\end{aligned} \tag{2.5}$$

say. Replacing y_n by $-y_n$ in the formula above, one obtains $x(-P_n - Q) = x(-P_{n+1}) = x(P_{n+1})$. Therefore,

$$\begin{aligned}
\frac{f_{n+1}}{g_{n+1}} &= \frac{-(tg_n + f_n)(tg_n - f_n)^2 - ag_n(tg_n - f_n)^2 + f(t)g_n^3(1 - y_n)^2}{g_n(tg_n - f_n)^2} \\
&= \frac{(tg_n + f_n)(bg_n + tf_n) + 2g_n(af_n + cg_n) - 2f(t)g_n^2 y_n}{(tg_n - f_n)^2} \\
&= \frac{S}{(tg_n - f_n)^2},
\end{aligned} \tag{2.6}$$

say.

Remark 2.1.11. The assumption $P_{n\pm1} \neq O$ is equivalent to $P_n \neq \pm Q$, or $x(P_n) = f_n/g_n \neq t$. Since in Case 2 above $P_n \neq O$, this means $x(P_n) = f_n/g_n \neq t$, i.e., $f_n \neq tg_n$.

Suppose $P_n \neq O$, so that coprime polynomials f_n and $g_n \in \mathbb{F}[t]$ exist with $x(P_n) = f_n/g_n$. Put $y_n := y(P_n)$ as above. Then

$$f(t)y_n^2 = \frac{f_n^3}{g_n^3} + a\frac{f_n^2}{g_n^2} + b\frac{f_n}{g_n} + c,$$

hence $(f(t)g_n^2 y_n)^2 \in \mathbb{F}[t]$, which implies $f(t)g_n y_n \in \mathbb{F}[t]$. Therefore, R and S are also polynomials. Moreover, f_{n-1}/g_{n-1} and f_{n+1}/g_{n+1} are in lowest form; by multiplying them, we get

$$\begin{aligned}\frac{f_{n-1}f_{n+1}}{g_{n-1}g_{n+1}} = \frac{RS}{(tg_n - f_n)^4} &= \frac{(tf_n - bg_n)^2 - 4cg_n\left[(t+a)g_n + f_n\right]}{(tg_n - f_n)^2} \\ &= \frac{T}{(tg_n - f_n)^2},\end{aligned} \tag{2.7}$$

say. If we show that, up to a non-zero constant,

$$g_{n-1}g_{n+1} = (tg_n - f_n)^2, \tag{2.8}$$

up to the same constant, then

$$f_{n-1}f_{n+1} = (tf_n - ag_n)^2 - 4cg_n\left[(t+a)g_n + f_n\right].$$

Using Lemma 2.1.7, it follows that the right-hand-side of this expression has the same degree as $t^2 f_n^2$. Hence we get

$$\begin{aligned}d_{n-1} + d_{n+1} &= \deg(f_{n-1}f_{n+1}) \\ &= \deg(t^2 f_n^2) \\ &= 2d_n + 2.\end{aligned}$$

Now we prove (2.8). It follows from the second equality in (2.7) that $(tg_n - f_n)^2 \mid RS$. Write $(tg_n - f_n)^2 = R_1 S_1$ for certain $R_1, S_1 \in \mathbb{F}[t]$ such that $R_1 \mid R$ and $S_1 \mid S$. Since

$$\frac{f_{n-1}}{g_{n-1}} = \frac{R}{(tg_n - f_n)^2} = \frac{R}{R_1 S_1} = \frac{R/R_1}{S_1},$$

we get $g_{n-1} \mid S_1$. Similarly, we get $g_{n+1} \mid R_1$. Therefore,

$$g_{n-1}g_{n+1} \mid (tg_n - f_n)^2.$$

The equality (2.8) will follow if we prove that also

$$(tg_n - f_n)^2 \mid g_{n-1}g_{n+1}. \tag{2.9}$$

Suppose (2.9) is not true, then an irreducible polynomial $\lambda(t) \in \mathbb{F}[t]$ exists such that $v_\lambda((tg_n - f_n)^2) > v_\lambda(g_{n-1}g_{n+1})$, where v_λ is valuation on $\mathbb{F}(t)$ corresponding to $\lambda(t)$. We claim that λ and the valuation v_λ have the following properties.

(a) $v_\lambda((tg_n - f_n)^2) > 0$;

(b) $\lambda \nmid g_n$;

(c) $v_\lambda(T) > 0$;

(d) $v_\lambda(R) > 0$ and $v_\lambda(S) > 0$.

Property (a) is immediate from the assumption

$$v_\lambda((tg_n - f_n)^2) - v_\lambda(g_{n-1}g_{n+1}) > 0.$$

Since $v_\lambda((tg_n - f_n)^2) > 0$ by Property (a), the condition $\lambda \mid g_n$ would imply $\lambda \mid tg_n - (tg_n - f_n) = f_n$, violating the fact that g_n and f_n are coprime; hence, Property (b) follows.
To see Property (c), note that (2.7) implies

$$v_\lambda(f_{n-1}f_{n+1}) - v_\lambda(g_{n-1}g_{n+1}) = v_\lambda(T) - v_\lambda((tg_n - f_n)^2);$$

hence,

$$v_\lambda(T) - v_\lambda(f_{n-1}f_{n+1}) = v_\lambda((tg_n - f_n)^2) - v_\lambda(g_{n-1}g_{n+1}),$$

which by our assumption is strictly positive. This implies that $v_\lambda(T) > 0$.
Finally, to prove Property (d), note that we already saw that $(tg_n - f_n)^2 \mid RS$; hence, Property (a) implies that $\lambda \mid RS$. Therefore $\lambda \mid R$ or $\lambda \mid S$. Suppose $\lambda \nmid R$, then from (2.5), we get

$$v_\lambda(g_{n-1}) - v_\lambda(f_{n-1}) = v_\lambda((tg_n - f_n)^2) > 0.$$

Since $\gcd(f_{n-1}, g_{n-1}) = 1$, this implies $v_\lambda(f_{n-1}) = 0$; hence, the equality above reduces to

$$v_\lambda(g_{n-1}) = v_\lambda((tg_n - f_n)^2).$$

From (2.7), we now deduce

$$v_\lambda(f_{n+1}) - v_\lambda(g_{n+1}) = v_\lambda(T) > 0.$$

Since the polynomials f_{n+1} and g_{n+1} are co-prime, it follows that $v_\lambda(g_{n+1}) = 0$. Therefore,

$$v_\lambda(g_{n+1}g_{n-1}) = v_\lambda((tg_n - f_n)^2),$$

contradicting our initial assumption. Hence, indeed $\lambda \mid R$. An analogous argument shows that $\lambda \mid S$. Indeed, if $\lambda \nmid S$, then (2.6) shows

$$v_\lambda(g_{n+1}) - v_\lambda(f_{n+1}) = v_\lambda((tg_n - f_n)^2) > 0,$$

which implies $v_\lambda(f_{n+1}) = 0$ and $v_\lambda(g_{n+1}) = v_\lambda((tg_n - f_n)^2)$. Again applying (2.7) shows in this case that

$$v_\lambda(f_{n-1}) - v_\lambda(g_{n-1}) = v_\lambda(T) > 0$$

and $v_\lambda(g_{n-1}) = 0$. Therefore,

$$v_\lambda(g_{n+1}g_{n-1}) = v_\lambda((tg_n - f_n)^2),$$

which is a contradiction. This finishes the proof of the Properties $(a), (b), (c)$ and (d).

Properties (a) and (d) imply that the valuations at λ of

$$f(t)g_n^3(1-y_n)^2 = S + (tg_n + f_n)(tg_n - f_n)^2 + ag_n(tg_n - f_n)^2$$

and of

$$f(t)g_n^3(1+y_n)^2 = R + (tg_n + f_n)(tg_n - f_n)^2 + ag_n(tg_n - f_n)^2$$

are both positive, as is seen by considering the right-hand-side. Also, $v_\lambda((1-y_n)^2)$ and $v_\lambda((1+y_n)^2)$ can not both be positive: since $(1-y_n)+(1+y_n) = 2$ and the characteristic is not equal to 2, this would yield a contradiction. If we suppose $v_\lambda((1-y_n)^2) \leq 0$, then $v_\lambda(f(t)) > 0$ since $v_\lambda(f(t)g_n^3(1-y_n)^2) > 0$. Similarly, if $v_\lambda((1+y_n)^2) \leq 0$, it follows that $v_\lambda(f(t)) > 0$. So we conclude in all cases that $\lambda \mid f$.

By computing modulo $(tg_n - f_n)$ one clearly has $f_n \equiv tg_n \mod (tg_n - f_n)$; hence,

$$T \equiv \left[(t^2g_n - bg_n)^2 - 4cg_n((t-a)g_n + tg_n)\right] \mod (tg_n - f_n),$$

i.e.,

$$T \equiv g_n^2(t^4 - 2bt^2 - 8ct - 4ac + b^2) \mod (tg_n - f_n).$$

Properties $(a), (b)$, and (c) therefore show

$$\lambda \mid (t^4 - 2bt^2 - 8ct - 4ac + b^2) = \delta(t),$$

say. A calculation reveals that the resultant of δ and f equals the square of the discriminant of f, which is nonzero constant in $\mathbb{F}$. Since the resultant is an $\mathbb{F}[t]$- linear combination of f and δ, this contradicts the fact that f and δ are divisible by λ. So the lemma follows in this case. □

Remark 2.1.12. Note that the polynomial δ, appearing in the proof above, is precisely the numerator appearing in the formula for $x(2P)$.

From the above identity, we obtain that the function d_n can be expressed as a polynomial in n, as follows.

Lemma 2.1.13. *The function d_n satisfies*

$$d_n = n^2 + a_q n + q.$$

Proof. This follows by induction on n, using the Lemmas 2.1.10 and 2.1.9. □

Proof of Hasse's theorem. Consider the quadratic polynomial

$$d(x) = x^2 + a_q x + q.$$

Assume that Hasse's theorem were false for $E/\mathbb{F}$. This is equivalent to the statement $a_q^2 - 4q > 0$, which implies that $d(x)$ has two zeroes. Suppose $x_1 < x_2$ are two zeroes of the above polynomial. Note that the quadratic function $d(x)$ is negative at all values x between x_1 and x_2. By Lemma 2.1.13 and the definition of the number d_n, $d(x)$ takes non-negative values at all integers x. In particular, this implies that the interval (x_1, x_2) does not contain any integer. Hence taking $n = \lfloor x_1 \rfloor$ (the largest integer $\leq x_1$), we have

$$n \leq x_1 < x_2 \leq n + 1. \tag{2.10}$$

It is not possible that both $x_1, x_2 \in \mathbb{Z}$ since this would imply

$$n(n+1) = x_1 x_2 = q,$$

contradicting the fact that $n(n+1)$ in even and q is odd. As a consequence,

$$0 < x_2 - x_1 < 1.$$

This is impossible since $a_q^2 - 4q = (x_1 - x_2)^2$ is assumed to be a positive integer. Therefore,

$$a_q^2 - 4q \leq 0.$$

This completes the proof of Hasse's theorem. □

2.1.4 A case of the Weil conjectures

The previous result has a beautiful consequence.

Theorem 2.1.14. *Let E be an elliptic curve defined over $\mathbb{F}_q$. Let $a = q + 1 - \#E(\mathbb{F}_q)$. Then the Frobenius endomorphism satisfies the equation*

$$\phi_q^2 - [a]\phi_q + [q] = 0.$$

Moreover a is the unique integer such that

$$a \equiv \mathrm{Tr}((\phi_q)_m) \mod m$$

for all m coprime to p.

Proof. Let $u = \phi_q^2 - [a]\phi_q + [q]$. If u is not zero, then it has a finite kernel. We need to prove that u has a kernel which is infinite. To do so, let m be a positive integer coprime to p and

$$(\phi_q)_m = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}.$$

Since $\phi_q - 1$ is separable we have

$$\#\ker(\phi_q - 1) = \deg(\phi_q - 1) \equiv \det((\phi_q)_m - I) \equiv \alpha\delta - \beta\gamma - (\alpha + \delta) + 1 \pmod{m}.$$

On the other hand $\det((\phi_q)_m) \equiv \deg(\phi_q) \equiv q \pmod{m}$ and since $\#\ker(\phi_q - 1) = q+1-a$ one has

$$\mathrm{Tr}((\phi_q)_m) = \alpha + \delta \equiv a \pmod{m}.$$

By Cayley-Hamilton (if m is prime) or by a straightforward computation with matrices, we have

$$(\phi_q)_m^2 - [a]_m(\phi_q)_m + [q]_m I_m \equiv 0 \pmod{m}.$$

(Note that $X^2 - aX + q$ is the characteristic polynomial of $(\phi_q)_m$. This means that u is 0 on $E[m]$. As m can go to infinity, this means that u is 0. □

Definition 2.1.15. The polynomial $X^2 - aX + q$ is called the *characteristic polynomial of the Frobenius* (or Weil polynomial). The integer a is called the *trace of the elliptic curve.*

Remark 2.1.16. This formula is the first example of a beautiful theorem, true for any smooth projective (absolutely irreducible) algebraic variety over a finite field. This theorem is known as Weil conjectures.

2.1.5 Supersingular elliptic curves

Let E be an elliptic curve over $\mathbb{F}_q$. Remember that for the prime p, unlike other m coprime to p, one has $\#E[p] = p$ or 1.

Definition 2.1.17. The curve E is said *supersingular* if $E[p] = \{O\}$.

We can reformulate this definition in terms of the trace a.

Proposition 2.1.18. *The curve E is supersingular if and only if $a \equiv 0 \pmod{p}$.*

Proof. With the notation of Exercice 11, assume that $a \equiv 0 \pmod{p}$. One has

$$\#E(\mathbb{F}_{q^i}) = q^i + 1 - s_i \equiv 1 - s_i \pmod{p}.$$

Since $s_1 \equiv a \equiv 0 \pmod{p}$ by the induction formula $s_i \equiv 0 \pmod{p}$ so

$$\#E(\mathbb{F}_{q^i}) \equiv 1 \pmod{p}.$$

In particular there is no non-trivial p-torsion point.
Conversely, assume that $a \not\equiv 0 \pmod{p}$. The recurrence formula implies that $s_{i+1} \equiv a s_i \pmod{p}$ hence $s_i \equiv a^i \pmod{p}$. Fermat's little theorem implies that $a^{p-1} \equiv 1 \pmod{p}$ therefore $\#E(\mathbb{F}_{q^{p-1}}) = q^{p-1} + 1 - s_{p-1} \equiv 0 \pmod{p}$. This means that E has a non-trivial p-torsion point and so E is not supersingular. □

Corollary 2.1.19. *Suppose $p \geq 5$ is a prime. Then $E/\mathbb{F}_p$ is supersingular if and only if $a = 0$.*

2.2 Number of points on elliptic curves over finite fields: practice

With the development of elliptic cryptography and the use of elliptic curves over large finite fields, several methods have been created to compute very efficiently the number of points on these objects. Unfortunately, they often rely on deep consideration (cohomology, canonical lift, deformation, complex multiplication,...) and we will not be able to explain them here. However, we can give some easy ways to do this, but less secure or slower.

2.2.1 Counting points

When $p > 2$, we can always write our elliptic curve $E : y^2 = f(x)$ with $\deg f = 3$. Hence the number of points on $E(\mathbb{F}_p)$ is

$$1 + p + \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p} \right).$$

Obviously the complexity is $O(p)$ and one can reach in this way $p \approx 2^{30}$.

2.2.2 Baby steps-giant steps

This is based on Hasse-Weil bound

$$|p + 1 - \#E(\mathbb{F}_p)| < 2\sqrt{p}$$

The idea is to pick a random point $P \in E(\mathbb{F}_p)$ and to compute an integer $m \in (p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ such that $mP = 0$. If m is the only such number in the interval, it follows that $m = \#E(\mathbb{F}_p)$. It is easy and fast to pick a point P randomly by choosing an x and see if $f(x)$ is a square.

Remark 2.2.1. To avoid problem that m is not the only such number in the interval, Mestre showed that one can work simultaneously with the curve and its quadratic twist.

Actually, we do things a bit differently. Theorem 2.1.14 tells us that

$$[p + 1]P - [\#E(\mathbb{F}_p)]P = [k]P, \quad k \in \{-2\sqrt{p} + 1, \ldots, 2\sqrt{p} - 1\}.$$

If $R = [p + 1]P$, this means that $R = [k]P$. We are going to check this equality.

Baby steps : make a list of the first $s = \lceil \sqrt[4]{p} \rceil$ multiples of P and compute $R = [p + 1]P$. Note that we know $-jP$ as well. Check if $\pm jP = R$.

Giant steps : compute $Q = [2s]P$ and compute $R, R \pm Q, R \pm 2Q, \ldots R \pm tQ$ where $t = \lfloor 2\sqrt{p}/(2s) \rfloor \approx \sqrt[4]{p}$. As we can write $k = (2s)i + j$ with $i = \lfloor \frac{k}{2s} \rceil \in \{0, \pm 1, \ldots, \pm t\}$ (the closest integer) $R - [i]Q = [j]P$ is a match. Putting $m = p + 1 - (2s)i - j$ we get $mP = 0$ and we get an algorithm is $O(\sqrt[4]{p})$. This improves the previous method but it is still exponential.

2.2.3 To work with extensions

Let $E/\mathbb{F}_q$ be an elliptic curve over a small field where we can easily compute its number of points N. Let $t = 1+q-N$ and write $P(X) = X^2 - tX + q = (X-\alpha)(X-\beta)$. Then we can use the Exercise 11 to get the number of points over large extension: indeed the characteristic polynomial over $\mathbb{F}_{q^n}$ is given by the resultant of $P(X)$ and $z - X^n$. However, note that $\#E(\mathbb{F}_q)|\#E(\mathbb{F}_{q^n})$ hence we necessarily loose a bit of efficiency since we do not get a prime order. As there are also attacks for certain primes and certain degree extensions on the DL problem, this method is generally considered as less safe.

2.2.4 Schoof method

In 1985 Schoof was the first to describe a polynomial time algorithm to count the number of points on an elliptic curve E over a large prime field $\mathbb{F}_p$. In the remainder of this section, we will assume that $p > 3$ and

$$E : y^2 = x^3 + a_4 x + a_6 \text{ with } a_4, a_6 \in \mathbb{F}_p.$$

Recall that $|E(\mathbb{F}_p)| = p+1-t$ with t the trace of the Frobenius endomorphism p and by Hasse's Theorem we have $|t| \leq 2\sqrt{p}$. The main idea of Schoof's algorithm is to compute t modulo various small primes $\ell_1, \dots \ell_r$ such that $\prod_{i=1}^r \ell_i > 4\sqrt{p}$. The trace t can then be determined using the Chinese Remainder Theorem and the group order follows. If the largest prime ℓ_r is of order $O(\log p)$ then from the prime number theorem, it follows that r can be taken has $O(\log p/\log\log p)$.

Remark 2.2.2. Approximatively, we have indeed that $\prod_{i=1}^r \ell_i \approx \log p^{\log p/\log\log p} = \exp(\log\log p \cdot \log p/\log\log p) = p$

To illustrate the idea, we show how to compute $t \pmod 2$. Since p is an odd prime, we have $|E(\mathbb{F}_p)| \equiv t \pmod 2$, so $t \equiv 0 \pmod 2$ if and only if $E(\mathbb{F}_p)$ has a nontrivial $\mathbb{F}_p$-rational point of order two. The nontrivial points of order two are given by $(\xi_i, 0)$ with ξ_i a root of $X^3 + a_4X + a_6$. Therefore, if $X^3 + a_4X + a_6$ is irreducible over $\mathbb{F}_p$ we have $t \equiv 1 \pmod 2$ otherwise, $t \equiv 0 \pmod 2$. Note that the polynomial $X^3 + a_4X + a_6$ is irreducible over $\mathbb{F}_p$ if and only if $\gcd(X^3 + a_4X + a_6, X^p - X) = 1$. The computation of $t \pmod 2$ thus boils down to polynomial arithmetic modulo $X^3 + a_4X + a_6$.
More generally, we obtain the trace t modulo a prime $\ell > 2$ by computing with the ℓ-torsion points.

Remark 2.2.3. One can use powers of ℓ when ℓ is small as well to get higher congruences. We will not look at this.

Recall that the Frobenius endomorphism ϕ_p is defined by $\phi_p : E(\mathbb{F}_p) \to E(\mathbb{F}_p) : (x, y) \mapsto (x^p, y^p)$ and that it cancels its characteristic polynomial, i.e.

$$\phi_p^2 - [t]\phi_p + [p] = 0.$$

By restricting to nontrivial ℓ-torsion points $P \in E(\overline{\mathbb{F}}_p)$ we obtain the reduced equation in the $\mathbb{F}_\ell$-vector space $E[\ell](\overline{\mathbb{F}}_p)$

$$\phi_p^2(P) + [p_\ell]P = [t_\ell]\phi_p(P)$$

with $t_\ell \equiv t \pmod{l}$ and $p_l \equiv p \pmod{\ell}$ and $0 \leq t_\ell, p_\ell < l$.
$P = (x_1, y_1)$ is a nontrivial ℓ-torsion point if and only if x_1 is a root of the *ℓ-th division polynomial* F_ℓ (because $\ell > 2$, see Exercice 8 for F_3). The nontrivial ℓ-torsion points can therefore be described as the solutions of the system of equations

$$Y^2 - X^3 - a_4X - a_6 = 0, \quad F_\ell(X) = 0.$$

This implies that the equation

$$(X^{p^2}, Y^{p^2}) + [p_\ell](X, Y) = [t_\ell](X^p, Y^p)$$

holds modulo the polynomial $F_\ell(X)$ and $E(X, Y) = Y^2 - X^3 - a_4X - a_6$. To compute t_ℓ one simply try all $\tau \in \{0, \ldots, \ell - 1\}$ until we find the unique value τ for which the equation is true modulo $F_\ell(X)$ and $E(X, Y)$.

The computation of $[a](X, Y)$ is done using division polynomials and the classical formulas. Recall that for $\gcd(\ell, p) = 1$ we have $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and thus $\deg(F_\ell) = (\ell^2 - 1)/2$ (when $\ell \neq 2$). The computation of (X^{p^2}, Y^{p^2}) and (X^p, Y^p) modulo F_ℓ and $E(X, Y)$ clearly takes $O(\log p)$ multiplications in the ring $\mathbb{F}_p[X, Y]/(E(X, Y), F_\ell(X))$. Since $\deg F_\ell$ is of order $O(\ell^2)$, each of these multiplication takes $O(\ell^{2\mu} \log^\mu p)$ bit-operations (note that we can represent elements of $\mathbb{F}_p[X, Y]/(E(X, Y), F_\ell(X))$ as $P(X)Y + Q(X)$ with degree of Q and P less than degree of F_ℓ), so computing $t \pmod{\ell}$ requires $O(\ell^{2\mu} \log^{1+\mu} p)$ bit operations (as we have to do it $\log p$ when τ spans $0, \ldots, \ell - 1$). Summing over all primes ℓ_i this gives a complexity of $O(\log^{2+3\mu} p)$ bit-operations.

Remark 2.2.4. Recall that $1 < \mu \leq 2$ depends on the algorithm used for multiplication : school-book multiplication ($\mu = 2$), Karatsuba ($\mu = \log_2 3$) or FFT ($\mu = 1 + \epsilon$). The choice of Karatsuba or FFT only become relevant for very large fields (much more than crypto-sizes for FFT).

Note that if we could replace the division polynomials F_ℓ by alternative polynomials of lower degree, the complexity of the algorithm would drop considerably. This is part of the improvements of Atkin and Elkies leading to the so-called Schoof-Elkies-Atkin (SEA) algorithm. The last record is a computation with an elliptic curve over $\mathbb{F}_p$ with $p = 10^{2099} + 6243$.

3 Pairings

3.1 Review on divisors

We are going to assume that an elliptic curve is a genus 1 curve and that in this case, the Riemann-Roch theorem states that

$$\dim \mathcal{L}(D) = \deg(D)$$

for all divisor D on the curve of non negative degree.

Lemma 3.1.1 ([Sil92, Lem.III.3.3]). *Let E be an elliptic curve and $P, Q \in E$ then $(P) \sim (Q)$ if and only if $P = Q$.*

Proof. Let $D = (Q)$. Since $\deg(D) = 1$ then $\dim \mathcal{L}(D) = 1$ and since constants are in $\mathcal{L}(D)$ then it is only the constant. Hence $\operatorname{div} f = (P) - (Q)$ is equivalent to $f \in \mathcal{L}(D)$ hence f is constant and $P = Q$. □

Proposition 3.1.2 ([Sil92, Prop.III.3.4]). *Let E be an elliptic curve.*

1. *For every divisor $D \in \operatorname{div}^0(E)$ there exists a unique point $P \in E$ so that*

$$D \sim (P) - (O).$$

Let $\sigma : \operatorname{div}^0(E) \to E$ be the map given by this association.

2. *σ is surjective.*
3. *Let $D_1, D_2 \in \operatorname{div}^0(E)$. Then $\sigma(D_1) = \sigma(D_2)$ if and only if $D_1 \sim D_2$.*
4. *The inverse to σ is the map*

$$\begin{aligned} \kappa \quad : \quad & E \to \operatorname{Pic}^0(E) \\ & P \mapsto (P) - (O) \end{aligned}$$

5. *If E is given by a Weierstrass equation then the geometric group law on E and the group law induced from $\operatorname{Pic}^0(E)$ are the same.*

Proof. (1) We have that $\dim(\mathcal{L}(D+(O)) = 1$ so let f be a generator. Since $\operatorname{div}(f) \geq -D-(O)$ and $\deg(\operatorname{div}(f)) = 0$ it follows that

$$\operatorname{div}(f) = -D - (O) + (P)$$

for some $P \in E$. Hence $D \sim (P) - (O)$. Then using the lemma we see that P is unique.
(2) For any $P \in E$ we have $\sigma((P) - (O)) = P$.
(3) Let $D_1, D_2 \in \operatorname{div}^0(E)$ and set $P_i = \sigma(D_i)$. Then from the definition of σ

$$(P_1) - (P_2) \sim D_1 - D_2.$$

Hence $P_1 = P_2$ certainly implies that $D_1 \sim D_2$. Conversely we get $(P_1) \sim (P_2)$ hence by the lemma $P_1 = P_2$.
(5) For the last point, let E be given by a Weirstrass equation and $P, Q \in E$. It clearly suffices to show that

$$\kappa(P+Q) = \kappa(P) + \kappa(Q).$$

Let $f = \alpha X + \beta Y + \gamma Z$ a line L going through P, Q and let R be the third intersection point of L with E. Let $f' = \alpha' X + \beta' Y + \gamma' Z$ be the line through R and O. Then from the definition of the addition on E and the fact that the line $Z = 0$ intersects E at O with multiplicity 3, we have

$$\operatorname{div}(f/Z) = (P) + (Q) + (R) - 3(O)$$

and

$$\operatorname{div}(f'/Z) = (R) + (P+Q) - 2(O).$$

Hence

$$(P+Q) - (P) - (Q) + (O) = \operatorname{div}(f'/f) \sim 0.$$

So

$$\kappa(P+Q) - \kappa(P) - \kappa(Q) = 0.$$

□

Corollary 3.1.3 ([Sil92, Cor.III.3.5])**.** *Let E be an elliptic curve and $D = \sum n_P(P) \in \operatorname{div}(E)$. Then D is principal if and only if $\sum n_P = 0$ and $\sum n_P P = O$.*

3.2 The Weil pairing

Let E/K be an elliptic curve. For this section we fix an integer n prime to p. Let $T \in E[n]$, then there is a function f such that

$$\operatorname{div}(f) = n(T) - n(O).$$

Letting $T' \in E$ with $[n]T' = T$ (all non constant morphism is surjective), there is similarly a function g such that

$$\operatorname{div}(g) = \sum_{R \in E[n]} (T' + R) - (R).$$

One can easily check that $f \circ [n]$ and g^n have the same divisor, so after scaling we can assume that $f \circ [n] = g^n$. Now suppose that $S \in E[n]$ then for any point $X \in E$,

$$g(X+S)^n = f([n]X + [n]S) = f([n]X) = g(X)^n.$$

Hence we can define the *Weil pairing*

$$e_n : E[n] \times E[n] \to \mu_n$$

by $e_n(S,T) = g(X+S)/g(X)$. We need to check that it satisfies the properties we stated in Theorem 2.1.14.

Proof. (1) Linearity in the first factor is easy.

$$e_n(S_1+S_2,T) = \frac{g(X+S_1+S_2)}{g(X+S_1)}\frac{g(X+S_1)}{g(X)} = e_n(S_2,T)e_n(S_1,T).$$

For the second, let $f_1, f_2, f_3, g_1, g_2, g_3$ be functions as above for T_1, T_2 and $T_3 = T_1 + T_2$. Choose a function h with divisor $(T_1+T_2) - (T_1) - (T_2) + (O)$. Then $\operatorname{div}(f_3/(f_1f_2)) = n \operatorname{div} h$ so $f_3 = cf_1f_2h^n$ for some constant c. Compose with the multiplication by n-map, use $f_i \circ [n] = g_i^n$ and take n-th roots to find

$$g_3 = c' g_1 g_2 (h \circ [n]).$$

Now

$$\begin{aligned} e_n(S, T_1+T_2) &= \frac{g_3(X+S)}{g_3(X)} = \frac{g_1(X+S)g_2(X+S)h([n]X+[n]S)}{g_1(X)g_2(X)h([n]X)} \\ &= e_n(S,T_1)e_n(S,T_2). \end{aligned}$$

(2) Let τ_P be the translation by P. Then

$$\operatorname{div}\left(\prod_{i=0}^{n-1} f \circ \tau_{[i]T}\right) = n\sum_{i=0}^{n-1}([1-i]T) - ([-i]T) = 0.$$

Hence $\prod_{i=0}^{n-1} f \circ \tau_{[i]T}$ is constant and if we choose some T' with $[n]T' = T$ then $\prod_{i=0}^{n-1} g \circ \tau_{[i]T'}$ is also constant because its n-th power is the above product of the f's. Evaluating the product of g's at X and $X+T'$ yields

$$\prod_{i=0}^{n-1} g(X+[i]T') = \prod_{i=0}^{n-1} g(X+[i+1]T').$$

Now cancelling like terms gives

$$g(X) = g(X+[n]T') = g(X+T)$$

so

$$e_n(T,T) = g(X+T)/g(X) = 1.$$

(3) If $e_n(S,T) = 1$ for all $S \in E[n]$, so $g(X+S) = g(X)$ for all $S \in E[n]$ then $g = h \circ [n]$ (see [Sil92, III.4.10.b]) for some function h. But then

$$(h \circ [n])^n = g^n = f \circ [n]$$

so $f = h^n$. Hence $n \operatorname{div} h = \operatorname{div} f = n(T) - n(O)$ so $\operatorname{div} h = (T) - (O)$ and $T = O$.
(4) Let $\sigma \in \operatorname{Gal}(\bar{K}/K)$. if f, g are the functions for T then clearly f^σ and g^σ are the corresponding functions for T^σ. Then

$$e_n(S^\sigma, T^\sigma) = \frac{g^\sigma(X^\sigma + S^\sigma)}{g^\sigma(X^\sigma)} = e_n(S,T)^\sigma.$$

(5) Let $\{Q_1, \ldots, Q_k\} = \ker(u)$. Since u is separable then $k = \deg(u)$. Let

$$\operatorname{div}(f_T) = n(T) - n(O), \quad \operatorname{div}(f_{u(T)}) = n(u(T)) - n(O)$$

and

$$g_T^n = f_T \circ [n], \quad g_{u(T)}^n = f_{u(T)} \circ [n].$$

We have

$$\operatorname{div}(f_T \circ \tau_{-Q_i}) = n(T + Q_i) - n(Q_i).$$

Therefore

$$\begin{aligned} \operatorname{div}(f_{u(T)} \circ u) &= n \sum_{u(T'')=u(T)} (T'') - n \sum_{u(Q)=O} (Q) \\ &= n \sum_i ((T+Q_i) - (Q_i)) \\ &= \operatorname{div}(\prod_i f_T \circ \tau_{-Q_i}). \end{aligned}$$

For each i choose Q_i' with $nQ_i' = Q_i$. Then

$$g_T(P - Q_i')^n = f_T(nP - Q_i).$$

Consequently,

$$\begin{aligned} \operatorname{div}(\prod_i (g_T \circ \tau_{-Q_i'})^n) &= \operatorname{div}(\prod_i f_T \circ \tau_{-Q_i} \circ [n]) \\ &= \operatorname{div}(f_{u(T)} \circ u \circ [n]) \\ &= \operatorname{div}(f_{u(T)} \circ [n] \circ u) \\ &= \operatorname{div}(g_{u(T)} \circ u)^n. \end{aligned}$$

Therefore $\prod_i g_T \circ \tau_{-Q_i'}$ and $g_{u(T)} \circ u$ differ only by a constant.

The definition of e_n yields

$$\begin{aligned} e_n(u(S),u(T)) &= \frac{g_{u(T)}(u(X+S))}{g_{u(T)}(u(X))} \\ &= \prod_i \frac{g_T(X+S-Q_i')}{g_T(X-Q_i')} \\ &= \prod_i e_n(S,T) \\ &= e_n(S,T)^k = e_n(S,T)^{\deg(u)}. \end{aligned}$$

Note that it works also for the Frobenius endomorphism (even if it is not separable) since

$$e_n(\phi_q(S),\phi_q(T)) = \phi_q(e_n(S,T)) = e_n(S,T)^q$$

since ϕ_q is the q-th power on the element of $\bar{\mathbb{F}}_q$. □

3.3 Computation of the Weil pairing: practice

If we want to compute the Weil pairing for large values of n we need to find a proper way to avoid massive computations. Indeed, the definition of the Weil pairing involves a function g whose divisor includes contributions from all the n^2-torsion points of $E[n]$. We hence need another definition for the Weil pairing.

Theorem 3.3.1. *Let $S,T \in E[n]$ and let $D_S = (S) - (O)$ and $D_T = (T+R) - (R)$ for an n-torsion point R. Let f_S and f_T defined (up to a constant) by*

$$\operatorname{div}(f_S) = nD_S, \quad \operatorname{div}(f_T) = nD_T.$$

Then the Weil pairing is given by

$$e_n(S,T) = \frac{f_T(D_S)}{f_S(D_T)}.$$

By definition, $f_T(D_S) = \prod_{i=1}^r f_T(P_i)^{n_i}$ where $D_S = \sum_{i=1}^r n_i(P_i)$ (here we assume also that the support of $\operatorname{div}(f_T)$ is disjoint of the support of D_S). The proof of the theorem relies on Weil's reciprocity law, see [Sil92, Ex.III.3.16]. Using this new definition, one sees that one has to be able to compute values of the type $f_S(P)$ for a given point P and $\operatorname{div} f_S = n(S) - n(O)$. It is still time-consuming to produce directly a function f_S when n is large. However this can be done efficiently thanks to the following algorithm due to Victor Miller.

Definition 3.3.2. Let $m \in \mathbb{Z}, S \in E[n]$, one calls *Miller function* $f_{m,S}$ the function defined up to a scalar by

$$\operatorname{div}(f_{m,S}) = m(S) - (mS) - (m-1)(O).$$

Let $S_1, S_2 \in E$, we define the function $g_{S_1,S_2} = L_{S_1,S_2}/L_{S_1+S_2,-(S_1+S_2)}$ where $L_{S,T}$ is the line passing through S and T (possibly the tangent if $S = T$). Clearly from the definition of the addition law, one has

$$\mathrm{div}(g_{S_1,S_2}) = (S_1) + (S_2) - (S_1 + S_2) - (O).$$

By computing the divisors, one then sees that Miller functions can be built as follows: $f_{1,S} := 1$, and for $m_1, m_2 \in \mathbb{Z}$

$$\begin{aligned} f_{m_1+m_2,S} &= f_{m_1,S} \cdot f_{m_2,S} \cdot g_{[m_1]S,[m_2]S}, \\ f_{m_1 m_2,S} &= f_{m_1,S}^{m_2} \cdot f_{m_2,[m_1]S} = f_{m_2,S}^{m_1} \cdot f_{m_1,[m_2]S}. \end{aligned}$$

In particular

- $f_{m+1,S} = f_{m,S} \cdot g_{[m]S,S}$,
- $f_{2m,S} = f_{m,S}^2 \cdot g_{[m]S,[m]S}$,
- $f_{n,S} = f_S$.

This yields the following doubling and add algorithm:

Input: $S \in E[n]$, $P \in E[n]$, $n = (n_l, \ldots, n_0)_2$.
Output: $f_S(P)$
$R \leftarrow S, f \leftarrow 1$
for $(i \leftarrow l-1, i \geq 0, i--)$ **do**
  $f \leftarrow f^2 \cdot g_{R,R}(P)$
  $R \leftarrow [2]R$ } Doubling
if $(n_i = 1)$ **then**
    $f \leftarrow f \cdot g_{R,S}(P)$
    $R \leftarrow R + S$ } Addition
end if
end for
return f

Remark 3.3.3. This gives only half of the Weil pairing. It is then tempting to define a pairing only using this computation. It is indeed possible and leads to the notion of reduced Lichtenbaum-Tate pairing, see [CFA+06].

4 Travaux Dirigés

4.1 TD 1

4.1.1 Énoncés

Exercice 1 (Dessiner des courbes elliptiques sur $\mathbb{R}$)**.** On fera un tracé des courbes suivantes

$$E_1 : y^2 = x^3 - x + 1$$

et

$$E_2 : y^2 = x^3 - x$$

en étudiant le tableau de variations (domaine de définition, variations,...) des fonctions $\sqrt{x^3 - x + 1}$ et $\sqrt{x^3 - x}$.

Exercice 2 (j-invariant en caractéristique 2 et 3)**.** Vérifier à l'aide d'un logiciel de calcul formel que si deux modèles de Weierstrass sont isomorphes alors leurs j-invariants sont égaux.

Exercice 3 (Loi de groupe algébrique)**.** Écrire explicitement les coordonnées de $P + Q$ pour un modèle de Weierstrass simplifié dans le cas où P et Q sont distincts, distincts du point à l'infini et de somme non nulle. Ces formules sont-elles encore valables lorsque $P = Q$?

Vérifier qu'une addition nécessite une inversion (I), 2 multiplications (M) et 1 carré (S) sur K (on négligera les additions).

Exercice 4 (Associativité de la loi de groupe)**.** Grâce à un logiciel de calcul formel, montrer que la loi de groupe est associative (on se restreindra au cas générique de points distincts).

Exercice 5 (Préservation de l'addition par isomorphisme)**.** Montrer qu'un isomorphisme entre deux courbes elliptiques est un morphisme de groupes pour la loi usuelle sur les courbes.

Exercice 6 (Groupe des automorphismes)**.** Montrer que le groupe des automorphismes d'une courbe elliptique sur un corps algébriquement clos de caractéristique différente de 2 ou 3 est un groupe cyclique d'ordre 2 si le j-invariant est différent de 0 et 1728 (resp. 4 s'il est égal à 1728, resp. 6 s'il est égal à 0).

Remark 4.1.1. En caractéristiques 2 et 3, le groupe des automorphismes est plus gros et non abélien si $j = 0 = 1728$.

Exercice 7 (Forme de Legendre)**.** Mettre la courbe elliptique $E : y^2 = x(x-1)(x-\lambda)$ avec $\lambda \neq 0, 1$ sous forme de Weierstrass et montrer qu'alors

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

Montrer que si $j \neq 0, 1728$, il y a six valeurs distinctes de λ donnant ce j et que si λ_0 est une de ces valeurs alors les autres sont donnés par

$$\frac{1}{\lambda}, 1 - \lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda - 1}, \frac{\lambda - 1}{\lambda}.$$

Exercice 8 (Points de 2-torsion et de 3-torsion)**.** Soit $E : y^2 = x^3 + Ax + B$ une courbe elliptique en caractéristique $p \neq 2, 3$. Donner les coordonnées des points de 2-torsion et de 3-torsion.

4.1.2 Corrections

Correction exercice 1 Voir les dessins 1.1.1 du cours.

Correction exercice 2 Voir TP.

Correction exercice 3 Soient donc $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ deux points d'une courbe $E : y^2 = x^3 + Ax + B$. La droite passant par P et Q a pour pente $\lambda = (y_2 - y_1)/(x_2 - x_1)$ et a donc pour équation $y = \lambda x + \mu$ avec $\mu = (y_1x_2 - y_2x_1)/(x_2 - x_1)$. On remplace dans l'équation de la courbe $E : (\lambda x + \mu)^2 = x^3 + Ax + B$. On sait que les trois solutions en x de cette équation sont x_1, x_2 et x_3 l'abscisse du point $P+Q$. Comme $-(x_1 + x_2 + x_3)$ est le coefficient de degré 2 de l'équation $x^3 + Ax + B - (\lambda x + \mu)^2 = 0$ on obtient que $x_1 + x_2 + x_3 = -\lambda^2$ soit $x_3 = \lambda^2 - x_1 - x_2$. L'ordonnée y_3 du point $P + Q$ est donnée par $(-y_3 - y_1)/(x_3 - x_1) = \lambda$ soit $y_3 = y_1 - (x_1 - x_3)\lambda$. En résumé :

1. $\lambda = (y_2 - y_1)/(x_2 - x_1)$ (Une inversion et une multiplication) ;
2. $x_3 = \lambda^2 - x_1 - x_2$ (un carré) ;
3. $y_3 = y_1 - (x_1 - x_3)\lambda$ (une multiplication).

Ceci n'est plus valable si $P = Q$ car alors $x_2 = x_1$ et on ne peut calculer λ. On notera toutefois que

$$\frac{(y_2 + y_1)(y_2 - y_1)}{(y_2 + y_1)(x_2 - x_1)} = \frac{y_2^2 - y_1^2}{(y_2 + y_1)(x_2 - x_1)} = \frac{x_1^3 + Ax_1 + B - (x_2^3 + Ax_2 + B)}{(y_2 + y_1)(x_2 - x_1)} = \frac{x_1^2 + x_2^2 + x_1x_2 + A}{y_2 + y_1}$$

pour lequel il n'y a plus de problème lorsque $P = Q$ (mais à nouveau lorsque $Q = -P$).

Correction exercice 4 Voir TP.

Correction exercice 5 Remarquons tout d'abord que l'image du point à l'infini est encore le point à l'infini. En effet, l'isomorphisme $(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t)$ s'écrit en coordonnées projectives $(x : y : z) \mapsto (u^2x + rz : u^3y + u^2sx + tz : z)$. Ainsi l'image de $(0 : 1 : 0)$ est bien le point $(0 : 1 : 0)$. De plus puisque cette isomorphisme est affine, il préserve les droites et les tangentes et donc la construction géométrique de la somme de deux points (et du double d'un point).

Correction exercice 6 Puisque la caractéristique de k (algébriquement clos) est différente de 2 et 3, on peut supposer $E : y^2 = x^3 + Ax + B$. Les automorphismes de E sont donc de la forme $x' = u^2x$ et $y' = u^3y$ avec $u \in k^*$. On a alors $u^6y'^2 = u^6x'^3 + Au^2x' + B$ soit $y'^2 = x'^3 + A/u^4x' + B/u^6$. Il faut et il suffit donc que $A/u^4 = A$ et que $B/u^6 = B$. On distingue trois cas

1. $AB \neq 0$ *i.e.* le j-invariant de E est différent de 0 et de 1728 car $j = 1728 \cdot 4A^3/(4A^3 + 27B^2)$. Dans ce cas, on obtient $u^2 = \pm - 1$ c'est-à-dire $x' = x$ et $y' = \pm y$.

2. $B = 0$ alors on a la condition $u^4 = 1$ et le groupe des automorphismes est engendré par $x' = -x$ et $y' = iy$.

3. $A = 0$ alors on a la condtion $u^6 = 1$ et si on note j une racine cubique de l'unité, le groupe des automorphismes est engendré par $x' = jx$ et $y' = -y$.

Correction exercice 7 Voir TP.

Correction exercice 8 Par définition P est un point de 2-torsion ssi $2P = O$. La droite tangente à P doit donc être verticale. En regardant la dérivée de la fonction $\sqrt{x^3 + Ax + B}$, ceci se produit pour les zéros de $x^3 + Ax + B$ (et le point à l'infini). Les points de 2-torsion sont donc O et les 3 points $(x_i, 0)$ tel x_i est solution de $x^3 + Ax + B$ (les points sont distincts puisque le polynôme est sans facteur carré).
De même P est un point de 3-torsion ssi $3P = O$ *i.e.* $2P = -P$. La droite tangente en P doit donc recouper la courbe E en P uniquement : P est donc un point d'inflexion. On peut les calculer en étudiant la fonction $\sqrt{x^3 + Ax + B}$ ou comme les zéros de la hessienne $\det((\partial F/\partial x_i))$ où $F(x_1, x_2, x_3) = x_2^2 x_3 - x_1^3 - Ax_1 x_3^2 - Bx_3^3$. On peut aussi écrire $2P = -P$ algébriquement. Choisissons cette dernière possibilité. Soit $P = (x_0, y_0)$ différent du point à l'infini. On calcule $2P$ en calculant la pente λ de la tangente en P : $\lambda = -(3x_0^2 + A)/(-(2y_0)) = (3x_0^2 + A)/(2y_0)$. On raisonne comme à l'exercice 3 et on obtient que $3x_0 = \lambda^2$ soit

$$3x_0(4y_0^2) = 12x_0(x_0^3 + Ax_0 + B) = (3x_0^2 + A)^2$$

Ce qui nous donne l'équation

$$3x^4 + 6Ax^2 + 12Bx - A^2 = 0.$$

Les points de 3-torsion sont le point 0 et les points $(x_0, \pm y_0)$ où x_0 est solution de l'équation précédente.

4.2 TD 2

4.2.1 Énoncés

Exercice 9 (Quelques fonctionnalités de Sage)**.** Soit $E/\mathbb{F}_{101} : y^2 = x^3 + 3x + 5$. Demander à Sage

1. De donner l'ordre de $E(\mathbb{F}_{101})$ et de lister tous les points rationnels.
2. De donner le polynôme de Weil de la courbe.
3. De donner le polynôme de Weil de la courbe sur $\mathbb{F}_{101^2}$. Vérifier que ceci correspond à l'exercice 11.
4. Tracer les points de la courbe $E/\mathbb{F}_p : y^2 = x^3 + x + 1$ pour $p = 101, 2003$ et 10007.
5. Que remarquez-vous ?

Exercice 10 (Nombre minimum de points des courbes elliptiques)**.** En utilisant la borne de Hasse-Weil, démontrer que les seuls corps finis pour lesquels il existe une courbe elliptique sans point affine rationnel sont $\mathbb{F}_2$, $\mathbb{F}_3$ et $\mathbb{F}_4$. Pour chacun de ces corps, en utilisant l'ordinateur, trouver explicitement ces courbes.

Exercice 11 (Nombre de points sur les extensions)**.** Soit $E/\mathbb{F}_q$ une courbe elliptique de trace a. Soit α, β les racines du polynôme caractéristique du Frobenius ϕ_q. Montrer que $|\alpha| = |\beta| = \sqrt{q}$ (on commencera par montrer que $|a| \leq 2\sqrt{q}$).
Soit $s_i = \alpha^i + \beta^i$. Alors $s_0 = 2$, $s_1 = a$ et montrer que

$$s_{n+1} = as_n - qs_{n-1}.$$

En utilisant le fait que $X^{2i} - s_i X^i + q^i$ est divisible par $X^2 - aX + q$, exprimer en fonction de α, β le nombre de points de E sur une extension de degré i de $\mathbb{F}_q$.
Soit $Z(E,t) = \exp(\sum_{i=1}^{\infty} \#E(\mathbb{F}_{q^i})\frac{t^i}{i})$ la série formelle en t. Montrer que

$$Z(E,t) = \frac{1 - at + qt^2}{(1-t)(1-qt)}.$$

Exercice 12 (Une "famille de" courbes supersingulières)**.** Soit q impair et $q \equiv 2 \pmod 3$. Soit $B \in \mathbb{F}_q^*$. Montrer que la courbe elliptique $E : y^2 = x^3 + B$ est supersingulière (on commencera par montrer que tout élément de $\mathbb{F}_q$ a une unique racine cubique dans $\mathbb{F}_q$).

Exercice 13 (Nombres de courbes supersingulières)**.** Calculer à l'aide de l'ordinateur pour les 100 premiers p premiers, le nombre de classes de $\bar{\mathbb{F}}_p$-isomorphismes de courbes elliptiques supersingulières sur $\mathbb{F}_p$.

4.2.2 Corrections

Correction exercice 9 Voir TP.

Correction exercice 10 D'après Hasse-Weil $|E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$, donc $|E(\mathbb{F}_q)| \geq q + 1 - 2\sqrt{q} = (\sqrt{q} - 1)^2$. Ce nombre est strictement plus grand que 1 dès que $q > 4$. Puis voir TP.

Correction exercice 11 On sait que $\#E(\mathbb{F}_q) = q + 1 - a$, les bornes de Hasse-Weil donne donc $|a| \leq 2\sqrt{q}$. Puisque le polynôme caractéristique du Frobenius est $X^2 - aX + q$ on a que $\Delta = a^2 - 4q \leq 0$ avec égalité si et seulement si $a = \pm 2\sqrt{q}$. On a donc deux cas :

- Si $a = \pm 2\sqrt{q}$ (en particulier q est un carré) alors $X^2 \pm 2\sqrt{q} + q = (X \pm \sqrt{q})^2$ et le résultat est établi.
- Sinon les racines α et β sont complexe conjuguées donc $|\alpha| = |\beta|$ et puisque leur produit vaut q, on a le résultat.

Le deuxième résultat s'obtient facilement puisque

$$as_n - qs_{n-1} = (\alpha + \beta)(\alpha^n + \beta^n) - \alpha\beta(\alpha^{n-1}) + \beta^{n-1}) = \alpha^{n+1} + \beta^{n+1}.$$

Remarquons que $X^{2i} - s_i X^i + q^i = (X^i - \alpha^i)(X^i - \beta^i)$ et il est divisible par $(X - \alpha)(X - \beta)$ dans $\mathbb{Z}[X]$. Soit $Q(X) \in \mathbb{Z}[X]$ le quotient. On a alors

$$(\phi_q^i)^2 - (\alpha^i + \beta^i)\phi_q^i + q^i = Q(\phi_q)(\phi_q^2 - a\phi_q + q) = 0.$$

Puisque $\phi_q^i = \phi_{q^i}$ et que le polynôme caractéristique de ϕ_{q^i} est unique, on a que $\alpha^i + \beta^i$ est la trace de $E(\mathbb{F}_{q^i})$. Donc $\#E(\mathbb{F}_{q^i}) = q^i + 1 - s_i$.
Pour finir, il suffit de remarquer que

$$\#E(\mathbb{F}_{q^i}) \cdot \frac{t^i}{i} = \frac{t^i}{i} + \frac{(qt)^i}{i} - \frac{(\alpha t)^i}{i} - \frac{(\beta t)^i}{i}$$

et que $\sum_{i=1}^{\infty} \frac{(zt)^i}{i} = -\log(1 - zt)$.

Correction exercice 12 Puisque $q \equiv 2 \pmod 3$, $q - 1 = 1 + 3n$ donc 3 et premier à q et donc inversible modulo $q - 1$. Soit r tel que $3r = 1 + (q - 1)m$. Pour tout $a \in \mathbb{F}_q^*$ (pour $a = 0$ c'est clair), on a alors $(a^r)^3 = a^{3r} = a^{1+(q-1)m} = a \cdot (a^{q-1})^m = a$ car $\mathbb{F}_q^*$ est un groupe cyclique d'ordre $q - 1$. a^r est donc une solution de $x^3 = a$. La solution est de plus unique car si $x^3 = y^3$ (avec x et y non nuls) alors en appliquant r des deux côtés, on trouve $x = y$.
Pour toute valeur de $y \in \mathbb{F}_q$, il existe donc une unique solution à $y^2 - B = x^3$. La courbe E a donc $q + 1$ points (le 1 provient du point à l'infini). Sa trace est nulle donc la courbe est supersingulière.
Remarquez que toutes les courbes E ont même j-invariant égal à 0. On ne peut donc

pas vraiment parler de famille.

Correction exercice 13 Voir TP.

4.3 TD 3

4.3.1 Énoncés

Exercice 14. 1. Soit $E/\mathbb{Q} : y^2 = x^3+2x-2$. Montrer que E est une courbe elliptique.

2. et soit $P = (1, 1) \in E(\mathbb{Q})$. Calculer $2P$ et $3P$ "à la main" (en se servant de SAGE comme d'une grosse calculatrice) puis vérifier sur l'ordinateur.

3. Soit $E/\mathbb{F}_5 : y^2 = x^3 + x + 1$. Quel est son nombre de points rationnels ? Même question sur $\mathbb{F}_{5^2}$. Vérifier avec l'ordinateur. La courbe E est-elle supersingulière ?

4. Les courbes $E/\mathbb{F}_7 : y^2 = x^3 + x + 1$ et $E'/\mathbb{F}_7 : y^2 - 3xy - y = x^3 - x^2 + 2x + 2$ sont-elles isomorphes ? Sur $\bar{\mathbb{F}}_7$?

Exercice 15. Montrer que si une courbe est anomale sur $\mathbb{F}_q$ (i.e. son nombre de point est égal à au cardinal du corps de de base) elle ne l'est pas sur $\mathbb{F}_{q^2}$. En supposant la caractéristique différente de 2, montrer que si $(x, y) \in E(\bar{\mathbb{F}}_q)$ alors

$$q(x, y) = (x^q, y^q) + (x^{q^2}, -y^{q^2}).$$

Exercice 16. On considère les courbes suivantes sur $\mathbb{F}_2$, dites courbes de Koblitz

$$E_1 : y^2 + xy = x^3 + 1, \quad E_2 : y^2 + xy = x^3 + x^2 + 1.$$

1. Montrer que le polynôme de Weil de E_i est $P_i = X^2 - (-1)^i X + 2$.

2. Ces courbes sont-elles supersingulières ?

On considère maintenant $d > 1$ un entier et E_i sur $\mathbb{F}_{2^d}$ pour $i = 1, 2$.

3. Calculer l'ordre de E_i sur $\mathbb{F}_4$.

4. Existe-t-il un d tel que l'ordre de E_i est premier ?

5. Est-ce un inconvénient ou un avantage en cryptographie ?

L'opération du Frobenius $\phi_2 : (x, y) \mapsto (x^2, y^2)$ est rapide en caractéristique 2 pour une base bien choisie. On souhaite donc écrire la multiplication par un entier k en "base ϕ_2". Pour cela, remarquons que ϕ_2 annule P_i et que donc il correspond à une racine $\mu_i = (-(-1)^i + \sqrt{-7})/2$. Choisissons $i = 2$ et $\mu = \mu_2$. Comme l'anneau $\mathbb{Z}[\mu]$ est euclidien et que $|\mu| = 2$, on va pouvoir développer $k = \sum_{j=0}^{r} \epsilon_j \mu^j$ avec $\epsilon_j \in -1, 0, 1$ et ainsi $[k] = \sum_{j=0}^{r} [\epsilon_j] \phi_2^j$. On peut également procéder de manière plus simple en écrivant un élément de $\mathbb{Z}[\mu]$ comme $a + b\mu$ puis en effectuant la division euclidienne de a et b par 2 en remplaçant 2 par $\mu - \mu^2$.

6. Écrire 7 en base μ.

7. Écrire 7 en base 2.

8. Que remarque-t-on au niveau de la longueur du développement ?

4.3.2 Corrections

Correction exercice 15 Une courbe $E/\mathbb{F}_q$ est anomale si et seulement si sa trace $a = (q+1) - q = 1$. La trace de $E/\mathbb{F}_{q^2}$ est égale à $2q - a^2 = 2q - 1$ qui est toujours différent de 1.
L'endomorphisme de Frobenius ϕ_q sur $E/\mathbb{F}_q$ satisfait $\phi_q^2 - \phi_q + [q] = [0]$ d'où le résultat en prenant un modèle de Weirstrass de la forme $y^2 = f(x)$.

Correction exercice 16

1. Il suffit de calculer le nombre de points sur E_i et on a alors $\#E_i(\mathbb{F}_2) = 1 - t + 2$.

2. Ces courbes ne sont pas supersingulières puisque 2 ne divise pas la trace. Cette propriété reste vraie sur toute extension car elle est équivalente à $\#E_i[2](\bar{\mathbb{F}}_2) = 4$. L'attaque MOV ne fonctionne donc pas sur ces courbes.

3. Si $P_i = (X - \alpha)(X - \beta)$, le polynôme de Weil sur $\mathbb{F}_4$ s'écrit $(X - \alpha^2)(X - \beta^2) = X^2 - (4 - (\alpha + \beta)^2)X + 4$. Donc $\#E_1(\mathbb{F}_4) = \#E_2(\mathbb{F}_4) = 8$.

4. Non car $1 < \#E_i(\mathbb{F}_2) | \#E_i(\mathbb{F}_{2^d})$.

5. C'est un inconvénient car puisqu'on veut un grand facteur premier dans l'ordre de $E_i(\mathbb{F}_{2^d})$ il faudra augmenter la taille de d d'au moins 2 bits par rapport à l'optimum envisageable.

6. $$7 = 1+3(\mu-\mu^2) = 1+3\mu-3\mu^2 = 1+\mu+(\mu-\mu^2)\mu-\mu^2-(\mu-\mu^2)\mu^2 = 1+\mu-2\mu^3+\mu^4 = 1+\mu+\mu^5.$$

7. $7 = 1 + 2 + 2^2$.

8. $5 > 2 \cdot 2$, il semblerait que le développement soit de longueur au moins double. En considérant $2^{2n} = (\mu - \mu^2)^{2n} = \mu^{2n}(\mu - 1)^{2n}$ on voit que c'est le cas pour un nombre infini de valeurs.

9. Le doublement de la longueur du développement est problématique mais est contrebalancée par la rapidité du Frobenius. De plus il existe des algorithmes qui permettent de réduire la longueur du développement.

4.4 TD1 de géométrie algébrique

4.4.1 Énoncés

Exercice 17. Soit $C = V(F)$ une courbe affine plane définie sur un corps algébriquement clos.

1. Montrer que C est l'union de deux courbes planes affines si et seulement si F n'est pas la puissance d'un polynôme irréductible. Si ce n'est pas le cas, on dira que C est irréductible.

2. Montrer que toute courbe plane est une union finie de courbes irréductibles, appelées ses composantes irréductibles.

Exercice 18. Étudier les singularités de

1. L'astroïde $\mathcal{C} : (x^2 + y^2 - 1)^3 + 27x^2y^2$;

2. La conchoïde de Nicomède : $\mathcal{C} : (x^2 + y^2)(x - 1)^2 = 4x^2$ (cette courbe permet de trissecter un angle, cf. Kirwan F. complex algebraic curves p.25).

3. Les surfaces $\mathcal{S}_1 : xt - yz = 0$ et $\mathcal{S}_2 : x^3 + y^3 + z^3 + t^3 = 0$ puis la courbe de $\mathbb{P}^3$: $\mathcal{C} : \{xt - yz = 0,\ x^3 + y^3 + z^3 + t^3\} = \mathcal{S}_1 \cap \mathcal{S}_2$.

4. De même avec $\mathcal{S}'_1 : t^2 - yz = 0$ et $\mathcal{C}' = \mathcal{S}'_1 \cap \mathcal{S}_2$.

Exercice 19.

1. Soit $F(x, y, z)$ un polynôme homogène de degré d. Montrer (Relation d'Euler) que
$$x\frac{\partial F}{\partial x} + y\frac{\partial F}{\partial y} + z\frac{\partial F}{\partial z} = d \cdot F(x, y, z)$$
(on prendra la dérivée partielle de $F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x, y, z)$ par rapport à λ puis $\lambda = 1$).

2. Si d est premier à a la caractéristique du corps, en déduire que la courbe plane projective $\mathcal{C} : F = 0$ est singulière au point projectif $P_0 = (x_0 : y_0 : z_0)$ si et seulement si
$$(\frac{\partial F}{\partial x}(P_0), \frac{\partial F}{\partial y}(P_0), \frac{\partial F}{\partial z}(P_0)) = (0, 0, 0).$$

3. Si le point P_0 n'est pas singulier, une équation de la tangente est
$$\frac{\partial F}{\partial x}(P_0)x + \frac{\partial F}{\partial y}(P_0)y + \frac{\partial F}{\partial z}(P_0)z = 0.$$

4. Etudier les singularités de $\mathcal{C}_1/\mathbb{C} : y^2z = x^3$ sur $\mathbb{C}$ puis sur $\overline{\mathbb{F}}_2$.

Exercice 20. On appelle conique projective Q sur un corps k, une courbe plane donnée par un polynôme homogène de degré 2 qui est irréductible sur $\overline{k}$. On suppose que $\mathrm{char}(k) \neq 2$.

1. Supposons $k = \overline{k}$. Montrer qu'il existe un système de coordonnées (X, Y, Z) de $\mathbb{P}^2$ tel qu'une équation de la conique est $X^2 - YZ = 0$. En particulier Q est non singulière.

2. En déduire que Q est isomorphe à $\mathbb{P}^1$. Peut-on déduire un résultat similaire si k n'est pas algébriquement clos ?

3. Comment réalise-t-on géométriquement cet isomorphisme ?

4. Montrer que si $k = \mathbb{F}_q$ alors Q possède toujours un point rationnel. En déduire que Q est isomorphe à $\mathbb{P}^1$.

On suppose maintenant que $k = \mathbb{Q}$.

5. En utilisant la théorie des formes quadratiques, montrer qu'il existe une transformation projective définie sur $\mathbb{Q}$ telle que Q est isomorphe à $ax^2 + by^2 = z^2$ pour $a, b \in \mathbb{Q} \setminus \{0\}$.

6. Montrer que par une transformation diagonale supplémentaire, on peut supposer que a, b sont des entiers sans facteurs carrés et que $|a| \geq |b|$.

7. Montrer que si Q a un point rationnel alors b est un carré modulo tout p divisant a. En déduire que b est un carré modulo a. Il existe donc m, a_1 avec $|m| \leq |a|/2$ et $m^2 = b + aa_1$.

8. Montrer que si $m^2 = b + aa_1$ et que si $(x : y : z)$ est un point de Q alors

$$a_1(z^2 - by^2)^2 + b((my - z)x)^2 = ((mz - by)x)^2.$$

   En déduire que Q a un point rationnel si et seulement si il en est de même pour $a_1x^2 + by^2 = z^2$.

9. Montrer que si $|a| > 1$ alors $|a_1| < |a|$ et qu'on peut donc se ramener au cas où b n'est pas un carré modulo a ou $|a| = |b| = 1$ pour lequel il existe une solution si et seulement si au moins l'un des deux nombres est positif.

Exercice 21. On souhaite montrer des versions faibles du théorème de Bézout. Soit $F, G \in k[x, y]$ avec k algébriquement clos, sans facteur commun.

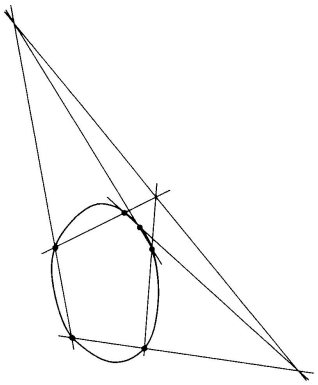
1. Montrer qu'il existe un polynôme $d \in k[x]$ non nul et des polynômes $A, B \in k[x, y]$ tels que $d = AF + BG$.

2. En déduire que l'intersection de $V(F)$ et $V(G)$ est finie.

3. La courbe $\{(t, \sin(t)), t \in \mathbb{C}\}$ est-elle algébrique ?

Une seconde version. Soit une courbe projective $C = V(F)$ avec $F \in k[x, y, z]$ homogène de degré $n > 0$. Soit L une droite du plan projective qui n'est pas une composante de C.

FIGURE 4.1 – Hexagone de Pascal



4. Montrer que $C \cap L$ est constitué d'au plus n points.

5. Soit p un point n'appartenant pas à C. Montrer qu'avec au plus $n(n-1)$ exceptions, une droite L passant par p coupe C en exactement n points.

Exercice 22. Montrer le résultat suivant :

Proposition 4.4.1. *Si deux courbes planes projectives $\mathcal{C}_1, \mathcal{C}_2$ sur $\mathbb{C}$ de degré n s'intersectent en exactement n^2 points et qu'il existe une courbe irréductible $\mathcal{D}$ de degré $m < n$ contenant mn de ces points alors il existe une courbe de degré au plus $n - m$ contenant les $n(n - m)$ points résiduels.*

Pour se faire on note P_1, P_2, R les équations respectives de $\mathcal{C}_1, \mathcal{C}_2$ et $\mathcal{D}$ et $p = [a : b : c]$ un point de $\mathcal{D}$ qui n'appartient pas à $\mathcal{C}_1 \cap \mathcal{C}_2$. Montrer qu'il existe une combinaison linéaire de P_1 et P_2 contenant p. Conclure en utilisant Bézout.

On utilisera ce résultat pour montrer le corollaire :

Corollary 4.4.2 (Hexagone mystique de Pascal). *Les paires de côtés opposés d'un hexagone inscrit dans une conique irréductible se rencontrent en trois points colinéaires.*

Exercice 23. Soit $\mathcal{C} : f = 0$ une courbe projective plane de degré 4. On suppose que $\mathcal{C}$ est non-singulière. Si L est une droite, elle peut couper $\mathcal{C}$ en des points avec les multiplicités suivantes :

1. $(1, 1, 1, 1)$: c'est le cas générique.

2. $(2, 1, 1)$: c'est le cas où L est tangente au premier point.

3. $(3, 1)$: dans ce cas, le premier point est un point d'inflexion.

4. $(2, 2)$: ces droites sont appelées bitangentes.

5. (4) : ces points sont appelés point d'hyperinflexion. Une quartique générale n'en possède pas.

Calculer les bitagentes à la quartique de Plücker

$$4(x^2+y^2+2y)^2+(2y+3)(y+1)(y^2-x^2)=-\frac{1}{360}.$$

Pour se faire, on remplace y par $\alpha x+\beta$ et z par 1 dans f puis on exprime le fait que la droite $y=\alpha x+\beta$ est bitangente par le fait que le polynôme en la variable x est un carré parfait : si g est un polynôme de degré 4 quelconque, on a

$$g(x)=ax^4+bx^3+cx^2+dx+e=a(x^2+b/(2a)x+(4ac-b^2)/(8a^2))^2+*\cdot x+*.$$

Ceci donne deux conditions, une sur le terme en x et l'autre sur le terme constant. Par le calcul d'un résultant on élimine par exemple β entre ces deux équations pour obtenir une condition sur α. Cette équation (de degré 28 génériquement) donne les valeurs de α puis on remonte aux valeurs de β. On traitera à part les cas des droites à l'infini ou 'verticales'.

4.4.2 Solutions

Correction exercice 17

1. Par le corollaire 5.1.8, si $F = \prod F_i^{e_i}$, on a aussi que $C = V(G)$ avec $G = F_1 \cdots F_r$ irréductibles distincts. Si $r > 1$ alors $C_1 = V(F_1)$ et $C_2 = V(F_2 \cdots F_r)$ sont deux courbes telles que $C = C_1 \cup C_2$ et $C_1 \neq C_2$ (en effet si $C_1 = C_2$ alors $I(C_1) = (F_1) = I(C_2) = (F_2 \cdots G_r)$ ce qui est impossible puisque les idéaux sont premiers entre eux). Si $r = 1$ alors on a que $C = V(F_1)$. S'il existait $C_1 = V(H) \subset C$ non trivial alors $I(F_1) \subset I(H)$ et donc H diviserait F_1, ce qui n'est pas possible.

2. on procède par une récurrence immédiate.

Correction exercice 18 Voir TP.

Correction exercice 19

1. Dérivons la composée de $g : \lambda \mapsto (\lambda x, \lambda y, \lambda z)$ avec la fonction $F : (x, y, z) \mapsto F(x, y, z)$ On a

$$\partial(F \circ g)/\partial\lambda = (\partial F/\partial x, \partial F/\partial y, \partial F/\partial z) \cdot {}^t(\partial\lambda x/\partial\lambda, \partial\lambda x/\partial\lambda, \partial\lambda x/\partial\lambda)$$

   qui donne le résultat. La dérivation du second membre est directe.

2. On choisit une carte affine autour du point qui nous intéresse. Comme l'équation est symétrique, supposons qu'il s'agisse d'un point avec $z_0 \neq 0$. Alors le point est singulier si et seulement si $\partial F(x, y, z)/\partial x = \partial F(x, y, z)/\partial y = 0$ en $(x_0, y_0, 1)$. Si cela est le cas alors on voit que $\partial F(x, y, z)/\partial z = 0$ puisque $F(x_0, y_0, z_0) = 0$. Inversement si un point vérifie que ses trois dérivées partielles sont nulles alors puisque d n'est pas nul, F est également nul et il est donc un point de la courbe.

3. Une équation affine de la tangente en $(x_0 : y_0 : 1)$ est

$$y - y_0 = -\frac{\partial F/\partial x}{\partial F/\partial y}(x_0, y_0, 1)(x - x_0).$$

   En développant, on obtient alors

$$\partial F/\partial x(P_0)x + \partial F/\partial y(P_0)y - (x_0\partial F/\partial x(P_0) + \partial F/\partial y(P_0)y_0) = 0.$$

   Le dernier terme vaut $\partial F/\partial z(P_0)$ puis en homogénéisant en $(x : y : z)$, on obtient le résultat.

4. Dans le premier cas, on obtient le vecteur dérivée : $(-3x^2, 2yz, y^2)$. Le point $(0 : 0 : 1)$ est donc l'unique point singulier sur $\mathbb{C}$ et sur $\mathbb{F}_2$.

Correction exercice 20

1. une quadrique est donnée par sa matrice symétrique et un changement de variables correspond à une forme quadratique équivalente. La classification sur $\bar{k}$ en caractéristique différente de 2 nous dit que celles-ci sont données par leur rang. On voit que les formes de rang 1 et 2 ne donnent pas des équations irréductibles. Si le rang est 3, on a donc a forme $x^2 + y^2 + z^2 = 0$ qui peut être transformée aisément en $X^2 - YZ = 0$. Les critères de singularité montrent que cette courbe est lisse.

2. On a l'isomorphisme $\mathbb{P}^1 \to Q$ donné par $(u : v) \mapsto (uv : u^2 : v^2)$ d'inverse $(x : y : z) \mapsto (y : x)$ si $(x, y) \neq (0, 0)$ et $(0 : 1)$ sinon. Cela ne marche pas sur $\mathbb{R}$ par exemple car la conique $x^2 + y^2 + z^2 = 0$ n'a pas de point réel alors que $\mathbb{P}^1$ en a.

3. On peut le réaliser en projetant la conique sur une droite à partir d'un point de celle-ci.

4. Écrivons Q sous la forme $ax^2 + by^2 = z^2$. Pour tout y, les fonctions $x \mapsto ax^2 + by^2$ et $z \mapsto z^2$ prennent $(q + 1)/2$ valeurs. Comme il y a q valeurs dans $\mathbb{F}_q$, il existe donc une valeur commune et donc un point sur Q.

5. La classification nous donne une forme $ax^2 + by^2 + cz^2 = 0$ avec a, b, c non nuls. En divisant par $-c$, on peut se ramener à la forme indiquée.

6. Si $a = a_1/a_2$ et $b = b_1/b_2$ on multiplie par $(a_2b_2)^2$ et on fait le changement de variables $z \mapsto (a_2b_2)z$. On a donc que a et b sont des entiers. Les facteurs carrés peuvent "rentrer" dans les x et y. Puis on peut intervertir x et y le cas échéant pour l'inégalité sur les normes.

7. Soit $(x_0 : y_0 : z_0)$ un point rationnel qu'on peut supposer à coordonnées entières premières entre elles. En réduisant modulo p on a donc que $by_0^2 \equiv z_0^2 \pmod{p}$. Si $y_0 \not\equiv 0 \pmod{p}$ c'est fini. Sinon on voit que $p|z_0$. En réinjectant dans l'équation on a alors que $p^2|ax_0^2$. Comme a est sans facteur carré, on aurait p qui divise aussi x_0. Exclu. Comme b est un carré pour tous les p divisant a et que a est sans facteur carré, le TRC nous montre que b est un carré modulo a. L'existence de m et a_1 est simplement la définition d'être un carré modulo a.

8. On développe l'expression (notons la A)

$$\begin{aligned} A &= a_1(ax^2)^2 + x^2(bm^2y^2 + bz^2 - 2bmyz - m^2z^2 - b^2y^2 + 2bmyz) \\ &= a_1a^2x^4 + x^2(m^2(by^2 - z^2) + b(z^2 - by^2)) \\ &= x^4(a_1a^2 - m^2a + ba) \\ &= 0 \end{aligned}$$

   Ainsi, si Q a un point rationnel alors l'équation A montre que $a_1x^2 + by^2 = z^2$ en a un également. En permutant les valeurs de a et de a_1 dans l'équation de A, puisque la condition $m^2 = b + aa_1$ est symétrique, on voit que l'on peut inverser le raisonnement et en déduire l'existence d'un point rationnel de Q en fonction d'un point rationnel de $a_1x^2 + by^2 = z^2$.

9. Puisque $|b| \leq |a|$, on a $|m^2 - b| \leq m^2 + |a| \leq a^2/4 + |a|$. D'où $|a_1| \leq |a|/4 + 1$. Puisque a est un entier et que $|a| > 1$ on peut supposer $|a| \geq 2$. On a donc que l'inégalité $|a_1| < |a|$ est satisfaite. En procédant récursivement, on peut donc à chaque fois que b est un carré modulo a, diminuer $|a|$ et donc $|b|$. La procédure s'arrête au moment où b n'est plus un carré modulo a (alors l'équation n'a pas de solution rationnelle d'après ce qui précède) ou alors $|a| = 1$ et donc $|b| = 1$. L'équation a une solution si et seulement si ab est négatif.

4.5 TD2 de géométrie algébrique

4.5.1 Énoncés

Exercice 24. On souhaite montrer des versions faibles du théorème de Bézout. Soit $F, G \in k[x, y]$ avec k algébriquement clos, sans facteur commun.

1. Montrer qu'il existe un polynôme $d \in k[x]$ non nul et des polynômes $A, B \in k[x, y]$ tels que $d = AF + BG$.

2. En déduire que l'intersection de $V(F)$ et $V(G)$ est finie.

3. La courbe $\{(t, \sin(t)), t \in \mathbb{C}\}$ est-elle algébrique ?

Une seconde version. Soit une courbe projective $C = V(F)$ avec $F \in k[x, y, z]$ homogène de degré $n > 0$. Soit L une droite du plan projective qui n'est pas une composante de C.

4. Montrer que $C \cap L$ est constitué d'au plus n points.

5. Soit p un point n'appartenant pas à C. Montrer qu'avec au plus $n(n-1)$ exceptions, une droite L passant par p coupe C en exactement n points.

Exercice 25. Montrer le résultat suivant :

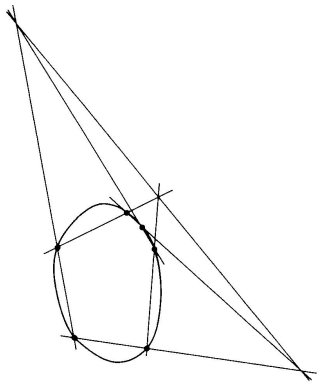
Proposition 4.5.1. *Si deux courbes planes projectives $\mathcal{C}_1, \mathcal{C}_2$ sur $\mathbb{C}$ de degré n s'intersectent en exactement n^2 points et qu'il existe une courbe irréductible $\mathcal{D}$ de degré $m < n$ contenant mn de ces points alors il existe une courbe de degré au plus $n - m$ contenant les $n(n - m)$ points résiduels.*

Pour se faire on note P_1, P_2, R les équations respectives de $\mathcal{C}_1, \mathcal{C}_2$ et $\mathcal{D}$ et $p = [a : b : c]$ un point de $\mathcal{D}$ qui n'appartient pas à $\mathcal{C}_1 \cap \mathcal{C}_2$. Montrer qu'il existe une combinaison linéaire de P_1 et P_2 contenant p. Conclure en utilisant Bézout.

On utilisera ce résultat pour montrer le corollaire :

Corollary 4.5.2 (Hexagone mystique de Pascal). *Les paires de côtés opposés d'un hexagone inscrit dans une conique irréductible se rencontrent en trois points colinéaires.*

Figure 4.2 – Hexagone de Pascal



Exercice 26. Soit $\mathcal{C} : f = 0$ une courbe projective plane de degré 4. On suppose que $\mathcal{C}$ est non-singulière. Si L est une droite, elle peut couper $\mathcal{C}$ en des points avec les multiplicités suivantes :

1. $(1, 1, 1, 1)$: c'est le cas générique.
2. $(2, 1, 1)$: c'est le cas où L est tangente au premier point.
3. $(3, 1)$: dans ce cas, le premier point est un point d'inflexion.
4. $(2, 2)$: ces droites sont appelées bitangentes.
5. (4) : ces points sont appelés point d'hyperinflexion. Une quartique générale n'en possède pas.

Calculer les bitagentes à la quartique de Plücker

$$4(x^2 + y^2 + 2y)^2 + (2y + 3)(y + 1)(y^2 - x^2) = -\frac{1}{360}.$$

Pour se faire, on remplace y par $\alpha x + \beta$ et z par 1 dans f puis on exprime le fait que la droite $y = \alpha x + \beta$ est bitangente par le fait que le polynôme en la variable x est un carré parfait : si g est un polynôme de degré 4 quelconque, on a

$$g(x) = ax^4 + bx^3 + cx^2 + dx + e = a(x^2 + b/(2a)x + (4ac - b^2)/(8a^2))^2 + * \cdot x + *.$$

Ceci donne deux conditions, une sur le terme en x et l'autre sur le terme constant. Par le calcul d'un résultant on élimine par exemple β entre ces deux équations pour obtenir une condition sur α. Cette équation (de degré 28 génériquement) donne les valeurs de α puis on remonte aux valeurs de β. On traitera à part les cas des droites à l'infini ou 'verticales'.

4.5.2 Solutions

Correction exercice 24

1. On considère les polynômes $F, G \in k(x)[y]$. C'est un anneau principal dans lequel F et G sont premiers entre eux. En effet s'il existait un polynôme R non constant en y qui divise F et G alors si $S(x)$ est le ppcm des dénominateurs de R on a que $SR|SF$ et $SR|SG$ dans $k[x, y]$ Comme S est de degré 0 en y, il existe un facteur non constant de SR qui divise F et G. On peut donc appliquer le théorème de Bézout dans $k(x)[y]$ et il existe $A_0, B_0 \in k(x)[y]$ tel que $1 = A_0F + B_0G$. En multipliant comme précédemment par les ppcm des dénominateurs de A_0 et B_0, on obtient le résultat.

2. Soit (x, y) un point de $F = G = 0$ alors $d(x) = 0$. Cette équation a donc un nombre fini de solutions en x. On peut raisonner de même avec y.

3. Non car elle a une infinité d'intersections avec l'axe des abscisses.

4. Quitte à changer de coordonnées, on peut supposer que la droite est $x = 0$. On a alors qu'un point $(0 : y, z)$ est solution si et seulement si $F(0, y, z) = 0$. Comme x n'est pas une composante, ceci n'est pas le polynôme nul et c'est donc un polynôme homogène de degré n en y, z. Écrivons ce polynôme sous la forme $\sum a_i y^i z^{n-i} = \prod_{i=1}^{n}(\alpha_i y - \beta_i z)$. Alors les solutions est l'ensemble $\{(\beta_i : \alpha_i)\}$ qui a au plus n éléments.

5. On peut supposer que $P = (0 : 0 : 1)$ et que la droite est donnée par $y = \alpha x$ ou $x = 0$ (qui correspond à $\alpha = \infty$). En injectant dans l'équation, on obtient $F(x, \alpha x, z)$ qui est de degré au plus n en α. C'est également un polynôme homogène de degré n en z (car $(0 : 0 : 1)$ n'est pas sur la courbe) vu comme polynôme dans $k(\alpha)[x, z]$. On cherche les α tel que ce polynôme est des racines multiples. Cela correspond à l'annulation de son discriminant qui est un polynôme de degré au plus $n(n-1)$ en α. On a donc le résultat (la solution $\alpha = \infty$ étant prise en compte : elle n'intervient que lorsque le degré est $< n(n-1)$).

Correction exercice 25 On souhaite que $\alpha P_1(a, b, c) + \beta P_2(a, b, c) = 0$ ce qui est toujours possible. On note $R = \alpha P_1 + \beta P_2$. Alors puisque$p$ est un point de la courbe $\mathcal{D}$ différent de $\mathcal{C}_1 \cap \mathcal{C}_2$, R est $\mathcal{D}$ se coupe en au moins $nm + 1$ points. Compte tenu de leur degré, ceci n'est possible que si $\mathcal{D}$ a une composante en commun avec R. Comme $\mathcal{D}$ est irréductible, il faut que $\mathcal{D}|R$. Soit alors $U = R/\mathcal{D}$. C'est une courbe de degré au plus $n - m$ (car R est de degré au plus n) et on vérifie facilement que $U(q) = 0$ pour tout $q \in \mathcal{C}_1 \cap \mathcal{C}_2$.
On considère pour $\mathcal{C}_1$ et $\mathcal{C}_2$ les deux courbes de degré 3 composées par 3 côtés non adjacents et pour $\mathcal{D}$ la conique irréductible. Alors les neufs points d'intersection sont les 6 points sur la conique et les 3 points d'intersection des cotés opposés (qui n'appartiennent en effet jamais à la même courbe). Le résultat précédent nous dit alors que les 3 points résiduels sont sur une courbe de degré $3 - 2 = 1$.

5 Appendices

5.1 Nullstellensatz

Let k be a (commutative) field and $n > 0$ a positive integer.

Definition 5.1.1. Let S be any subset of $k[X_1, \ldots, X_n]$. We say that

$$V(S) = \{x \in k^n,\ \forall P \in S\ P(x) = 0\}$$

is the *affine algebraic set* associated to S.

Let $F_1, \ldots, F_r \in k[X_1, \ldots, X_n]$ polynomials and $I = (F_1, \ldots, F_r)$ be the ideal generated by the F_is. One also denote $V(F_1, \ldots, F_r) = V(I)$.

Example 5.1.2. $V(\{1\}) = \emptyset$ and $V(\{0\}) = k^n$.

Conversely

Definition 5.1.3. Let V be a subset of k^n. One defines the *ideal associated to* V as

$$I(V) = \{P \in k[X_1, \ldots, X_n],\ \forall x \in V, P(x) = 0\}.$$

Clearly $V(I(V)) = V$ if V is an affine algebraic set (*i.e.* $V = V(I)$ for an ideal I). One has also $I \subset I(V(I))$ but there is not in general equality. A first obstruction is that k needs to be algebraically closed. A second obstruction is that I 'forgets' about the exponents : if $n = 2$ and $I = (X^2)$ then $I(V(I)) = (X) \neq I$.

In the sequel, we assume that k is algebraically closed and not countable (for instance $\mathbb{C}$ but not $\bar{\mathbb{F}}_p$). The following results do not neeed this last hypothesis but the proofs are simpler.

Lemma 5.1.4. *Let K be an extension of k of at most countable dimension (as a k-vector space). Then $K = k$.*

Démonstration. It is enough to show that K is algebraic over k. Otherwise there would be a transcendental element in K and hence a subfield isomorphic to $k(T)$. This subfield contains the non countable family $1/(T - a)$ with $a \in k$ and this family is free. Indeed a relation

$$\sum_{i=1}^{n} \frac{\lambda_i}{T - a_i} = 0$$

implies, multiplying by $T - a_i$ and letting $T = a_i$ that $\lambda_i = 0$. □

Proposition 5.1.5 (weak Nullstellensatz)**.** *Let $I \in k[X_1, \ldots, X_n]$ be an ideal distinct from $k[X_1, \ldots, X_n]$. Then $V(I)$ is not empty.*

Démonstration. We can always embed I in a maximal ideal, so we can assume that I is maximal. Let $K = k[X_1, \ldots, X_n]/I$ be the residual field. Since $k[X_1, \ldots, X_n]$ is a vector space of at most countable dimension over k, it is the same for K. Hence $K = k$. We can consider the images of $X_1, \ldots, X_n$ under the quotient by$I$. They belong to K and hence to k. Let us denote them $a_1, \ldots, a_n$. If $P \in I$ then $P(a_1, \ldots, a_n) = 0$ (by definition of the images under the quotient by I). Hence $(a_1, \ldots, a_n) \in V(I)$. □

To state the Nullstellensatz, we need the notion of *radical*

$$\mathrm{rac}(I) = \{P \in k[X_1, \ldots, X_n],\ \exists r \in \mathbb{N},\ P^r \in I\}.$$

Theorem 5.1.6 (Nullstellensatz)**.** *Let I be an ideal of $[X_1, \ldots, X_n]$. Then $I(V(I)) = \mathrm{rac}(I)$.*

Démonstration. Let $R = k[X_1, \ldots, X_n]$, $I = (P_1, \ldots, P_r)$ (since R is noetherian) and $V = V(I)$. Clearly $\mathrm{rac}(I) \subset I(V(I))$. Conversely, let $P \in I(V)$. We need to prove that $P^m \in I$ for m big enough. Let us consider the 'localized ring' R_P which is isomorphic to $k[X_1, \ldots, X_n, T]/(1 - TP)$. We are going to show that $IR_P = (1) = R_P$. Indeed, this means that $1 = \sum P_i Q_i / P^m$ and hence $P^m \in I$. Let $J = (P_1, \ldots, P_r, 1 - TP)$ in $k[X_1, \ldots, X_n, T]$. One has $V(J) = \emptyset$. Indeed if $(x_1, \ldots, x_n, t) \in V(J)$, then $(x_1, \ldots, x_n) \in V$ and then would cancel P and could not cancel $1 - TP$. Hence $J = (1)$ by the weak Nullstellensatz. This means that $1 = \sum P_i Q_i + A(1 - TP)$ in $k[X_1, \ldots, X_n, T]$ for $A, Q_i \in k[X_1, \ldots, X_n, T]$ and equivalently that $1 = \sum P_I Q_i / P^m$ in R_P. □

Hence, morally, I and V are inverse of each other and create a bridge between the algebraic world and the geometric one.

Corollary 5.1.7. $I(k^n) = I(V(\{0\})) = \mathrm{rac}\,(0) = (0)$.

Corollary 5.1.8. *Let $P \in k[X_1, \ldots, X_n]$ such that $P = P_1^{a_1} \cdots P_r^{a_r}$ with the P_i irreducible and distinct. Then $I(V(P)) = (P_1 \cdots P_r)$.*

Let us say some words about the projective case

Definition 5.1.9. Let S be any subset of $k[X_0, \ldots, X_n]$. We say that

$$V_p(S) = \{x \in \mathbb{P}^n,\ \forall P \in S\ P(x) = 0\}$$

is the *projective algebraic set* associated to S. Conversely if $V_p \subset \mathbb{P}^n$, we define

$$I_p(V_p) = \{P \in k[X_0, \ldots, X_n],\ \forall x \in V_p, P(x) = 0\}.$$

By $P(x) = 0$ we mean that this stands for any representative of x. It is then easy to show that we can assume S to be finite and generated by homogeneous elements.

Example 5.1.10. $V_p((0)) = \mathbb{P}^n$. $V_p((X_0, \ldots, X_n)) = \emptyset$

Theorem 5.1.11 (projective Nullstellensatz)**.** *Let k be algebraically closed, I be a homogeneous ideal of $k[X_0, \ldots, X_n]$ and $V = V_p(I)$.*

1. $V_p(I) = \emptyset \iff (X_0, \ldots, X_n) \in \mathrm{rac}(I)$;
2. *If $V_p(I) \neq \emptyset$ then $I_p(V_p(I)) = \mathrm{rac}(I)$.*

Démonstration. When V_p is empty, it means that V is reduced to the origin of k^{n+1} and therefore $\mathrm{rac}(I) = (X_0, \ldots, X_n)$. Let us assume that $V_p = V_p(I)$ is not empty and let us consider $V = V(I) \subset k^{n+1}$ the associated 'cone'. To prove the second point, since V_p is now non empty, we have $I_p(V) = I(V) = \mathrm{rac}(I)$ by the affine Nullstellensatz. □

A word about automorphisms of the projective space $\mathbb{P}^n$: one can show that there are necessarily linear, although the proof is not elementary (see [Har77, Ex.7.1.1]). Hence this group is isomorphic to $\mathrm{GL}_{n+1}(k)/k^*$.

5.2 Conics, parametrization and projective transformations

5.3 Resultant and Bézout theorem

Let $C = V(F)$ and $C' = V(G)$ be two projective plane curves with no common component over an algebraically closed field k. We have already seen that $C \cap C'$ is finite (see exercice 24). We now want to make this more precise, using an *ad hoc* definition for the multiplicity of intersection. Let us choose the coordinates x, y, z in such a way that $q = (0 : 0 : 1)$ does not belong to C and C' and such that $L : z = 0$ is not a component of C or C'. We also assume that no line through q contains more than one point of intersection of $C \cap C'$. We write in this coordinates $F = A_0 z^m + \ldots + A_m$ and $G = B_0 z^n + \ldots + B_n$ where $A_i, B_i \in k[x, y]$ are homogeneous polynomials of degree i. Since $q \notin C \cup C'$ we get that $A_0(0,0)B_0(0,0) \neq 0$ so there are non-zero constant. From resultant theory, it follows that the resultant $R(x, y)$ of F and G with respect to z is a homogenous polynomial –check this by the definition– of degree mn and that a projective point $(x_0 : y_0)$ is a solution of R if and only if there exists z_0 such that $(x_0 : y_0 : z_0)$ is a solution of F and G (note that there is no issue with the leading terms and that one can consider the points $(x : 1)$ and $(1 : y)$ successively). More geometrically, $(x_0 : y_0)$ is the projection from q on the line L of the intersection point $(x_0 : y_0 : z_0)$. Note that because of our assumption, z_0 is unique for each $(x_0 : y_0)$. We hence obtain our first result.

Proposition 5.3.1. *C and C' have at most mn intersection points.*

To go further, we then define the *multiplicity of intersection* at a point $p = (x_0 : y_0 : z_0)$ as the multiplicity of the 'projective' root $(x_0 : y_0)$ in R. With this definition, one has of course

Proposition 5.3.2. *Counting with multiplicity, C and C' have exactly mn intersection points.*

Remark 5.3.3. More intrinsically,the intersection multiplicity is the length of the $\mathcal{O}_P$-module $\mathcal{O}_P/(F,G)$ where $\mathcal{O}_P$ is the localization with respect to the maximal ideal defining P in the ring $k[x,y]/(F)$ (see [Har77]).
Without this, one can prove the following :

1. the definition of intersection multiplicity does not depend on the choice of a coordinate system. Intuitively, this comes from the fact that the multiplicity of the roots has to be constant as the roots stay the same for any continuous change of variables.

2. Let $\nu_p(C)$ be the multiplicity of a point $p = (a,b)$ on the curve C, i.e. if we write $F = \sum_i \alpha_i (x-a)^i (y-b)^j$, the multiplicity is the degree of the lowest non-vanishing term in this expression. In particular a point p is non-singular if and only if its multiplicity is one. Determinant manipulations show that the intersection multiplicity at p of C and C' is greater or equal to $\nu_p(C) \cdot \nu_p(C')$. If C and C' are non singular at p then the intersection multiplicity is 1 if the tangents are distinct.

Bibliography

[CFA+06] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography.* Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[Ful89] William Fulton. *Algebraic curves.* Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[Har77] R. Hartshorne. *Algebraic geometry.* Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Sil92] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[Was03] Lawrence C. Washington. *Elliptic curves.* Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2003. Number theory and cryptography.